IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 25 June 2014; revised 28 November 2014; accepted 28 December 2014.
Date of publication 8 January 2015; date of current version 3 March 2017.

Digital Object Identifier 10.1109/TETC.2015.2389532

DTD: A Novel Double-Track Approach to Clone Detection for RFID-Enabled Supply Chains

JUN HUANG[1], (Member, IEEE), XIANG LI[1], CONG-CONG XING[2], WEI WANG[3], (Member, IEEE), KUN HUA[4], (Senior Member, IEEE), AND SONG GUO[5], (Senior Member, IEEE)

[1]School of Information and Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]Department of Mathematics and Computer Science, Nicholls State University, Thibodaux, LA 70310 USA
[3]Department of Computer Science, San Diego State University, 5500 Campanile Dr, San Diego, CA 92115 USA
[4]Department of Electrical and Computer Engineering, Lawrence Technological University, Southfield, MI 48075 USA
[5]School of Computer Science and Engineering, University of Aizu, Aizuwakamatsu 965-8580, Japan
CORRESPONDING AUTHOR: J. HUANG (xiaoniuadmin@gmail.com)

ABSTRACT Toward improving the traditional clone detection technique whose performance may be affected by dynamic changes of supply chains and misread, we present a novel and effective clone detection approach, termed double-track detection, for radio frequency identification-enabled supply chains. As part of a tag's attributes, verification information is written into tags so that the set of all verification information in the collected tag events forms a time series sequence. Genuine tags can be differentiated from clone tags due to the discrepancy in their verification sequences which are constructed as products flow along the supply chain. The verification sequence together with the sequence formed by business actions performed during the supply chains yield two tracks which can be assessed to detect the presence of clone tags. Theoretical analysis and experimental results show that our proposed mechanism is effective, reasonable, and has a relatively high clone detection rate when compared with a leading method in this area.

INDEX TERMS RFID, supply chain, clone detection.

I. INTRODUCTION

In radio frequency identification (RFID) enabled supply chains, every product is equipped with an RFID tag which contains a unique product identifier: electronic product code (EPC). Each supply chain participant stores some particular EPC information related to the event in its EPC Information Services (EPCIS) repository for processing. Supply chain partners can record, store, and share information related to these identifiers through RFID infrastructures (e.g., EPCglobal Network).

While RFID technology allows logistics enterprises to implement a transparent and real-time supply chain management system and deliver significant improvements for warehouse management efficiency, it, unfortunately, also brings in some problems. For example, criminals and terrorists carrying clone tags would endanger the safety of patients in medical industry [1], clone tags impose a serious threat to military and national security [2], and the presence of cloned tags can cause severe economic losses in the logistics industries [3]–[6], which directly affects consumers' interests and properties. To resolve these issues, clone-attack prevention and detection methods have been studied.

Prevention: Prevention techniques based on cryptography, such as encryption, decryption, and authentication, typically involve key distribution and management policies. These safety measures usually not only require extra storage spaces, but also need additional encryption operations [3], [7], and therefore are not suitable to be implemented in those low-cost tags that have weak computational power.

Detection: Since no form of prevention strategy can completely prevent clone attacks, clone attack detection techniques will thus be a beneficial supplement. In many cases,

when a system security is compromised or the tracking system malfunctions, counterfeiters may inject unlimited number of clone products into the supply chain. In this regard, clone detection techniques are the only means to protect consumers' interests and constitute a fundamental component of a secure infrastructure. The study of RFID clone tags detection thus not only possesses certain strategic significance, but presents an interesting challenge for researchers as well.

In this paper, we propose an effective clone detecting approach: Double-Track Detection (DTD). Since events are generated by reading RFID tags, we store a verification sequence value ν in a tag memory; this verification sequence value ν is updated to $\nu + 1$ after the tag is detected by the reader, and the related tag event data (updated ν) is stored in the local database. In order to protect privacy, the initial ν-value should be randomized. In cases when an attacker modifies the value of ν, our scheme can still detect clones because it may cause duplicated ν-values. We assume that tag EPC cannot be rewritten, but tag memory can be read and rewritten, and the ν-value is of 8 bits. With products flowing in the supply chain, all ν values form a verification sequence which will show a certain kind of regularity with a series of trajectory. While the verification sequence constitutes one track of product information, business action information of events forms another track. Our clone detection scheme works by checking the correctness of these two tracks with reference to specific tag events. Since it does not depend on a predefined structure of supply chains or a product information flow, it is flexible regarding the dynamically changing supply chains, and suitable for general deployment.

The rest of this paper is organized as follows. Section 2 reviews related work in RFID clone detections. Section 3 briefly describes RFID-enabled supply chains. Our proposed clone detection approach is introduced in Section 4, and is evaluated in Section 5 with comparison to the other research work. Section 6 concludes the paper.

II. RELATED WORK

Staake, Thiesse, and Fleisch [8] presented a preliminary study for the supply chain RFID security solutions based on track-and-trace, highlighting the negative impact of incomplete tracks on cloning attack detections when partners do not record or share track data. Mirowski and Hartnet [9] used statistical anomaly to detect clones by checking the change of the ownership of RFID tags, operations based on readers, tags and reader ID, and the time stamp marks of events. Tag paths (visited readers) are verified by the data saved in tag memory in [10] and [11]. Lee and Bang [12] proposed a pattern mining algorithm, using event track records to mine the legitimate supply chain model by which counterfeit product detection algorithms can be generated. Although these proposed mechanisms are all suitable for the low-cost (EPC C1G2 [13], [14]) tags, they need the related supply chain structure and product flow information in order to work properly, resulting in some weak performance and less robustness when faced with supply chain dynamic changes, product recalls and product transportation errors.

Zanetti, Fellmann, and Capkun [15] proposed a track-and-trace-based privacy-preserving clone detection method, which detects clones by verifying the correctness of two consecutive events in time, without relying on the global knowledge of supply chain structures or the product flow information. It works well with product recalls and product delivery errors. However, the clone detection rate is not improved. A pattern-matching approach was proposed in [16] by Kerschbaum and Oertel to detect illegal transactions between supply chain partners. In [17], Zanetti, Capkun, and Juels proposed to add a random tail and a tail pointer in each user-defined block in EPC tags. In each event, the reader increments the tail pointer and updates the pointed random bits. Clone products can be detected by inspecting the consistency between tails and tail pointers. Although enjoying a relatively high detection rate, this method seriously reduces the tag processing speed, and induces considerably large communication and memory overheads. Bu et al. [5] and Bu, Liu, and Xiao [7] suggested the use of hash functions in detecting clones. Under this scheme, two tags with the same ID always response to the reader queries simultaneously when they are within the reading range of the reader, resulting in the fact that genuine tags and clone tags will make inevitable irreconcilable collisions. Because it requires that genuine tags and clone tags be present at the same time and in the location, this method can only be used in certain scenarios.

III. RFID-ENABLED SUPPLY CHAIN AND EVENTS: A FORMAL VIEW

We consider RFID-enabled supply chains in which each product is equipped with an RFID tag; a product and its tag are considered to be inseparable. Every RFID tag contains a unique product identifier (EPC) which is to be read by different readers at different locations. Each tag-reading at a location creates an event which is stored in the local EPC Information Services (EPCIS) database that can be accessed and shared by supply chain partners via RFID infrastructures (e.g., EPCglobal network), so all the events related to a specific tag data are stored in a distributed manner. Supply chain participants can send related event information (for example, EPC + partners database address) to Discovery Services (DS). Data stored in partners and DS databases can be accessed through authentication and access control mechanisms, and the DS creates a virtual product history path by accessing the distributed EPCIS repositories. Participants in supply chains include manufacturers, wholesalers and retailers, and we assume that the legitimate supply chain participants are not malicious (i.e., they will not cover up attackers).

An event corresponds to a reading of the RFID tag of a product. In local databases, an event for a product (identified by its id = EPC) that occurs at time t, denoted by $e(id, t)$,

is formally defined as follows:

$$
\begin{aligned}
e(id,t) &= (\ell,\tau,\nu,\sigma) \in L \times T \times V \times S \\
L &= \text{set of locations of supply chain participants} \\
T &= \{rcv, shp, inv\} \\
V &= \{0,\ldots,255\} \\
S &= \{tru, fls\}
\end{aligned}
$$

where the attributes $\ell \in L$, $\tau \in T$, $\nu \in V$, and $\sigma \in S$ represent the location, a business transaction (receiving (*rcv*), shipping (*shp*), and inventory (*inv*)), the verification value, and the success (*tru*) or failure (*fls*) of updating the verification value in an event, respectively. Two special events $e(id, t_{in})$ and $e(id, t_{out})$ are created for a product when the product initially enters into the supply chain (i.e., when an EPC tag is assigned to a product at the manufacturer) and eventually leaves the supply chain (i.e., the product is sold at a retailer). So clone products can be easily detected using the corresponding events if they appear on the supply chain before $e(id, t_{in})$ or after $e(id, t_{out})$. An event is considered to be proprietary and confidential. Any supply chain participants only know their direct business partners, and can join or leave the supply chain at any time. We define clones as counterfeit products carrying legitimate EPCs, and multiple readings of one tag are assumed to be processed during the data collection stage.

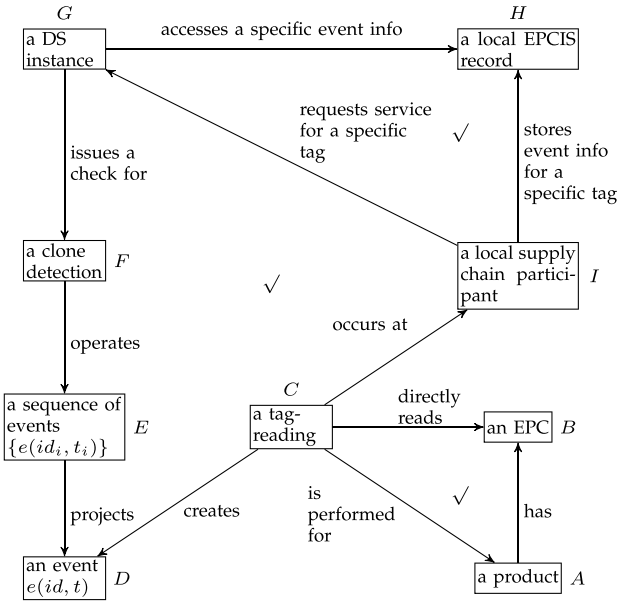


FIGURE 1. The Olog model for RFID-enabled supply chain activities.

The activities associated with clone detection in RFID-enabled supply chains can be understood and formalized as an Olog model [18] as shown in Fig. 1, in which each box represents a type and each arrow denotes a (mathematical) function from the source box to the target box. The check mark ($\surd$) indicates that the enclosing figure is *commutative*, i.e., any two paths leaving from the same source box and ending at the same target box are equivalent. For example, the check mark in the triangle ABC states that the EPC which is being read in a tag-reading is the same EPC of the product for which the tag-reading action is performed.

IV. CLONE DETECTION MECHANISM

A verification sequence is formed by following some stipulated rules except that the initial item in the verification sequence may be assigned randomly by the manufacturer. Our approach detects the presence of clones by examining, for two consecutive events in time, the successiveness of the ν values and the consistency of business transactions.

A. VERIFICATION SEQUENCE CONSTRUCTION

A verification sequence for a tag is built up by successively updating the ν-value in the tag. ν-value updating is completed in a non-interactive manner, i.e., by the participating RFID reader alone. It is a natural extension of the tag-reading process in the sense that a new event containing the updated ν-value will be created after the current event (containing an old ν-value) has been read. The procedure of the ν-value updating includes the following steps: (1) Read the EPC and the ν-value from the tag memory. (2) Increase ν by 1 and write the result back into the tag memory. Tag-writing mistakes are indicated by the status attribute σ. When the reader does not receive an acknowledging response from the tag for the writing operation, or the writing operation fails, σ will be set to *fls*. (3) Create an event $e(id, t) = (\ell, \tau, \nu, \sigma)$, and add it to the local database. Of course, supply chain participants must agree to the above specifications. In addition, the reader is capable of signaling a request at any time to disable the σ-attribute.

B. EVENT COLLECTION

Any supply chain participants may request some product-related information (e.g., EPC + partners database address) from the DS which then accesses the distributed EPCIS databases to create a history path of events for this product. When requested by supply chain partners, our clone detection approach may be authorized, as a third-party service, to access, collect, and analyze all events associated with a particular tag EPC to build the track of events for this tag EPC.

C. DOUBLE TRACK RULE VERIFICATIONS

All available events associated to a specific tag EPC are collected and ordered by time to form an event sequence. The machinery of our clone detection approach can be precisely expressed by the following formula and rules

$$e(id,t) = (\ell,\tau,\nu,\sigma) \tag{1}$$

$$\frac{e(id,t_i)_2 = rcv}{e(id,t_{i+1})_2 = shp/inv \quad e(id,t_i)_1 = e(id,t_{i+1})_1} \tag{2}$$

$$\frac{e(id,t_i)_2 = shp}{e(id,t_{i+1})_2 = rcv \quad e(id,t_i)_1 \neq e(id,t_{i+1})_1} \tag{3}$$

$$\frac{e(id,t_i)_2 = inv}{e(id,t_{i+1})_2 = inv/shp \quad e(id,t_i)_1 = e(id,t_{i+1})_1} \tag{4}$$

$$\frac{e(id,t_i)_4 = tru = e(id,t_{i+1})_4}{e(id,t_{i+1})_3 - e(id,t_i)_3 \equiv 1 \pmod{256}} \tag{5}$$

where t_i and t_{i+1} represent two arbitrary consecutive points in time, and $e(id,t)_k$ $(k = 1, 2, 3, 4)$ means the k-th component of $e(id,t)$.

Formula (1) is just a redisplay of the event formulated in Section 3. Rule (2) states that for any given event, if the business transaction of this event is "receiving" ($e(id,t_i)_2 = rcv$), then this event must be followed by a shipping or inventory event recorded at the same location. In a similar fashion, rule (3) stipulates that a shipping event recorded at a location must be followed by a receiving event recorded at a different location, and rule (4) states that an inventory event must be followed by either an inventory or a shipping event at the same location. Rule (5) states that if the verification values of two time-consecutive events are well documented, then the verification value of the later event is one more than that of the early event modulo 256. We can regroup rules (2)-(5) into two (composite) rules as follows

$$\begin{aligned} \textit{Rule I} &= \textit{rule}(2) \vee \textit{rule}(3) \vee \textit{rule}(4) \\ \textit{Rule II} &= \textit{rule}(5) \end{aligned}$$

and any pair of time-consecutive events passes the check if and only if both Rule I and Rule II are satisfied.

D. CLONE DETECTION

We can examine the correctness of all such pairs for any given set of events through the above two rules, thereby forming a double-track inspection for clones. If all examinations yield correct (pass) results, then there is no presence of clones; otherwise, there are some clones. These two situations are illustrated in Fig. 2(a) and 2(b) respectively, where 2(a) shows the detection result with no clone products and 2(b) with clone products. Note, interestingly, that the detection of clone existence in 2(b) would have been not possible without Rule II, since Rule I gives a pass to all inspections. Incidentally, accidents may conceal the presence of clones or create incorrect observations leading to a false alarm. There are three types of accidents: misevent, misread, and miswrite and their respective effects are illustrated in 2(c). For instance, due to the misevent at time t_2 or the miswrite at time t_3 the first examination yields a "fail" and therefore causes a false alarm since there is no clone involved in that examination. The result of the third examination should have been a "fail" since there is a clone product; but because of the misreading of the clone tag at time $t_{4<i<5}$, no event is created for this clone product for that time and thus the existence of the clone is concealed.

We now address the issue of determining the cause of failure when the double-track rule verification yields a negative result. That is, does the failure suggest the presence of some clone products or is it caused by the combination of misevent, misread, and miswrite? Assume P_{mr} is the misreading probability of the reader. The readings of the tags can be considered as binomially distributed as shown in formula (6), where N_m is the total number of missing events that would be required to restore all incorrect sequences in the considered track, and N is the total number of events. In order to investigate the relationship between failed rule verifications and the *minimum* number of possible missing events, we focus on Rule I and "forget" about Rule II and the business transaction *inv* since these two elements can only increase the number of possible missing events. The result is shown in Table 1 where ℓ_i and τ_i are used to denote $e(id,t_i)_1$ and $e(id,t_i)_2$ respectively to save the space. When the calculated probability exceeds a certain threshold δ, then the cause of the rule verification failure can be regarded as clones; otherwise, it is due to the combination of misevent,

id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time t	t_1	t_2	t_3	t_4	t_5
Genuine prod event	$(l_1, rcv, 10, tru)$	$(l_1, inv, 11, tru)$	$(l_1, shp, 12, tru)$	$(l_2, rcv, 13, tru)$	$(l_2, shp, 14, tru)$
Tag tracks	l_1	l_1	l_1	l_2	l_2
	rcv	inv	shp	rcv	shp
	10	11	12	13	14
Rule I	pass	pass	pass	pass	
Rule II	pass	pass	pass	pass	
Result	pass	pass	pass	pass	

(a)

id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time t	t_1	t_2	$t_{2<i<3}$	t_3	t_4	t_5
Genu p event	$(l_1, rcv, 10, tru)$	$(l_1, inv, 11, tru)$		$(l_1, shp, 12, tru)$	$(l_2, rcv, 13, tru)$	$(l_2, shp, 14, tru)$
Clone p event			$(l_1, inv, 12, tru)$			
Tag tracks	l_1	l_1	l_1	l_1	l_2	l_2
	rcv	inv	inv	shp	rcv	shp
	10	11	12	12	13	14
Rule I	pass	pass	pass	pass	pass	
Rule II	pass	pass	fail	pass	pass	
Result	pass	pass	fail	pass	pass	

(b)

id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time t	t_1	t_2	t_3	t_4	$t_{4<t<5}$	t_5
Genuine prod event	$(l_1, rcv, 10, tru)$	$(l_1, inv, 11, tru)$ misevent	$(l_1, shp, 10, tru)$ miswrite	$(l_2, rcv, 13, tru)$		$(l_2, shp, 14, tru)$
Clone prod event					$(l_2, inv, 13, tru)$ misread	
Tag tracks	l_1		l_1	l_2		l_2
	rcv		shp	rcv		shp
	10		10	13		14
Rule I	pass		pass	pass		
Rule II	fail		fail	pass		
Result	fail		fail	pass		

(c)

FIGURE 2. Rule verification results for events generated (a) by a genuine product, (b) by both genuine and clone products together, and (c) by both genuine and clone products while misevent, misread, and miswrite are considered.

TABLE 1. Failed rule verifications and the number of misevents.

ℓ_i	τ_i	ℓ_{i+1}	τ_{i+1}	min # of misevents	$N_m(i)$
α	rcv	α	rcv	(α, shp), (β, rcv), (β, shp)	3
α	rcv	α	shp	(α, shp), (β, rcv), (β, shp), (α, rcv)	4
α	rcv	β	rcv	(α, shp)	1
α	rcv	β	shp	(α, shp), (β, rcv)	2
α	shp	α	rcv	(β, rcv), (β, shp)	2
α	shp	α	shp	(β, rcv), (β, shp), (α, rcv)	3
α	shp	β	shp	(β, rcv)	1
α	shp	β	rcv	(γ, rcv), (γ, shp)	2

misread, and miswrite.

$$P_{tr} = 1 - \sum_{k=N_m}^{N} C_k^N P_{mr}^k (1 - P_{mr})^{N-k} \quad (6)$$

$$P_{tr} > \delta \quad (Clone) \quad (7)$$

$$P_{tr} \leq \delta \quad (Read/Write\ error) \quad (8)$$

In summary, we proposed a probability method which is coupled with double-track sequence verifications to determine the presence of clones. The specific steps are as follows: (i) Use Rules I and II to determine if a given pair of time-consecutive events is in the correct order; the answer is positive if and only if both Rule I and Rule II are satisfied. There is no presence of clone products in the given set of events if all examinations for every time-consecutive pair of events yield a positive answer. (ii) When result obtained from (i) is negative, use formulas (6), (7), and (8) to determine the presence of clones.

V. PERFORMANCE EVALUATION

In this section, we evaluate our clone detection scheme by a simulation experiment. A 15-partner supply chain in the form of a 4-level binary tree is constructed by using the Arena [19] simulation software. Products flow in the supply chain from the manufacturer to retailers via one or several distributors. Our clone detection approach will be triggered when a genuine or counterfeit product leaves the supply chain (sold to customers). The manufacturer (top level) produces 1000 genuine products every day, and 10 clone products are randomly injected into different levels in the supply chain on a daily basis.[1] Specific parameters of the simulation are shown in Table 2 (adapted from [17]).

The following aspects regarding our clone detection approach are evaluated: storage space requirement, computation workload, communication cost, and the clone detection rate. The use of a EPC C1G2 RFID tag is considered in the evaluation.

A. STORAGE SPACE REQUIREMENT

Only a small amount (8 bits) of storage space is required for our clone detection scheme which can be generally met by any (even low-cost) tags. Our scheme will not increase the number of events in the local database. The set of relevant attributes of each event is extended by ν and σ, resulting in only 7% increases in event size.

[1]The clone product injection rate is stipulated to be 1% in the simulation. By the way in which the DTD works, if the clone injection rate is higher than 1%, then the clone detection rate would not be less than the current clone detection rate.

TABLE 2. Simulation parameters.

Parameter	Value
Misread probability(P_{mr})	$N(5\%, 1\%)$
Miswrite probability(P_{mw})	$N(5\%, 1\%)$
Misevent probability(P_{me})	$N(5\%, 1\%)$
Production rate for genuine products	1000 products/day
Production rate for counterfeit products	10 products/day
Production time	2 months
Shipping time	8AM every day
Stocking time	$N(3, 0.5)$ days
Transportation time	$N(1, 0.25)$ days
Output load (demand)	Uniformly distributed
Supply-chain structure	4-level binary tree
ν value	8 bits
Counterfeit injection point	Random at any partner

B. COMPUTATION WORKLOAD

Tags themselves do not perform any computations. Readers only perform a primitive operation (increment by 1 for the ν-value stored in tags), and the rule verifications are simple and lightweight logical operations.

C. COMMUNICATION COST

While our clone detection scheme requires the reader perform some extra writing operations, it does not inflict any communication overheads with the local databases at the back end. Also, compared with the tailing mechanism by Zanetti, Capkun, and Juels [17], our scheme induces a simpler communication process that needs to update the ν-value (8 bits) only, while the tailing mechanism requires 3 bytes (16 bits for the tail and the pointer and 8 bits for the flag).

D. CLONE DETECTION RATE

Note that the presence of clones will not be detected by the work in [15] when the business transactions in clones and in genuine products are consistent. This issue, however, is well resolved in our clone detection scheme by enforcing the consecutiveness of the ν-values in two adjacent events in addition to the requirement of business transaction consistency. Clearly, in theory, clones can still be potentially detected even if the business transactions in clone products and in genuine products do not show any evidence of counterfeits, which will lead to a higher rate of clone detections. This theoretical observation is verified by the experimental results: the hit rate of our clone detection scheme is 91.3% when the misread probability $P_{mr} = 0.01$, misevent probability $P_{me} = 0.05$, and the false detection rate $FDR = 0.001$. This is a 6% increase when compared to Zanetti's work in [15] under the same P_{mr}, P_{me} and FDR; moreover, the hit rate of our work is as high as 98.3% when $FDR = 0.04$, as shown in Fig. 3 (a) and (d). Also, Fig. 3 (a) and (b) indicate that misread has a greater impact than misevent on our clone detection approach. Injecting clones into a lower level of the chain generates fewer events than injecting clones into an upper level; for the same number of failed incidents on the double-track checking of adjacent event pairs, a shorter event trace gives clearer evidence on the presence of clones than a longer event trace.

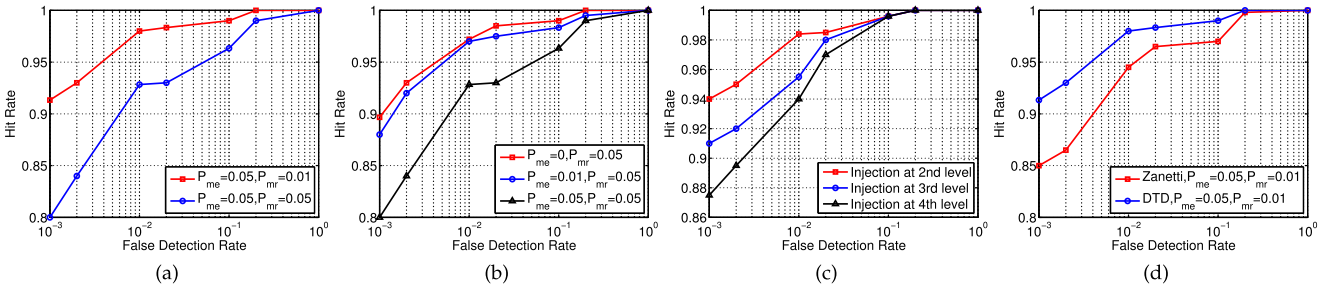


FIGURE 3. Relations between false detection rate and hit rate. (a) Impact of misread and misevent. (b) Impact of misread and misevent. (c) Impact of injection level. (d) Methods comparison.

So for a fixed false detection rate, the hit rate when clones are injected into a lower level is higher than that when clones are injected into an upper level, which is shown in Fig. 3(c).

In short, the simulation results demonstrate that our proposed double-track clone detection approach outperforms Zanetti's work [15] in term of clone detection rate under the same testing environment and with the same parameter settings.

VI. CONCLUSION

Conventional clone product detection techniques in RFID-enabled supply chains depend on the global structure of the supply chain or product flows, and thus are insufficient when the fact that supply chains change dynamically is taken into consideration. We proposed a simple yet effective clone detection scheme which overcomes this inadequacy by devising a double-track checking on the consistency of related events. We argue that our work makes the following contributions:

- The simplicity of the proposed scheme yields its independency on the structure of supply chains and thus makes it universally usable.
- The double-track verification strategy in the proposed scheme eliminates the overlook of clones that is inevitable in Zanetti's work [15].
- The proposed scheme has a competitively high clone detection rate with a reduced communication overhead.

As the future work, we plan to investigate scenarios where readers can be hijacked by attackers and business partners may behave illegally. Consumers' privacy protection issue will be focused on as well.

REFERENCES

[1] E. Lefebvre, L. Castro, and L. A. Lefebvre, "Prevailing issues related to RFID implementation in the healthcare sector," in *Proc. 10th WSEAS Int. Conf. Appl. Comput. Appl. Comput. Sci. (ACACOS)*, Mar. 2011, pp. 266–272.

[2] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, "EPC RFID tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Nov. 2009, pp. 33–42.

[3] J. H. Khor, W. Ismail, and M. G. Rahman, "Prevention and detection methods for enhancing security in an RFID system," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Jan. 2012, Art. ID 891584.

[4] Z. D. Sun and J. D. Sun, "RWMS: RFID based weapon management system," in *Proc. Int. Conf. Manage., Manuf., Mater. Eng.*, Jan. 2012, pp. 386–390.

[5] K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, "Unreconciled collisions uncover cloning attacks in anonymous RFID systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 429–439, Mar. 2013.

[6] M. Lehtonen, F. Michahelles, and E. Fleisch, "How to detect cloned tags in a reliable way from incomplete RFID traces," in *Proc. IEEE Int. Conf. RFID*, Apr. 2009, pp. 257–264.

[7] K. Bu, X. Liu, and B. Xiao, "Fast cloned-tag identification protocols for large-scale RFID systems," in *Proc. IEEE 20th Int. Workshop Quality Service (IWQoS)*, Jun. 2012, pp. 1–4.

[8] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network: The potential of RFID in anti-counterfeiting," in *Proc. ACM Symp. Appl. Comput. (SAC)*, Mar. 2005, pp. 1607–1612.

[9] L. Mirowski and J. Hartnett, "Deckard: A system to detect change of RFID tag ownership," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 7, pp. 89–98, 2007.

[10] E.-O. Blass, K. Elkhiyaoui, and R. Molva, "Tracker: Security and privacy for RFID-based supply chains," in *Proc. 18th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2011, pp. pp. 1–20.

[11] K. Elkhiyaoui, E.-O. Blass, and R. Molva, "CHECKER: On-site checking in RFID-based supply chains," in *Proc. 5th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Apr. 2012, pp. 173–184.

[12] H. S. Lee and H. C. Bang, "Detecting counterfeit products using supply chain event mining," in *Proc. 15th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan. 2013, pp. 744–748.

[13] *EPC C1G2*. [Online]. Available: http://www.impinj.com/, accessed Sep. 1, 2014.

[14] *EPC C1G2*. [Online]. Available: http://www.rfidchina.org/, accessed Sep. 1, 2014.

[15] D. Zanetti, L. Fellmann, and S. Capkun, "Privacy-preserving clone detection for RFID-enabled supply chains," in *Proc. IEEE Int. Conf. RFID*, Apr. 2010, pp. 37–44.

[16] F. Kerschbaum and N. Oertel, "Privacy-preserving pattern matching for anomaly detection in RFID anti-counterfeiting," in *Proc. 6th Int. Conf. Radio Freq. Identificat., Secur. Privacy Issues*, Jun. 2010, pp. 124–137.

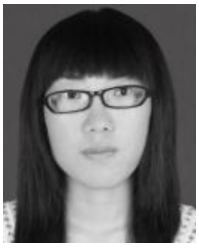
[17] D. Zanetti, S. Capkun, and A. Juels, "Tailing RFID tags for clone detection," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Apr. 2013, pp. 1–17.

[18] D. I. Spivak, *Category Theory for the Sciences*. Cambridge, MA, USA: MIT Press, 2014.

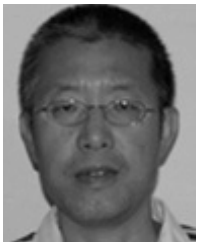
[19] A. Memari, A. Anjomshoae, M. R. Galankashi, and A. R. Bin Abdul Rahim, "Scenario-based simulation in production-distribution network under demand uncertainty using ARENA," in *Proc. 7th Int. Conf. Comput. Converg. Technol. (ICCCT)*, Dec. 2012, pp. 1443–1448.

JUN HUANG (M'10) received the B.S. degree in computer science from the Hubei University of Automotive Technology, China, in 2005, the M.S. (Hons.) degree in computer science from the Chongqing University of Posts and Telecommunications, China, in 2009, and the Ph.D. (Hons.) degree from the Institute of Network Technology, Beijing University of Posts and Telecommunications, China, in 2012. He is currently an Associate Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications.

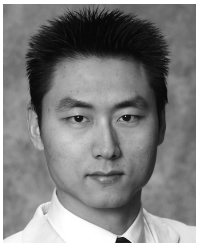
Dr. Huang was a Visiting Researcher with the Global Information and Telecommunication Institute, Waseda University, Tokyo, from 2010 to 2011, and a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, SDSMT, USA, from 2013 to 2014. He has authored over 50 refereed journal/conference papers. His current research interests include network optimization and control, and Quality-of-Service. He is a member of the Association for Computing Machinery (ACM). He received a runner-up of best paper award from ACM Symposium on Applied Computing 2014 and a best paper award from AsiaFI 2011.



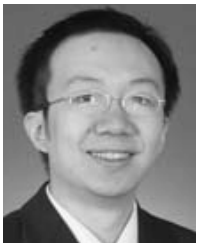
XIANG LI is currently pursuing the master's degree with the School of Communication, Chongqing University of Posts and Telecommunications. His current research interest includes Internet of Things security.



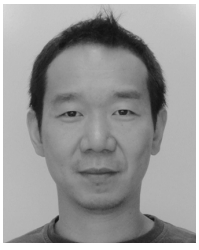
CONG-CONG XING received the Ph.D. degree in computer science from Tulane University, New Orleans, USA. He joined Nicholls State University, Thibodaux, USA, as a Faculty Member in 2001. He is currently a Professor of Computer Science with Nicholls State University. His research interests include theoretical foundations of programming languages, type theory, algebraic graph transformation, and network behavior analysis.



WEI WANG (M'10) received the Ph.D. degree in computer engineering from the University of Nebraska—Lincoln, USA, in 2009. He is currently an Assistant Professor with the Department of Computer Science, San Diego State University, USA. His major research interests include wireless sensor networks, multimedia computing, information security, and educational robotics. He won two best paper awards of the IEEE Wireless Communications and Networking Conference 2008 and the Annual Simulation Symposium in 2011. He serves as an Associate Editor of *Security and Communication Networks* journal (Wiley), the Guest Editor of three Special Issues for Hindawi IJDSN on Energy-Efficient Sensor Networks, Underwater Wireless Sensor Networks, and Data Dissemination in Vehicular Environments, the Program Chair of Association for Computing Machinery Research in Adaptive and Convergent Systems from 2014 to 2015, the Workshop Co-Chair of ICST BodyNets 2013, the Chair of the IEEE CIT-MMC track 2012, the Vice Chair of the IEEE ICCT-NGN track 2011, the Program Chair of the ICST IWMMN 2010, and a Technical Program Committee Member for many international conferences, such as the Global Communications Conference, the IEEE International Conference on Communications, and the IEEE Wireless Communications and Networking Conference.



KUN HUA received the B.S. and M.S. degrees in electrical and computer engineering from the University of Xi'an Jiaotong University, Xi'an, China, in 1999 and 2004, respectively, and the Ph.D. degree in computer and electronic engineering from the University of Nebraska—Lincoln, Lincoln, NE, USA in 2008. From 2009 to 2010, he was with the Department of Computer and Electronics Engineering, University of Nebraska—Lincoln, where he was a Post-Doctoral Research Associate and an Instructor. His research interests include wireless communications, wireless sensor network, digital signal processing, and embedded system design.



SONG GUO received the Ph.D. degree in computer science from the University of Ottawa, Canada. He is currently a Full Professor with the School of Computer Science and Engineering, University of Aizu, Japan. He has authored over 250 papers in referred journals and conferences in these areas. His research interests are mainly in the areas of protocol design and performance analysis for computer networks. He is a senior member of the Association for Computing Machinery. He received three IEEE/ACM best paper awards. He currently serves as Associate Editor of the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING with duties on emerging paradigms in computational communication systems, and on editorial boards of many others. He has also been in Organizing and Technical Committees of numerous international conferences.