International Journal of Hybrid Information Technology
Vol.9, No.2 (2016), pp. 1-10
http://dx.doi.org/10.14257/ijhit.2016.9.2.01

Modeling Mutual Intraceability of Mobile RFID Systems Using BRS-based Approach

[1]He Jialiang, [2]Ding Jifeng, [3]Xu Xiaoke and [4]Xu Zhiqiang

[1,2,3]College of Information and Communication Engineering, Dalian Nationalities University, China
[4]Department of digital media technology, Sichuan College of Media and Communications, China
E-mail: urchin2012@sina.com; dingjifeng@yahoo.com.cn; xuxiaoke@sohu.com; starsep928@yahoo.com.cn

Abstract

Intraceability is the most important aspect of RFID security. Mobile RFID readers are used more and more widely, the privacy of mobile reader privacy holders should be considered. In this paper, a BRS-based approach for modeling mutual intraceability of mobile RFID systems is provided. Elements in a RFID protocol can be represented as bigraphs, communications between elements can be represented as reaction rules. RFID intraceability can be represented as behavioral congruence. We take a RFID air interface protocol for mobile RFID systems as a case study and show the usability of this approach.

Keywords*: BRS, Mutual intraceability, Mobile RFID systems*

1. Introduction

The metaphorical space of computer algorithms is mixed with the space of physical reality [1]. A bigraph is composed of a place graph which represents locations of computational nodes, and a link graph which represents interconnection of these nodes. Bigraphs are given dynamics by defining reaction rules that rewrite bigraphs to bigraphs; a Bigraphical Reactive System (BRS) is a set of such rules. Each BRS has a Labeled Transition System (LTS), the behavioral equivalence of which is congruence. There are two principal aims for the theory of BRS: (1) modeling ubiquitous systems, capturing mobile locality in the place graph and mobile connectivity in the link graph; (2) to be a meta-theory encompassing existing calculi for concurrency and mobility. There are bigraphical understanding of π-calculus [1], Petri nets [2], λ-calculus [3], CCS [4], mobile ambient, HOMER [5].

Radio Frequency Identification (RFID) is a technology which is used to identify remote objects labeled with RFID tags by wireless scanning without manual intervention, it is a key technology of the future IOT and has a great economical value. However, a tag cannot be switched off and will answer any request without asking for the agreement of its bearer. A holder's movements can be traced by tracking the RFID tags labeled on the items they are carrying. An early RFID tag will responds to any quest broadcast to it and replies with its unique identifier, so isn't secure. However, the tag encrypts its ID with a key shared between the tag and the reader, if the encryption is deterministic, the message is the same each time and the attacker can trace the tag by simply looking for this bit string [9].

Mobile RFID readers are used more and more widely, the privacy of mobile reader privacy holders should be considered. Since users commonly handle mobile readers while RFID-tagged objects are attached to goods or products in RFID search

ISSN: 1738-9968 IJHIT

systems. Usually, a message from a reader is more easily eavesdrops than a message from a tag [6].

In 2011, a BRS-based approach for modeling RFID tag intraceability is provided [7]. Based on this work, we propose a BRS-based approach for modeling mutual intraceability of mobile RFID systems in this paper. Elements in a RFID protocol are represented as bigraphs, communications between elements are represented as reaction rules, and intraceability is represented as behavioral congruence. A RFID air interface protocol for mobile systems is analyzed as a case study.

The rest of this paper is organized as follows. In the second section, we introduce BRS theory, RFID intraceability, and related works briefly. In the third section, the modeling approach is described detailed, including mappings from elements to bigraphs, communications to reaction rules, and intraceability to behavioral congruence. In the forth section, we take an example as a case study, and analysis results based on this approach are provided. In the fifth section, we draw some conclusions about this paper.

2. Background

2.1 Bigraph and Bigraphical Reactive Systems

The theory of Bigraphical Reactive Systems has been proposed as a topographical meta-model for mobile, distributed agents that can manipulate their own linkages and nested locations. Bigraphs generalize both the link structure characteristic to the π-calculus and the nested location structure characteristic to the Mobile Ambient calculus. A bigraph consists of two structures: the place graph and the link graph. The place graph is a tuple of unordered trees that represents the topology of the system. The roots of the trees are referred to as regions, the nodes are often referred to as places and may represent locations or other process constructors such as action prefixing, some of the leaves may be sites making the bigraph a multi-hole context. Each non-site place is typed with a control and it has a number of ports linked together by the link graph. The link graph represents the connectivity in the system, corresponding to shared names in the λ-calculus. Free names are represented by links connected to a set of names in the (outer) interface of the bigraph [5].

In so-called pure bigraphs, the place graph and the link graph can be considered to be orthogonal structures, since the nesting of the places and the connections of the links have no interrelationship. Pure bigraphs are sufficient to represent calculi such as the pure Mobile Ambient calculus. The orthogonality breaks when we move to so-called binding and local bigraphs. Binding bigraphs has been introduced to capture the notions of binding and scope of names as found in the π-calculus. In binding bigraphs we allow for a node to have binding ports, and require that any other port linked to the same link as a binding port to be within the node of the binding port. The definition of binding bigraphs has been refined into local bigraphs. In local bigraphs, the free names are all explicitly located at the regions of the bigraph, the same name possibly located at several regions. Correspondingly, holes are explicitly annotated by a set of names connected to links. Local bigraphs are used to facilitate the presentation of the λ-calculus [3].

2.2 RFID Intraceability

Privacy property about RFID system may be split in two classes broadly: tracking, whereby the actions of individuals are recorded and their future behaviors potentially are inferred because of using RFID tags associated with them; and information leakage, whereby personal or intimate information stored in a RFID tag is revealed without the consent of its owner [9]. If responding message in authentication process from a tag or a reader always contains a changeless value, namely the response are linkable to each other or distinguishable from those of other tags or other readers, an adversary can recognize

and locate the tag or the reader by intercepting and analyzing. That is to say, the location privacy of the user that attached by the tag or that hold the mobile reader can be traced.

2.3 Related Works

In [1], Jensen and Milner provide the BRS theory, and illustrate bigraphical representations of asynchronous π-calculus(Aπ), and prove the LTS and bisimilarity derived from BRS are corresponding to traditional LTS and bisimilarity of Aπ. In [11], Milner provides axioms for bigraphical structure. In [2], Milner provides bigraphical representations of condition-event Petri-net. In [3], Milner defines binding bigraph and local Bigraph, and provides bigraphical representations of a λ-calculus. In [5], the authors provide bigraphical representations of HOMER.

While a number of papers discuss the privacy problems raised by RFID technologies ([12-14]), few of them precisely define what they mean by intraceability. In [15], Avoine, *et al.*, give a formal definition of intraceability firstly. Some other attempts to formalize intraceability then followed ([10, 16]). However, all these methods are carried out in the computational model, which is poorly supported by automatic tools. In the symbolic world, Deursen, *et al.*, define intraceability [8]. In [9], Myrto, *et al.*, formally define strong and weak forms of intraceability in the applied pi-calculus which in some cases makes it possible to automatically check if a RFID tag running a particular protocol is intraceable. This paper is inspired by Myrto's work.

3. BRS-based Modeling

3.1 Elements

A simple air interface protocol for mobile RFID systems is shown in Figure 1. A reader sends a message (RID) to a tag, the tag responses to the reader with its identifier (TID).

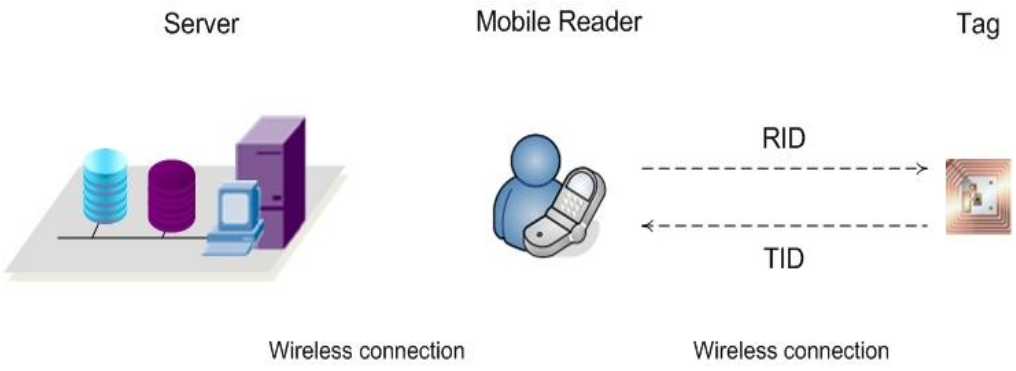


Figure 1. A Simple RFID Interaction for Mobile RFID Systems

Representing this communication with π-calculus as follows.

$$System = Reader|Tag \quad (1)$$

$$Reader = \bar{c}(RID).c(x) \quad (2)$$

$$Tag = vid.c(y).\ \text{If}\ (y = RID)\ \text{Then}\ \bar{c}(TID) \quad (3)$$

In which, c represents a public channel, x and y represent messages being transmitted through the channel, RID is the unique identifier of a reader, TID is the unique identifier of a tag. Representing this communication with bigraphs as follows.

$$\ulcorner\ System\urcorner \equiv \ulcorner\ Reader|Tag\urcorner \quad (4)$$

$$\ulcorner\ Reader\urcorner \equiv Sum \circ (Send_{c,RID}\square_0) \circ Get_{c(x)}\square_1 \quad (5)$$

$$\lceil Tag \rceil \equiv /TID \circ Get_{c,y} \square_0 \circ \text{If } \square_1 \square_2 \square_3 \circ$$
$$(Cnd \square_4 \circ Cmp_{y,RID} \circ T/z | \text{Then}_T \square_5 \circ Send_{c,TID} | \text{Else}_F \square_6 \circ 0) \quad (6)$$

From above equations, we can extract bigraph controls in table 1.

Table 1. Controls of Bigraph

Control	Activity	Interfaces	Functions
$Sum \square_{0 \ldots} \square_{n-1}$	*Active*	$<n, (\phi, \ldots, \phi), \phi> \rightarrow <1, (\phi), \phi>$	*Merge sites into a region*
$Send_{x,y}$	*Atomic*	$<0, (), \{x, y\}> \rightarrow <1, (\phi), \{x, y\}>$	*Send data,* $\bar{x}(y)$
$Get_{x(z)}$	*Passive*	$<1, (\{z\}), \{x, y\}> \rightarrow <1, (\phi), \{x, z\}>$	*Get data, x(z).P*
$/z$	*Atomic*	$<0, (), z> \rightarrow \varepsilon$	*z is an inner name, vz*
$If \square_0 \square_1 \square_2$	*Passive*	$<3,(\phi, \phi, \phi), \phi> \rightarrow <3,(\phi, \phi, \phi), \phi>$	*If statement*
$Cnd \square$	*Passive*	$<1, (\phi), \phi> \rightarrow <1, (\phi), \phi>$	*Condition expression*
$Cmp_{x,y,z}$	*Atomic*	$<0, (), \{x, y, z\}> \rightarrow <1,(\phi),\{x,y,z,T,F\}>$	*Compar two items, output: T for same, otherwise F*
$Then_T \square$	*Active*	$<1, (\{T\}), \{T\}> \rightarrow <1, (\{T\}), \{T\}>$	*Then statement*
$Else_F \square$	*Active*	$<1, (\{F\}), \{F\}> \rightarrow <1, (\{F\}),\{F\}>$	*Else statement*

Graphical representation of each control in Figure 2.

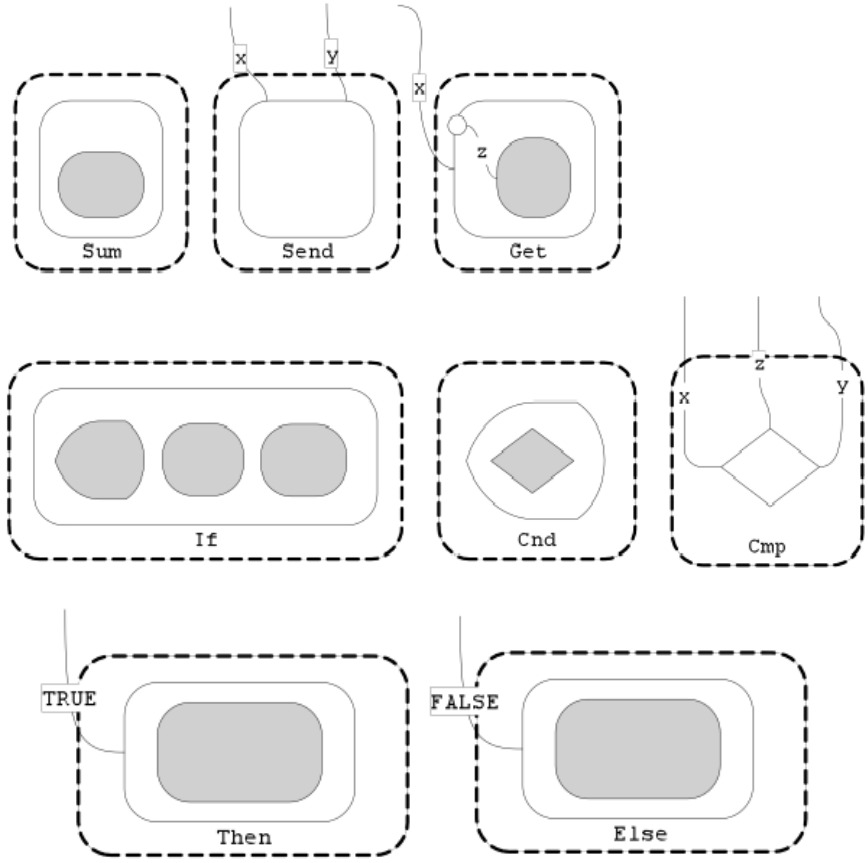


Figure 2. Bigraphical Representations of Controls

The mobile RFID system can be represented as a composed bigraph in Figure 3.

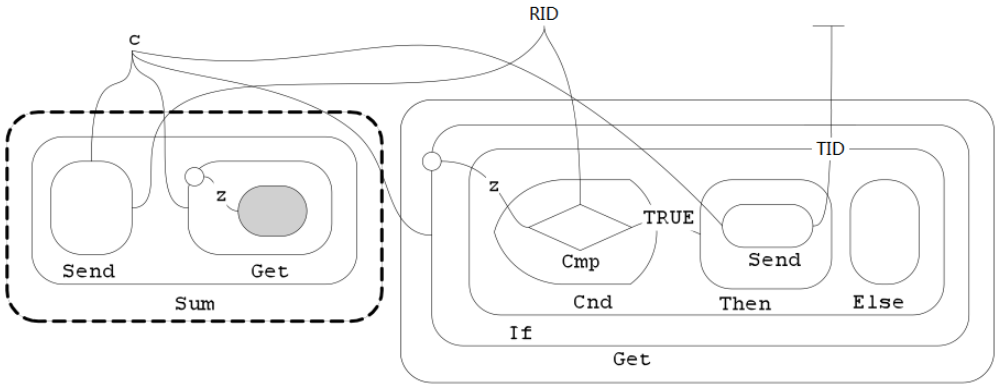


Figure 3. Bigraph Representation of the Mobile RFID System

3.2 Communications

In BRS theory, communications in process calculus such as applied π-calculus can be represented as reaction rules. For example, there is an applied π-calculus communication.

$$\bar{x}(y)|x(z).P \rightarrow \{y/z\}P \tag{7}$$

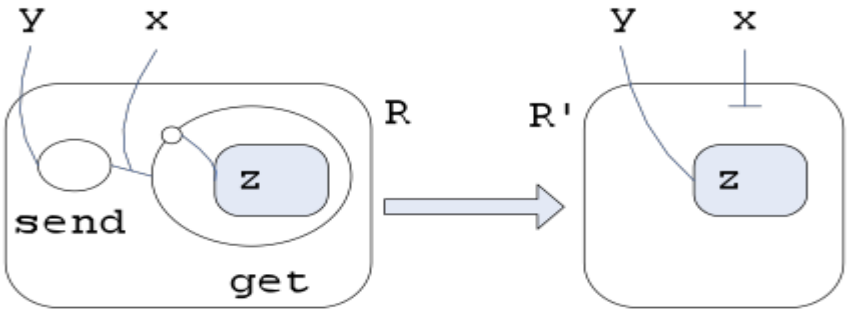


Figure 4. An Example of Bigraph for Communication

We can show its reaction rule in bigraph in Figure 4. The corresponding reaction rule as follows.

$$Send_{x,\,y}|\ Get_{x(z)}\square \rightarrow x|\ y/z\square \tag{8}$$

We can represent other reaction rules in the same way. For an example:

$$\text{If } (y = Hello) \text{ Then } P \rightarrow P \text{ (if } y = Hello) \tag{9}$$

We can show its reaction rule in bigraph in Figure 5..

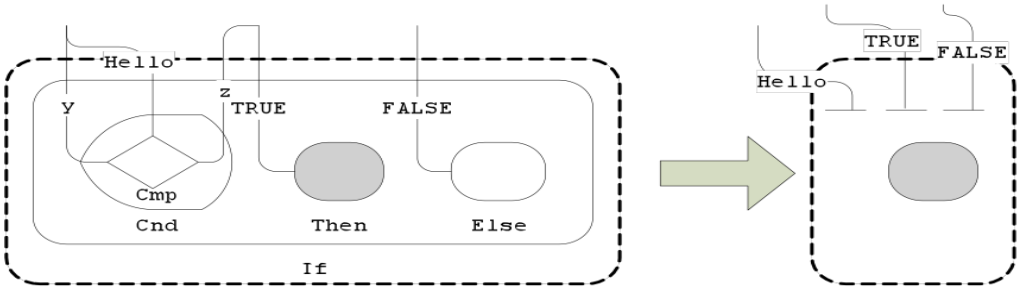


Figure 5. Bigraph for this Reaction Rule

The corresponding reaction rule as follows:

$$\text{If } \square_0\square_1\square_2\circ(Cnd\square_3\circ Cmp_{x,y,z}\circ T/z|\ \text{Then}_T\square_4|\ \text{Else}_F\square_5\circ 0)|\ Hello/x \rightarrow \square_6 \quad (10)$$

3.3 Mutual Intraceability

From the viewpoint of process calculus, mutual intraceability of mobile system is same as behavioral congruence. Let P is a RFID protocol.

$$P \equiv v\tilde{n}.(Server|!R|!T) \quad (11)$$

$$P' \equiv v\tilde{n}.(Server|!R|!T') \quad (12)$$

$$P'' \equiv v\tilde{n}.(Server|!R'|!T) \quad (13)$$

R and R' are readers, *T* and *T'* are tags. *P* preserves mutual intraceability for mobile systems if

$$P \approx P' \quad \text{or} \quad P \approx P'' \quad (14)$$

It is that intraceability would allow readers and tags to execute themselves at most once. The intruder cannot tell the difference between *P* and *P'*. In BRS, we can refer to: Tag intraceability is the same as behavioral congruence of the two bigraphs:

$$\begin{gathered}\ulcorner\ System\urcorner \equiv \ulcorner\ Server\ |!Reader|!Tag\urcorner \\ \approx \\ \ulcorner\ System'\urcorner \equiv \ulcorner\ Server|!Reader|!Tag'\urcorner\end{gathered} \quad (15)$$

Reader intraceability is the same as behavioral congruence of the two bigraphs:

$$\begin{gathered}\ulcorner\ System\urcorner \equiv \ulcorner\ Server\ |!Reader|!Tag\urcorner \\ \approx \\ \ulcorner\ System'\urcorner \equiv \ulcorner\ Server\ |!Reader'|!Tag\urcorner\end{gathered} \quad (16)$$

Namely an intruder cannot recognize the difference between the two systems from behaviors through context.

3.4 Extensions

To represent a real RFID protocol, we may add more bigraph controls. Replication controls of Get and Send are useful in behavioral congruence.

Table 2. Replication Controls

Control	Activity	Interfaces	Functions
$!Send_{x,y}$	*Atomic*	$<0,(),\{x,y\}>\rightarrow<1,(\varphi),\{x,y,y_1\}>$	*Replication and send,* $!\tilde{x}(z)$
$!Get_{x(z)}\square$	*Passive*	$<1,(\{z\}),\{x,z\}>\rightarrow<2,(\varphi,\varphi),\{x,z,z_1\}>$	*Replication and get,* $!x(z).P$

In the RFID protocols, asymmetric encryption and decryption are always useful. In the case of security protocols, typical function symbols include: *pbk* for constructing the public key *pbk*(*k*) associated to the secret key *k*; *aenc* for asymmetric encryption, which takes a plaintext and a public key and returns the corresponding cipher text; *adec* for asymmetric decryption, which takes a cipher text and the corresponding private key and returns the plaintext. $\pi 1$ and $\pi 2$ are respectively the projections on the first component and the second component of a *pair*.

$$\pi 1(pair(x, y)) = x \quad (17)$$

$$\pi 2(pair(x, y)) = y \quad (18)$$

$$adec(aenc(x, pbk(k)), k) = x \quad (19)$$

We can show corresponding controls in Table 3.

Table 3. Controls for Asymmetric Encryption and Decryption

Control	Activity	Interfaces	Functions
$pbk_k\square$	*Atomic*	$<0,(),\{k\}>\rightarrow<1,(\varphi),\{k,pk\}>$	*Generate public key*
$aenc_{x,y}\square_0\square_1$	*Passive*	$<2,(\varphi,\varphi),\{x,y\}>\rightarrow<1,(\varphi),\{x,y,z\}>$	*Encrypt x using key y*
$adec_{x,y}\square_0\square_1$	*Passive*	$<2,(\varphi,\varphi),\{x,y\}>\rightarrow<1,(\varphi),\{x,y,z\}>$	*Decrypt x using key y*
$\pi 1_{x,y}\square$	*Passive*	$<1,(\varphi),\{x,y\}>\rightarrow<1,(\varphi),\{x,y\}>$	*Projection return first*
$\pi 2_{x,y}\square$	*Passive*	$<1,(\varphi),\{x,y\}>\rightarrow<1,(\varphi),\{x,y\}>$	*Projection return second*

4. A Case Study

A simple RFID interaction for mobile RFID systems is represented with π-calculus.

$$P = \nu k.(Server|!R|!T) \quad (20)$$

$$Server = 0 \quad (21)$$

$$R = c(RID).\bar{c}(x_1).\bar{c}(x_2).\bar{c}(x_3).\bar{c}(x_4).\bar{c}(x_5).\bar{c}(x_6). \quad (22)$$

$$\text{If } (\pi 1(adec(x_1,k)) = \pi 1(adec(x_2,k)) = \pi 1(adec(x_3,k)) \text{ and } \pi 1(adec(x_4,k)) = \pi 1(adec(x_5,k)) = \pi 1(adec(x_6,k)) \quad (23)$$

Then Server(0)

$$T = \nu TID.!(\nu n.\dot{c}(x)).$$

$$\text{If } (x = RID) \text{ Then } c(aenc(pair(TID, n), pbk(k))) \quad (24)$$

The reader continuously emits a message (RID) and expects from a tag to answer with its identity (TID) paired with a fresh nonce *n*, the whole asymmetrically encrypted with the reader's public key *pbk*(*k*). Moreover, the reader may send some message to the database if it has seen two particular tags more than three times each.

At first glance, we cannot determine whether the protocol is intraceable. Representing the RFID protocol into BRS. Based on BRS theory, we can conclude that the protocol is traceable for both reader part and tag part.

Firstly, due to the fact that when an outside observer sees a message output on public channel, he knows that there are two tags that have executed themselves three times each and thus that it is not the case that each tag executes itself at most once.

Secondly, due to the fact that when an outside observer sees a message output on public channel, he knows that there are more than one reader that have executed themselves three times each and thus that it is not the case that each reader executes itself at most once.

5. Conclusion

Intraceability is an important problem in RFID domain. Many research works focus on it. A BRS-based modeling approach for mutual intraceability of mobile RFID systems is provided in this paper. We take a simple RFID air interface protocol for mobile RFID systems as a case study and find out that the protocol is not meet mutual intraceable using BRS theory. This approach is the first step to verify intraceability of RFID protocols in BRS theory. And automatic verify tools are under development. In the future, more works can be done in automatic BRS-based verification of RFID security protocols. And more, as bigraph is a topological meta-theory, the factors of space and time can be considered to modeling RFID security protocols.

Acknowledgements

This research was supported by Fundamental Research Funds for the Central Universities (No. DC201502060402), and Program for Liaoning Excellent Talents in University (No. LJQ2013125)

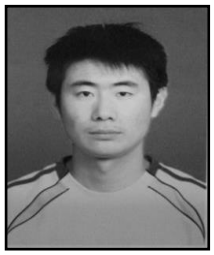
References

[1] O. H. Jensen and R. Milner, "Bigraphs and Mobile Processes (Revised)", University of Cambridge Press, United Kingdom, **(2004)**.
[2] J. J. Leifer and R. Milner, "Transition Systems, Link Graphs and Petri Nets", University of Cambridge Press, United Kingdom, **(2004)**.
[3] R. Milner, "Bigraphs Whose Names Have Multiple Locality", University of Cambridge Press, United Kingdom, **(2004)**.
[4] R. Milner, "Pure Bigraphs", University of Cambridge Press, United Kingdom, **(2005)**.
[5] M. Bundgaard and T. Hildebrandt, "Bigraphical Semantics of Higher-order Mobile Embedded Resources with Local Names", Electronic Notes in Theoretical Computer Science, Electronic Notes in Theoretical Computer Science Press, vol. 154, **(2006)**, pp. 7-29.
[6] J. Y. Chun, J. Y. Hwang and D. H. Lee, "RFID tag search protocol preserving privacy of mobile reader holders", IEICE Electronics Express, vol. 8, no. 2, **(2011)**, pp. 50-56.
[7] H. Jialiang, O. Dantong and X. Youjun, "A BRS-based Approach for Modeling RFID Intraceability", International Journal of Advancements in Computing Technology, vol. 3, no. 11, **(2011)**, pp. 96-103.
[8] T. van Deursen, S. Mauw and S. Radomirovic, "Intraceability of Rfid Protocols", Lecture Notes in Computer Science, Springer, vol. 5019, **(2008)**, pp. 1-15.
[9] M. Arapinis, T. Chothia, E. Ritter and M. Ryan, "Intraceability in the Applied Pi-calculus", In Proceedings of the 1st International Workshop on RFID Security and Cryptography, **(2009)**, pp. 01-06.
[10] S. Vaudenay, "On Privacy Models for Rfid", Lecture Notes in Computer Science, Springer, vol. 4833, **(2007)**, pp. 68-87.
[11] R. Milner, "Axioms for Bigraphical Structure", University of Cambridge Press, United Kingdom, **(2004)**.
[12] S. L. Garfinkel, A. Juels and R. Pappu, "Rfid Privacy: An Overview of Problems and Proposed Solutions", IEEE Security & Privacy, Institute of Electrical and Electronics Engineers, vol. 3, **(2005)**, pp. 34-43.
[13] G. Tsudik, M. Burmester, A. Juels, A. Kobsa, D. Molnar, R. Di Pietro and M. Rieback, "Rfid Security and Privacy: Long-term Research or Short-term Tinkering?", In Proceedings of 2008 ACM Conference on Wireless Network Security, **(2008)**, pp. 160-160.
[14] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Lecture Notes in Computer Science, Springer, vol. 2802, **(2003)**, pp. 201-212.
[15] G. Avoine, E. Dysli and P. Oechslin, "Reducing Time Complexity in Rfid Systems", Lecture Notes in Computer Science, Springer, vol. 3897, **(2005)**, pp. 291-306.
[16] M. Burmester, T. van Le and B. de Medeiros, "Provably Secure Ubiquitous Systems: Universally Composable Rfid Authentication Protocols", In Proceedings of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, **(2006)**, pp. 01-10.

Authors

He Jialiang, He was born in 1977, received the PhD degree in computer software and theory from Jilin University of China in 2012 and the Master degree in computer application from Jilin University of China in 2004. Now he is an associate professor at College of Information and Communication Engineering, Dalian Nationalities University, China. His papers have been published in some well-known international Journals and IEEE conferences. His main interests include Mobile Internet, Internet of Things, and Intelligent Business Information Processing.

Ding Jifeng, He was born in 1978, received the Master degree in Instrument Science and technology from Harbin Institute of Technology in 2005. Now he is a lecturer at College of Information and Communication Engineering, Dalian Nationalities University, China. His main interests include Internet of Things, and Intelligent Information Processing, etc.



Xu Xiaoke, He obtained his Bachelor (2002) in Electronic and Information Engineering and PhD (2008) in Communication and Information System from Dalian Maritime University in China. Now he is working at College of Information and Communication Engineering, Dalian Nationalities University. His research interests include complex networks and complex systems, nonlinear time series analysis, human mobility and dynamics applied to information spreading, and online social network analysis.

Xu Zhiqiang, He was born in 1981, received the Bachelor degree in communication Engineering from Communication University of China in 2004 and the Master degree in Electronics & Communication Engineering from Communication University of China in 2012. At present, he is an assistant professor of Communication & Media Institute of Sichuan, China. He is experienced the fields of Mobile Internet, Internet of Things, Intelligent Information Processing, etc., he also is a candidate of MSc of Technopreneurship & Innovation Program in Nanyang Technological University in Singapore.

