A Systematic Approach for the Reliability of RFID Systems

Inoue, Sozo
System LSI Research Center, Kyushu University | Graduate School of Information Science and Electrical Engineering, Kyushu University

Hagiwara, Daisuke
System LSI Research Center, Kyushu University

Yasuura, Hiroto
Graduate School of Information Science and Electrical Engineering, Kyushu University | System LSI Research Center, Kyushu University

https://hdl.handle.net/2324/6794478

出版情報：Proc. IEEE TENCON 2004, pp.183-186, 2004-11. IEEE
バージョン：

A Systematic Approach for the Reliability of RFID Systems

Sozo Inoue*†, Daisuke Hagiwara†, Hiroto Yasuura*†
*System LSI Research Center, Kyushu University
†Graduate School of Information Science and Electrical Engineering, Kyushu University
6–1 Kasuga-Koen, Kasuga-Shi, Fukuoka 816-8580 JAPAN
Email: {sozo|hagiwara|yasuura}@c.csce.kyushu-u.ac.jp

***Abstract*— In this paper, we address reliability issues in the 'Digitally Named World', which is the environment in which RFID (Radio Frequency Identification) tags are attached to any objects in the real world. We propose a systematic approach to maintain the reliability and analyze the effect of our approach, and show that the possibility of identification failure are reduced to $O(p^2)$ $(0 < p < 1)$ from $O(p)$ of the naive approach, where p is the possibility of failure on a single reader, on condition that the first and the final identifications of an object are ensured to be successful.**

I. Introduction

Our vision of the future is the *Digitally Named World*[1], which is the world in which 'Radio Frequency ID (*RFID*) tags', which are silicon chips with IDs and radio frequency functions within small sizes [2], [3], [4], [5], are attached to any goods, and can be found anytime via the networked-RFID readers launching with traceability requirements [6], [7], [8], [9], [11], [13], [10], [12]

However, since RFID is based on RF, the identification may naturally be unreliable caused by range or obstacles. In the library, unidentified books disappear from the inventory. In the air carrier, the baggage unidentified cannot be correctly found. In a supermarket, products unidentified in a basket result in inaccurate data in the sales system.

In this paper, we propose a systematic approach for improving the reliability. The underlying concept is highly important for reliability in ubicomp for stimulus from the real world including RFID identifications.

A. Systematic reliability maintenance

Systematic approach is important as well as individual improvement on each reader and each RFID tag for the total reliability. We focus on the detection of an exceptional state which differs from the ideal state of the real world, such as an identification error of an RFID tag.

Figure 1 is our abstraction. We prepare real-world constraints based on physical principles onto a database in the virtual world. The detection of the exception can be achieved by checking the consistency between the real-world constraints and the obtained data in the operation, including RFID identifications. Examples of real-world constraints are: 1. weight, 2. shape, 3. location, 4. geography which regulates the movement of objects.

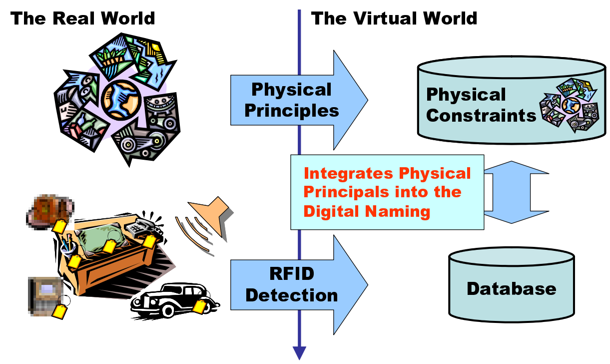

Fig. 1. The Common Abstraction for Systematic Reliability

We believe that this common abstraction should be equipped to the ubicomp system infrastructure. In the rest of the paper, we focus on the specific real-world constraints, which are reasonable and feasible ones in the current trends towards the Digitally Named World.

Here, we clarify the reliability problem and address several viewpoints that can be exploited to solve the problem. As far as the Digitally Named World relies on RF technology which resides in the real world as physical phenomena, the following problems occur:

- An RFID tag fails to be identified by a reader, because of either the length between the RFID tag and the reader, the placement and the direction of the RFID tag, the moving speed of the RFID tag or the reader, or the collision with other RF devices including RFID tags or RFID readers. In the supermarket example, several products attached with RFID tags unidentified in a basket result in inaccurate conversion of real world's events to the sales management system, and leads to inconsistency in the virtual world itself, such as a total sales' miscalculation, or a lack of the total amount.
- A human user can either intentionally or unintentionally make tags unidentified, by means of the failures shown in the previous item. Stealing products means an intentional misidentification, in which a customer displaces the product out of the communication area of the reader at a cash-desk, such that he/she exits skipping the cash-desk,

or hide the product ino a bag with an electromagnetic shield.

These problems originate from the nature of RF, but can be considered as a reliability problem of the Digitally Named World, since the problems cannot be solved by RF technology itself. Systematic approaches which can be applied to the fundamental system support mechanism (such as in a middleware) is important.

B. Real-world constraints

Although plenty of real-world constraints can be considered, our approach starts from the following constraints:

1) **Accompany Constraint**: if the system knows a group of multiple objects moving together, such as products in a basket, it can infer the existence of the all elements of the group only by identifying a part of the group, even if several products could not be identified directly.
2) **Route Constraint**: an object in the real world is sometimes designated specific possible routes to move, such as products routed on belt conveyers, and the products in the supermarket checked at the cash-desk before the exit. The system can consider an invalid route log as an identification error if it knows the routes.

In this paper, we describe the utilization of the constraints and analyze the effect of our approach, and show that the possibility of identification failure are reduced to $O(p^2)(0 < p < 1)$ from $O(p)$ of the naive approach, where p is the possibility of failure on a single reader, on condition that the first and the final identifications of an object are ensured to be successful. Moreover, we show the experimental result of the current implementation. How to capture the constraints is another problem, and we remark it for future challenges.

II. RFID Systems

RFID tags (or simply *tags*) are silicon chips with their IDs, radio frequency functions and some additional logic circuits and memories. In this section, we briefly describe the basic features and applications of RFID tags, which enables the Digitally Named World.

A. Basic features

Figure 2 is the basic architecture of an RFID tag. It has usually no battery, and the power and the clock are supplied via external radio frequency communication. The RFID tag computes with the power and the clock, and sends the result via radio frequency communication. We call the device which communicates with the RFID tag supplying the power and the clock an *RFID reader* (or simply a *reader*). An RFID tag consists of RF circuits which manipulate wireless communication, logic circuits which process small steps of computation, and memories such as a read only memory (ROM) or an electrically erasable read only memory (EEPROM). The memory is currently up to around 64 kilobytes. RFID tags are implemented in many shapes such as an IC card, a key ring, and a seal. There exist RFID tags each of whose dimension except the antenna is under 1mm each [4]. We call information systems which use RFID tags and (often networked) readers *RFID Systems* [5].

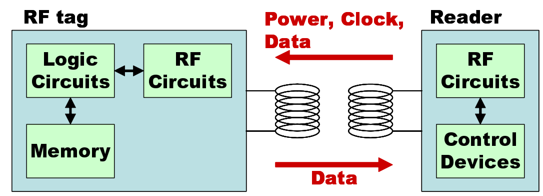

Fig. 2. An RFID tag and a reader

As illustrated in Figure 3, an RFID System is a system for supporting the Digitally Named World, which consists of RFID tags and readers [5].

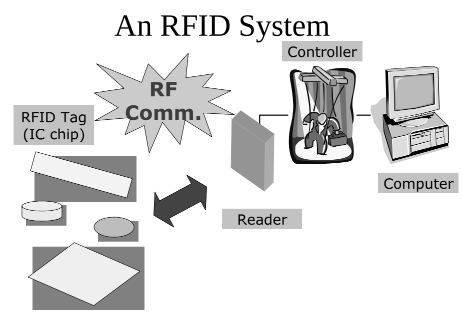

Fig. 3. An RFID System

III. Utilizing the Real-World Constraints

In this section, we present the mechanism for utilizing real-world constraints introduced in Section I-B, which we are developing for improving reliability of the system. We assume the following components as the basic architecture of the system: RFID readers connected to the networks, and the server(s) which provides services supported by the real-world constraints. (1) The server stores the following directed graph $D(V, A)$ initially as an Route Constraint: each RFID reader corresponds to the node $v \in V$, and each possible route of an RFID tag between readers corresponds to the arc $a \in A$. Figure 4 is an example of the graph. (2) The server prepares the data area for restoring Accompany Constraint, as n sets of accompanying objects: $G_0, \cdots, G_n$ which change dynamically as objects gather or separate. The constraints obey a rule for changing Accompany Constraint, configured before the initial execution. Although much work is necessary to establish the rule, we can present the simple rule: the objects identified in a particular reader are always grouped such as $G_i = \{Object4, Object10, User43\}$, and the group identified in a particular reader are always *un*-grouped.

At run time, RFID readers simply send their ID and that of an identified RFID tag to the server when the tag is identified. The server, triggered by the signals $t_{r,1}, \cdots, t_{r,k}$ from a reader r, behaves: For each tag $t_{r,j}$,

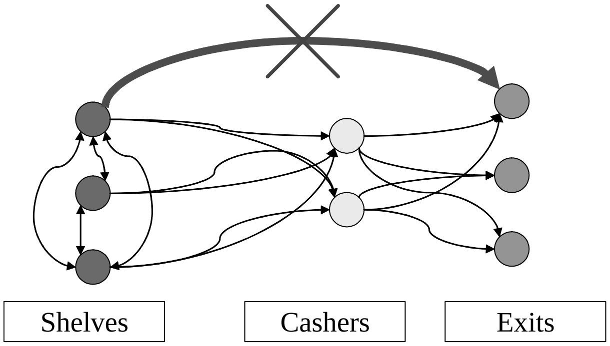

Fig. 4. An example of Route Constraint

1) If $t_{r,j}$ is grouped in a group G_i, throw an exception *ACCOMPANY_EXCEPTION* if some tag $t \in G_i$ is not identified in $t_{r,1}, \cdots, t_{r,k}$.
2) Apply the Accompany Constraint Rules to r and $t_{r,1}, \cdots, t_{r,k}$, and update $G_1, \cdots, G_n$, in which some tags in $t_{r,1}, \cdots, t_{r,k}$ are added to or removed from a group G_l, or create a new group G_{l+1}.
3) Throw an exception *ROUTE_EXCEPTION*, if the arc doesn't exist in the Route Constraint Graph, in which the arc originates from the reader node r' which corresponds to the previous log of the tag identification $t_{r,j}$.

Using the real-world constraint shown above, the system can improve the reliability as: if only $user43$ and $product4$ are identified for a group $G_i = \{Object4, Object10, User43\}$ in the supermarket example, $product10$ can be inferred to be identified by the Accompany Constraint; if a product once identified at a shelf was identified at an exit without identified at the cash-desk, the system can detect that the tracking error of the product occurred at the cash-desk.

IV. Analysis of Improvement

We show the improvement focusing on the effect of Route Constraint. We suppose the Route Constraint $D(V, A)$ includes no self loop. For an object b, we assume the object is transferred along the finite path $< r_{b_1}, \cdots, r_{b_k} >$ called the *real path* for b. We call the sequence $< r_{s_1}, \cdots, r_{s_l} >$ which the server receives for b's transfer the *sequence for* b. Note that $l \leq k$ and any node r_{s_i} is included in the real path. We define an *error* of the real path for b as the state of $< r_{s_1}, \cdots, r_{s_l} > \neq < r_{b_1}, \cdots, r_{b_k} >$. Applying Section III, we can naturally define:

Def. 1: For $D(V, A)$, the real path $t =< r_{b_1}, \cdots, r_{b_k} >$, and a sequence $s =< r_{s_1}, \cdots, r_{s_l} >$, an error of the continuous sub-sequence $< r_{s_i}, r_{s_{i+1}} >$ in s is said to be *detectable* when D has no arc $r_{s_i} r_{s_{i+1}}$. Moreover, an error of t is said to be *detectable* for s , when $r_{b_1} = r_{s_1}$, $r_{b_k} = r_{s_l}$, and any errors of $< r_{s_i}, r_{s_{i+1}} >$ is detectable, and *undetectable* when at least one of the errors is not detectable.

In the following, we classify undetectable errors.

Lemma 1: Errors of t are undetectable for s **iff** at least one of the following is satisfied: **1. (Lost Incoming)** none of $r_{b_1}, \cdots, r_{b_i}$ $(1 \leq i < k)$, are in s, **2. (Lost Outgoing)** none of $r_{b_i}, \cdots, r_{b_k}$ $(1 < i \leq k)$, are in s, **3. (Lost Parallel Path)** for 2 nodes r_i, r_j which has an arc $r_i r_j$, a path from r_i to r_j other than $< r_i, r_j >$ exists in t, or, **4. (Lost Loop)** for a loop in t such that $t =< r_{b_1}, \cdots, r_{b_i}, \cdots, r_{b_j}, \cdots, r_{b_k} > (b_i = b_j)$, none of the nodes in $< r_{b_{i+1}}, \cdots, r_{b_j} >$ or $< r_{b_i}, \cdots, r_{b_{j-1}} >$ are in s.

Proof: The proof is straightforward from the definition. QED.

For lost incoming / outgoing, many the practical situation can be easy to clarify the start/end point of the real path.

For lost parallel paths, we show graph transformation to avoid lost parallel paths.

Lemma 2: For nodes r_i, r_j which have the arc $r_i r_j$ and have another path from r_i to r_j, replace $r_i r_j$ with a new node r_k and arcs $r_i r_k$, $r_k r_j$. Here, there are no paths from r_i to r_k nor from r_k to r_j except themselves.

Proof: Suppose there is a path from r_i to r_k other than $r_i r_k$, then an incoming arc to r_k other than $r_i r_k$ exists. However, this contradicts that the number of outgoing arcs of r_k is 1. r_k to r_j is likewise. QED.

For lost loops, we show the upper bound of undetectable errors.

Lemma 3: Suppose the error possibility of a reader r is uniformly p $(0 < p < 1)$. For a real path s, the possibility that an error of s is undetectable is less than $2(1-p)p^2$, or $3(1-p)^2p^2$.

Proof: For each loop l_i in s where s loops l_i for $o > 0$ times, and t is detectable, l_i becomes undetectable for the possibility of less than $k(|t|, |l_i|)(1-p)^t p^{o|l_i|} < 2(1-p)p^2$, or $k'(|t|, |l_i|)(1-p)^t p^{o|l_i|} < 2(1-p)p^2$, which corresponds to looping once as lost loop. For s with n loops, the possibility is less than $\{2(1-p)p^2\}^n \leq 2(1-p)p^2$, or $\{3(1-p)^2p^2\}^n \leq 3(1-p)^2p^2$. QED.

Without utilizing Route Constraints, the error rate for s is $1-(1-p)^{|s|}$, i.e., no errors in any node in s. Thus, we reduced the upper bound of the undetectability of s from $O(p)$ of the naive way to $O(p^2)$ $(0 < p < 1)$.

Theorem 1: For a Route Constraint $D'(V', A')$, which is transformed from D shown in Lemma 2, a real path t and the sequence s where $b_1 = s_1$ and $b_k = s_l$, the possibility that an error of s is undetectable is $O(p^2)$.

Proof: Straight forward from Lemma 1-3. QED.

V. Current Implementation

Our method is implemented as a location service in which the message from the closest vending machine is displayed on the terminal to users with active RFID tags sending ID every 7 seconds on 300MHz(Figure 6). The system provides, as well as the usability for users, traceability of users' detailed movement for advanced point of sales system.

We examined the effect of Route Constraint for improving error detection of identifications in a small setting with 3 readers in the campus, letting 19 users move as in Figure 5, and assuming the start/end node (New Lecture Bld.) can identify perfectly for the sake of omitting lost inputs/outputs

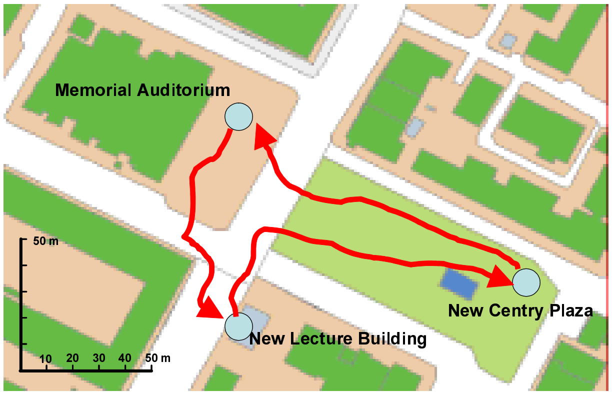

Fig. 5. Users' route

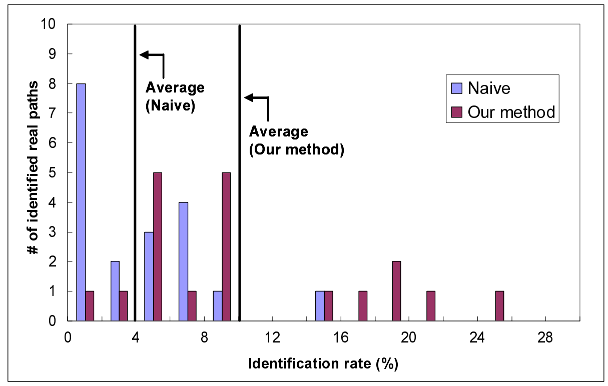

Fig. 7. The distribution of identification rate

(continuous identification error from/to the start/end node of the route).

Fig. 6. The service

Figure 7 is the result of the experience with/without our method logged at the server. An identification rate of a tag on a reader is

$$\frac{|ID| \times 7(sec)}{\frac{T_{next,first}+T_{this,last}}{2} - \frac{T_{this,first}+T_{previous-1,last}}{2}(sec)},$$

where $|ID|$ is the number of identification of the tag on the reader, and $T_{this(previous/next),first(last)}$ is the time of the first (last) identification of the tag on this (previous/next) reader in the real path(resp.). We can see that this rate become quite low since it includes the blank time users move between readers, identification errors, and UDP packet loss from the reader. The figure shows that, applying our method, the average identification rate became 10.01% from 3.9% of the naive approach, which is reasonably close to 7.7% conducted from Theorem 1 and the naive value.

VI. Conclusion

We proposed a method for improving reliability and eventually preserving the consistency in the Digitally Named World by exploiting a simple model of the behavior of the target objects and networked readers. This approach can be/should be generalized to incorporate more effective constraints in the real world, such as total weights, visual information, and sensor data et. al.

References

[1] S. Inoue, S. Konomi, H.Yasuura, "Privacy in the Digitally Named World with RFID Tags", *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing*, Sep. 2002.

[2] P. Hewkin, "Smart Tags - The Distributed Memory Revolution", *IEEE Review*, Jun. 1989.

[3] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels, "Low Cost RFID and the Electronic Product Code", *Proc. Workshop on CHES*, Aug. 2002.

[4] Mitsuo Usami, Masaru Ohki, "The μ-Chip: An Ultra-Small 2.45 GHz RFID Chip for Ubiquitous Recognition Applications", *IECE TRANS. ELECTRON., Vol. E86-C, No. 4*, Apl. 2003.

[5] Finkenzeller K., "RFID Handbook", *Nikkan Kogyo Pbl. Japan*, Feb. 2001.

[6] R. Want, K. P. Fishkin, A. Gujar, B. L. Harrison, "Bridging Physical and Virtual Worlds with Electronic Tags", *Proc. ACM CHI*, May 1999.

[7] Checkpoint Systems, Inc., "Checkpoint Library System", http://checkpointsystems.com/content/library/.

[8] Narita Airport Authority, "Narita Airport News", http://www.narita-airport.or.jp/naa_e/greenport/2001_11_12/05_airport_news.pdf.

[9] MIT AUTO-ID Center, http://www.autoidcenter.org/.

[10] RFID Journal, "Benetton to Tag 15 Million Items", http://www.rfidjournal.com/article/articleprint/ 344/-1/1, Mar. 2003.

[11] FoodTrace, http://www.eufoodtrace.org/

[12] Ubiquitous ID Center, "FTP: Food Traceability Project", http://www.uidcenter.org/press/TEP030623-e1.pdf, Jun. 2003.

[13] Japan Railway Co. Ltd. East, "Suica Card", http://www.jreast.co.jp/suica/.