可調式路徑的射頻識別供應鏈系統

RFID Supply Chain System with Adaptive Path

盧而輝 Erl -Huei Lu[1]

邱榮輝 Jung-Hui Chiu[2]

奚正德 Cheng-Ter Hsi[3]

張克章 Henry Ker-Chang Chang[4]

摘要

企業將射頻識別技術應用在供應鏈系統。然而，目前已知設計無法全面滿足安全性，效率和射頻識別供應鏈系統的隱私要求。在本文中，針對產品所有權移交方式，著手設計射頻識別的供應鏈系統架構，並完整歸納三種方案。利用狀態監測可改善供應鏈的能見度不足和產品無效遞送的問題。在鬆散的中心架構下，可信賴的授權者加強追踪回覆的即時性。我們提出的系統，可解決傳統的系統問題。這個系統採用可調整路徑的遞送方式，及鬆散的中心架構，以達到安全與透視性的要求。

關鍵字：射頻識別、供應鏈、可調式路徑、鬆散的中心架構、安全

Abstract

RFID had been applied by the industry in the supply chain systems. Nevertheless, most well-known schemes cannot completely satisfy the important requirements of security, efficiency and privacy of RFID supply chain systems. In this paper, delivering ways of ownership handover are summarized to three cases in comprehensive RFID supply chain system architecture. Status monitor improves inadequate visibility and useless delivery for products. Loosely centralized trusted authority enhances reply of tracking in time. We propose a system which solves problems of traditional system. The system is obviously achieved in a secure way and transparent visibility by adaptive delivered, loosely centralized architecture.

Keywords: RFID, Supply chain, Adaptive path, Loosely centralized architecture, Security

[1] 長庚大學電機工程學系教授(聯絡地址：333 桃園市龜山區文化一路 259 號，聯絡電話：03-2118800 轉 5322，E-mail: lueh@mail.cgu.edu.tw)。

[2] 長庚大學電機工程學系副教授(聯絡地址：333 桃園市龜山區文化一路 259 號，聯絡電話：03-2118800 轉 5698，E-mail: jhchiu@mail.cgu.edu.tw)。

[3] 長庚大學電機工程學系博士生(聯絡地址：333 桃園市龜山區文化一路 259 號，聯絡電話：03-2118800 轉 5698，E-mail: chengder@ms2.kntech.com.tw)。

[4] 長庚大學資訊管理學系教授(聯絡地址：333 桃園市龜山區文化一路 259 號，聯絡電話：03-2118800 轉 5866，E-mail: changher@mail.cgu.edu.tw)。

1. Introduction

Thanks to the technological advance, currently Radio Frequency IDentification (RFID) devices can be used to provide enhanced accuracy for shipping, receiving, and moving goods. They have already helped businesses to reduce costs and improve operational efficiency in current applications. However, some accidents will generate extra cost to solve problem. In a world awash with risks of natural and manmade variety, for example: earthquake, tsunami, terrorist attack, transportation incident, damaged products and etc. If an accident occurs in material flow, one way is skipping the accident node and transfers to next node. Otherwise, products are delivered to specified process node when are checked out to find problem of quality. The abnormal products should be immediately reprocessed and repacked to avoid useless delivery and further cost. Next, security weaknesses of RFID technology must be considered due to the unsecure wireless communication channel between tags and readers, the limited computing power of tags, the potential weakness of the communication protocols. Related RFID security issues have recently become a hot research topic (Henrici, D. 2008; Van Deursen T., and Radomirovi´c, S. 2008a; Rotter, P. 2008; Sarma, S., Weis, S. A. and Engels, D. 2003; Garfinkel, S. L., Juels, A. and Pappu, R. 2005; Juels, A. 2006) and also have the security discussion extended from the RFID technology to supply chain applications (Li, Y., and Ding, X. 2007; Kapoor, G., Zhou, W. and Piramuthu., S. 2008; Van Deursen, T., and Radomirovic, S. 2008b; Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010; Juels, A., Pappu, R., and Parno., B. 2008; Song, B. 2008; Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012; Zuo, Y., and O'Keefe, T. 2011).

The modern supply chain is the primary processing mechanism of supplier. For instance, RFID technology helps distribution companies by delivering more precise inventory control and better visibility and it can reduce the cost of stock holding at all transfer stations in the supply chain system. Extra attention should be paid to the trust problem between all formal partners of supply chain except illegal or unauthorized entity. Only legitimate and authorized enterprises may obtain authorized limited information of tagged product by the trusted authority due to owner agreement during the gathering, inventory, tracking, sharing, and ownership handover procedures in supply chain. All the information flows need to pass through the trusted authority (TA) to handle the material flow in a centralized architecture. Especially, there is no connection exists between partners. Product traceability system is established to maintain information of supply chain. The information includes exposed accidents from TA and monitored product status from partner. TA simultaneously generates updated keys of massive products during multiple ownership handover and sometimes responses tracking requests from authenticated partners. This will make Trusted Authority (TA) to be a bottleneck in supply chain system due to heavy computational load. The result will cause delay and inflexibility for TA to provide better visibility. Hence, TA moves some computational loads to enterprises in a loosely centralized architecture. In order to stay competitive, the enterprises are seeking a supply chain system with high efficiency, low cost, and strong security. For the sake of commercial competition, the issues of security and efficiency are widely discussed in the supply chain systems (Li, Y., and Ding, X. 2007; Kapoor, G., Zhou, W. and Piramuthu., S. 2008; Van Deursen, T., and Radomirovic, S. 2008b; Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010; Juels, A., Pappu, R., and Parno., B. 2008; Song, B. 2008; Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012; Zuo, Y., and O'Keefe, T. 2011). Adversaries can easily intercept, block or fake information by using a forged reader or a compromised tag under insecure wireless environment in the RFID system. A supply chain system must reject the interrogation from the adversary and unauthorized parties.

Following literatures focus on the issues of the security and efficiency of supply chains. Li and Ding (Li, Y., and Ding, X. 2007) mentioned about how to protect RFID communications in supply chain systems. Afterwards, Kappor et al. (Kapoor, G., Zhou, W. and Piramuthu., S. 2008) suggested some modifications for the Li and Ding's protocol to eliminate vulnerabilities to several attacks, such as illegal tracking and Denial of Service (DoS) attack. Van Deursen et al. (Van Deursen, T., and Radomirovic, S. 2008b) showed how to track tagged products by collecting the relationship between the incoming and outgoing products. They (Kapoor, G., Zhou, W. and Piramuthu., S. 2008; Van Deursen, T., and Radomirovic, S. 2008b) also pointed out some flaws of Li and Ding's protocol and exhibited some attacks to authentication, untraceability, unlinkability, and synchronization issues of cryptographic key materials. Later on, Cai et al. (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009, Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010) designed a RFID-tagged supply chain system with dual security modes to improve its security, visibility and efficiency. In 2012, Lien et al. (Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012) presented a RFID based multi-batch supply chain system which involved the mutual authentication, the missing tag identification, and the multi-batch operation ability requirements of supply chain systems. Some traditional systems are declared to have advantages over (Li, Y., and Ding, X. 2007, Juels, A., Pappu, R., and Parno., B. 2008, Song, B. 2008, Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012), due to the summarized four factors: unlinkability (for anti-tracking), visibility (for handover), efficiency (for tag searching), and cost (for tag). However, merely these four factors cannot satisfy security and efficiency requirements entirely. For instance, collision problem is also discovered in Gao et al. (Gao, L., Ma, M., Shu, Y. and Wei, Y. 2013) again. In addition, inadequate visibility by authority and de-synchronous attack are exposed in this paper.

New architecture is designed for loosely centralized architecture to avoid bottleneck of the tightly centralized TA and status monitor to improve visibility. Moreover, it supports three delivering cases for flexibly delivered architecture. Our analysis shows that the proposed system provides a more secure, efficient RFID-based supply chain system with better visibility.

The rest of this paper is organized as follows. In Section 2, the related works and problem description are discussed. The RFID-based supply chain system architecture will be discussed in Section 3. In Section 4, a novel RFID-based supply chain system is proposed. The required protocols to build the novel RFID-based supply chain system will be described in details. In the last section, the conclusion is presented.

2. Related Works and Problem Description

According to the Francis (Francis, J. 2009), supply chains are the totality of processes spanning operations from supplier to end-customer, focused on material, work and information flow. The partners of supply chain are closely linked by processing negotiation through the delivery of information technology for information exchange and sharing, and deliver to the agreed member on time. The Council of Supply Chain Management Professionals (CSCMP) in its own website also emphasizes importance of coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers. Lambert et al. (Lambert, D. M., Cooper., M. C. 2000) adopts the definition of Global Supply Chain Forum that the relationship is a network structure besides one by one between partners of supply chain. Joshi (Joshi, Y. V., 2000) also raised a simple supply chain and flow of goods – multiple channels that deliver the goods about path change and multiple partners in material flow. Material flow is not only single business, but also total value chain. Gartner analyst highlighted a new frontier of performance for supply chain leaders in published rankings of its 2013 and 2014 supply chain top 25 (Rivera, J., and Goasduff. L. 2013; Rivera, J. 2014). More-advanced companies build on multitier visibility and supply network optimization across disparate businesses (Rivera, J., and Goasduff. L. 2013). In 2014, the internet of things allows for monitoring of performance across the value chain but also to collect and analyze the big data has also elevated the importance of supply chain security to prevent theft, counterfeiting and other forms of fraud. Supply chain as trusted and integrated partner is another standout trend (Rivera, J. 2014) and it also rely on security and privacy. The Logistics Performance Index (LPI) of the World Bank ranks the logistics of 160 countries in 2014 (LPI, 2014). The LPI’s one of components is “the ability to track and trace consignments”.

In Asif et al. (Asif, Z., Mandviwalla, M. 2005), RFID technology is able to monitor the quality of the goods by identifying goods in real-time environment of the supply chain. Attaching sensors of tag can detect temperature, humidity and pressure to handle a possible abnormal status. The design may improve the path transparency and prevent deterioration of product through the pre-agreed; for example: cold storage injury and the goods can be transferred to the handle partner early. Visibility by authority in supply chain system means TA could have the products delivering status and could control the delivering process to make sure that the right products to be delivered to the right place at the right time. There are material flows and information flow in proposed general model of supply chain visibility by McIntire (McIntire, J. S. 2010a; McIntire, J. S. 2010b). The most obvious features of huge data are filtered because the process is made visible in supply chain. Supply chain visibility is effective to estimate outcome measures except the case in which stakeholders do not agree on sharing data. Delen et al. (Delen, D., Hardgrave, B. C. and Sharda, R. 2007) conducted a case study using actual RFID data collected to prove better supply-chain management through the enhanced information visibility.

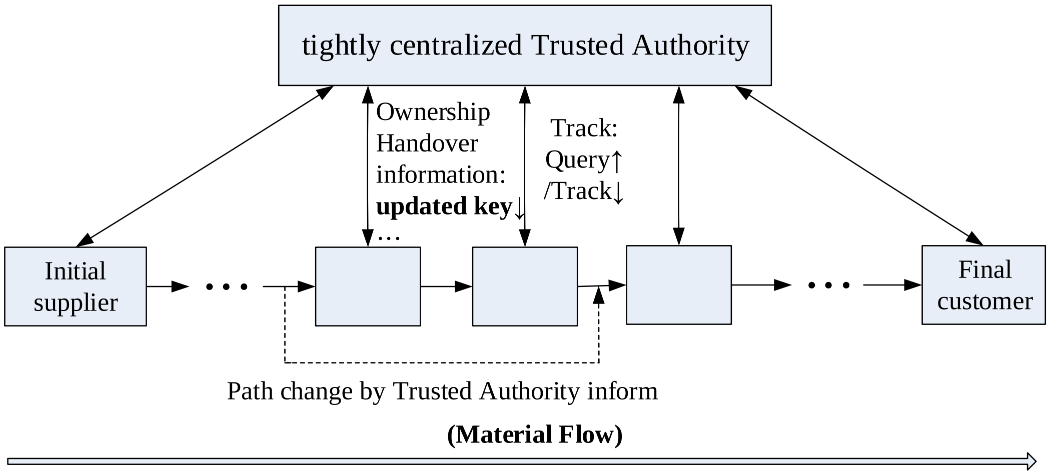
The researchers and companies have always devoted much attention to the security and efficiency problems of the RFID-based supply chain system. Some attacks and inefficiencies of the RFID systems were pointed out by Henrici (Henrici, D. 2008), Deursen et al. (Van Deursen T., and Radomirovi ́c, S. 2008a), Rotter (Rotter, P. 2008), Sarma et al. (Sarma, S., Weis, S. A. and Engels, D. 2003), and Garfiinkel et al. (Garfinkel, S. L., Juels, A. and Pappu, R. 2005). Similar to previous researches (Li, Y., and Ding, X. 2007; Kapoor, G., Zhou, W. and Piramuthu., S. 2008; Van Deursen, T., and Radomirovic, S. 2008b), Cai et al. (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010) summarized some security requirements of an RFID based supply chain system, include authorized access, authenticity of tags, unlinkability, visibility, forward/backward security, and de-synchronization resilience. Additionally, Lien et al. (Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012) added mutual authentication and missing tag identification requirements, and proposed a dynamic path of material flow to improve the tagged products delivery flexibility in a supply chain system. In this paper, previous problems are summarized to (1) inadequate visibility because of inelastic delivery path and loss of status monitor, (2) lower efficient responses of tracking owing to heavy loading for tightly centralized TA, (3) no integrated various delivery in ownership handover.

3. RFID-based Supply Chain System Architecture

The traditional systems declared proposed architecture that are suitable for various types of supply chain structures but only one group of tags follows a fixed handover path in a supply chain system (Li, Y., and Ding, X. 2007; Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010). They accentuate importance of visibility to share data by tracking tags. None of partners shares data of himself to another partner without mutual trusted basis. The current partner does not obtain information of handle partner to change the original delivering path in ownership handover except having trusted basis. To solving trust problem among all partners, this paper supports trusted authority to authorize legal partners through the owner's agreement to obtain limited information in Fig. 2. In addition, the previous literatures (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010; Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012; Gao, L., Ma, M., Shu, Y. and Wei, Y. 2013; Francis, J. 2009; Lambert, D. M., Cooper., M. C. 2000; Joshi, Y. V., 2000; Rivera, J., and Goasduff. L. 2013; Rivera, J. 2014; LPI, 2014; Asif, Z., Mandviwalla, M. 2005; McIntire, J. S. 2010a; McIntire, J. S. 2010b; Delen, D., Hardgrave, B. C. and Sharda, R. 2007) summarized complex situations and transparent visibility.

It is well known that material flow and information flow are key parts of the overall task of supply chain system. According to traditional system architecture in Fig. 1, all the information flows need to pass through the trusted authority (TA) to handle the material flow (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010; Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012). The tightly centralized architecture will make TA to be a bottleneck in the RFID-based supply chain system. In practice, a loosely centralized TA is enough for the RFID-based supply chain system. To meet the demands, a comprehensive RFID supply chain system architecture is proposed, as shown in Fig. 2. The proposed comprehensive architecture not only exposes the information flow and material flow clearly, but also includes the known initial scheduled one by one delivering path as case 1 (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010), the changing delivering path as case 2 (Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012), and the one to many splitting delivering paths of the other delivering way as case 3. Most delivery tasks happen in case 3: from distributor to customer in material flow. Therefore, new architecture may solve problems of traditional system in Section 2 by flexibly delivered path and loosely centralized TA.

In the proposed comprehensive architecture, as shown in Fig. 2, the RFID tags are attached to the pallets, cases, containers or items in the supply chain system. The Trusted Authority (TA) of a supply chain is assumed to be a loosely trusted and centralized back-end server for manufacturers, distributors, suppliers or distribution companies (or vendors), etc. TA monitors current products shipping and delivering status, maintains database information, and sends the relevant message to each partner before identifying the tags. The reader of partner provides power via the RF antenna and exchanges messages with tagged products to execute tags verification.



(Distributed architecture without tightly centralized Trusted Authority)

Fig. 1 Traditional RFID-based supply chain architecture

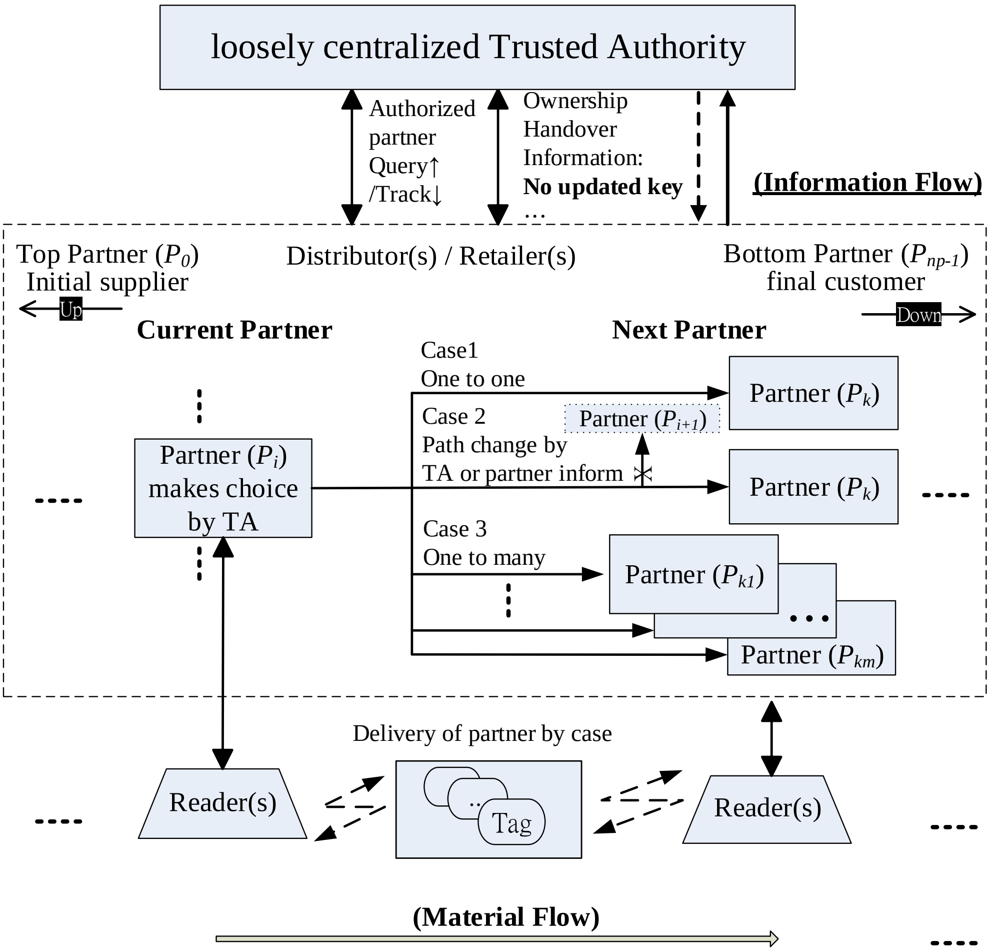


Fig. 2 Comprehensive RFID supply chain architecture

For tag ownership handover, the current partner P_i transports the tags to the next partner P_k following the scheduled order of information and material flow (k is followed with three cases shown in Fig. 2). Based on security requirements, the next partner P_k must ensure that the previous partner P_i no longer has the ability to identify and track tags after ownership handover. After the ownership handover to partner P_k, secret information of tags must be updated to be unknown to all the other partners except the partner P_k and TA.

The proposed scheme has a loosely centralized architecture, which is obvious different from a tightly centralized architecture as that of Cai et al.'s scheme (Cai, S., Li, T., Li, Y. and Deng, R. H. 2009; Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. 2010) or Lien et al.'s scheme (Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. 2012). There are delivering path and session key in TA.

4. A Novel RFID-based Supply Chain System

The proposed novel RFID-based supply chain system is based on the system architecture shown in Fig. 2. The achievement contains transparent visibility through the flexibility delivery path and status monitor. The loosely centralized TA may achieve efficient responses of tracking. Three cases of delivery satisfy for physical operation of material flow in ownership handover. It assumes that the communication channels are secure among partners, their RFID readers, and the trusted authority (TA). The partners always communicates with the tags through the reader. The partners in the supply chain are not all necessary to be trusted. The initialization, tag reading phase and ownership handover process between P_i and P_k are described in this section and illustrated flow chart of the novel system with classified phase in Fig. 3.

4.1 Initialization

The initialization is performed before a new batch product is delivered from top partner P_0. Trusted Authority generates all common secret sharing key and delivers to individual partner and attached tags. They are shared between TA and the ith partner. Product status information of tags is divided into dynamic and static data from attaching sensors and TA. Partner stores both data segments into memory. Tag only stores static data into memory. Expiration date of static data is initialized by TA. Dynamic data is generated in real-time environment which contains temperature, humidity, and pressure, etc. Related parameters are initialized to TA, partners and tags in supply chain.

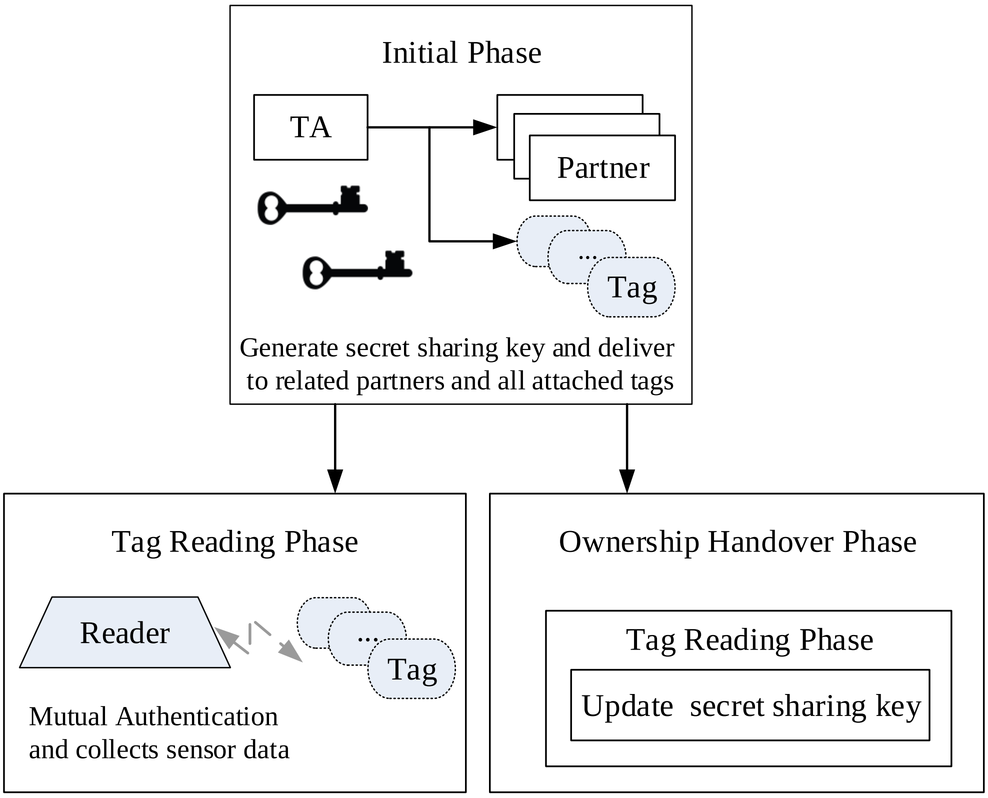

Initial Phase
TA
Partner
...
Tag
Generate secret sharing key and deliver to related partners and all attached tags
Tag Reading Phase
Reader
...
Tag
Mutual Authentication and collects sensor data
Ownership Handover Phase
Tag Reading Phase
Update secret sharing key

Fig. 3 Flow chart of the novel system

4.2 Tag Reading Phase

The tag reading phase conducts the mutual authentication and collects sensor data in Fig. 3. Reader R_i selects tag T_j and common secret sharing between j^{th} tag T_j and partner P_i. Then both performs mutually authentication. The ordering of selected is based on different applications (e.g. import, export and inventory)

4.3 Ownership handover process between P_i and P_k

A new ownership handover process is proposed in Fig. 4. TA is an authority of supply chain to handle the process, such as: manages all partner's database, monitors material delivery flows, decides handover path, and stores information of ownership handover from current partner P_i to next partner P_k or handle partner P_h. The whole process is divided into eight steps. Reader R_i and R_k simultaneously combine tag's responses and related data into after querying all tags. Next partner verified its signature from current partner in Step 5. TA receives its signature and verification result from P_i and P_k in Step 4 and Step 8, and provides visibility to authorized partner by querying and tracking.

Step 1 P_i → TA: P_i notifies TA to perform ownership handover.

Step 2 TA→ P_i: TA sends path to P_i. The $info_i$ contains case number and specified next partner that are determined on case and responses of tags. The next partner is following initial order in case1 and case3 besides TA may adjust delivery handover path of material flow in case2. The handle partner will support resetting next partner to handle partner when sensor data is detected in response of tag, for example: response of the attaching sensor reveals that tags suffer an abnormal temperature, and for safety these products need to be delivered to the handle partner for further inspection.

Step 3 P_i: The Reader R_i of partner P_i performs the generated sharing secret using tag reading phase that contains all the tag's responses. Generally, a little abnormal responses may occur from tags and list them in this Step (4).

Tag T_j generates temporary sharing secret of next partner and collects the sensor data about the temperature, humidity, and pressure, etc during the delivery process of the tagged product. Partner P_i receives sensor and compares it with the safety standard. If collected value not match to safety standard. Current partner will change specified delivery order to handled partner in material flow.

Step 4 P_i → TA: P_i signature with PKI secret key. P_i sends the signature to TA.

Step 5 P_i → P_k: By case of Fig. 2, P_i sends separately its signature to the next partner P_k. If P_k successfully verifies the signature then it continues to perform Step 6, else abort.

Step 6 P_i → P_k: P_i delivers all tags to P_k through the handover path of material flow.

Step 7 P_k: The step is similar to Step 3 to generate signature and updates sharing secret in the updated sharing secret using tag reading phase.

Step 8 P_k → TA: New owner P_k sends the result of verification process verification result to TA through a secure channel. (e.g. successful or not, missing tag identifier)

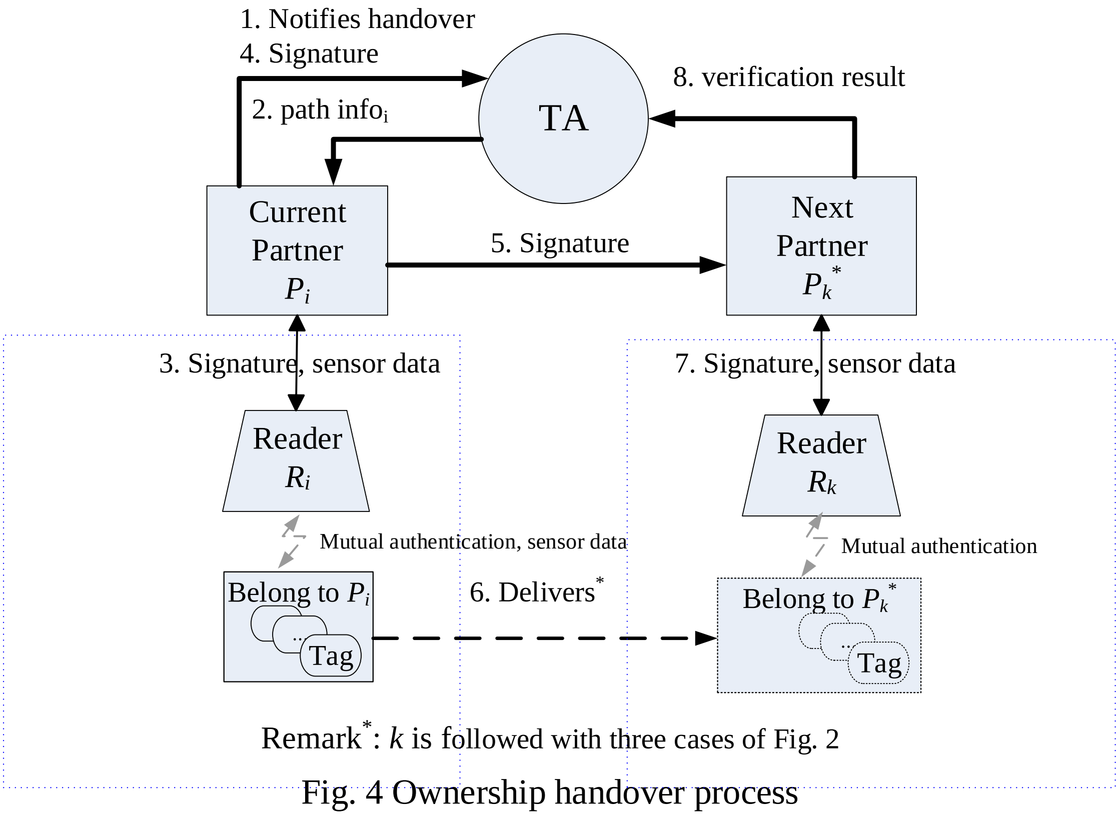


Fig. 4 Ownership handover process

5. Conclusion

Many researchers have paid much attention in efficiency of RFID supply chain systems. Related works and problem description are discussed in Section 2. In this paper, RFID based supply chain architecture and application scenario are described in Section 3. Our proposed system satisfies all of the requirements mentioned in this article. Adaptive delivered and loosely centralized architecture is designed to (1) monitor product status (2) improve useless delivery (3) support quickly reply of tracking (4) integrate three delivering cases. Thus the proposed RFID-tagged supply chain system achieves stronger security and better visibility; this application can extend to different activities for various purposes in the future.

References

Asif, Z., Mandviwalla, M. (2005), “Integrating the Supply Chain with RFID: A Technical and Business Analysis”, Communications of the Association for Information Systems, Vol. 15, No. 24, pp. 393–427.

Cai, S., Li, T., Li, Y. and Deng, R. H. (2009), Ensuring dual security modes in RFID-enabled supply chain systems, In This fifth information security practice and experience conference (ISPEC’09), pp. 372–383, China. April.

Cai, S., Li, Y., Li, T., Deng, R. H. and Yao, H. (2010), “Achieving High Security and Efficiency in RFID-Tagged Supply Chains”, International Journal of Applied Cryptography, Vol. 2, No. 1, pp. 3–12.

Delen, D., Hardgrave, B. C. and Sharda, R. (2007), “RFID for Better Supply-Chain Management through Enhanced Information Visibility”, Production and Operations Management, Vol. 16, No. 5, pp. 613–624.

Francis, J. (2009), “Keeping SCOR in your Supply Chain, Supply-Chain Benchmarking with SCOR”, Supply-Chain Council, http://supply-chain.org/f/SCOR Benchmarking - Presentation.ppt.

Gao, L., Ma, M., Shu, Y. and Wei, Y. (2013), “A security protocol resistant to intermittent position trace attacks and desynchronization attacks in RFID systems”, Wireless Personal Communications, Vol. 68, pp. 1943–1959.

Garfinkel, S. L., Juels, A. and Pappu, R. (2005), “RFID privacy: An overview of problems and proposed solutions”, Security & Privacy Magazine, IEEE, Vol. 3, pp. 34–43.

Henrici, D. (2008), “RFID Security and Privacy: Concepts, Protocols, and Architectures”, Springer Verlag, ISBN 978-3-540-79075-4.

Joshi, Y. V., (2000), “Information Visibility and Its Effect on Supply Chain Dynamics”, Master’s thesis, Massachusetts Institute of Technology, Department of Mechanical Engineering.

Juels, A. (2006), “RFID security and privacy: A research survey”, IEEE Journal on Selected Areas in Communications, Vol. 24 No. 2, pp. 381–394.

Juels, A., Pappu, R., and Parno., B. (2008), “Unidirectional key distribution across time and space with applications to RFID security”, In 17th USENIX security symposium, pp. 75–90.

Kapoor, G., Zhou, W. and Piramuthu., S. (2008), “RFID and information security in supply chains”, In Proceedings of international conference on mobile ad-hoc and sensor networks (MSN’08), pp. 59–62, IEEE Press, December

Lambert, D. M., Cooper., M. C. (2000), “Issues in Supply Chain Management”, Industrial Marketing Management Vol. 29, No. 1, pp. 65–83.

Li, Y., and Ding, X. (2007), “Protecting RFID communications in supply chains”, In Proceedings of the 2nd ACM symposium on information, computer and communications security (ASIACCS’07), pp. 234–241, Singapore, March.

Lien, Y.-H., Hsi, C.-T., Leng, X., Chiu, J.-H. and Chang., H.-C. (2012), “A RFID based multi-batch supply chain systems”, Wireless Personal Communications, Vol. 63 No. 2, pp. 393-413.

LPI, (2014), “Logistics Performance Index - International LPI”, The World Bank, 2014, http://lpi.worldbank.org/international.

McIntire, J. S. (2010a), “A Framework for Visibility Effectiveness”, http://www.supply-chain-visibility.com/2010/06/02/a-framework-for-visibility-effectiveness/.

McIntire, J. S. (2010b), "Updated Visibility Framework", http://www.supply-chain-visibility.com/2010/10/30/updated-visibility-framework/.

Rivera, J., and Goasduff. L. (2013), "Gartner Announces Rankings of Its 2013 Supply Chain Top 25", Winners Announced at Gartner Supply Chain Executive Conference, in Phoenix, Arizona, USA. http://www.gartner.com/newsroom/id/2494115.

Rivera, J. (2014), "Gartner Announces Rankings of Its 2014 Supply Chain Top 25". Winners Announced at Gartner Supply Chain Executive Conference, in Phoenix, Arizona, USA. http://www.gartner.com/newsroom/id/2747417.

Rotter, P. (2008), "A framework for assessing RFID system security and privacy risks", IEEE Journal on Pervasive Computing, Vol. 7, No. 2, pp. 70–77.

Sarma, S., Weis, S. A. and Engels, D. (2003), "Radio-frequency identification: Risks and challenges", RSA CryptoBytes, Vol. 6, No. 1, pp. 1–9, Winter Spring.

Song, B. (2008), "RFID Tag Ownership Transfer", Conference on RFID Security (RFIDSec'08). Budapest, Hungary. July.

Van Deursen T., and Radomirovi ́c, S. (2008a), "Attacks on RFID protocol", eprint, 310.

Van Deursen, T., and Radomirovic, S. (2008b), "Security of an RFID protocol for supply chains, e-Business engineering". In IEEE international conference (ICEBE '08), pp. 568–573, October, 22–24,

Zuo, Y., and O'Keefe, T. (2011), "RFID-enabled Logistic Flow Tracing in Supply Chains: Communication, Protocol, and Security", Global Telecommunications Conference (GLOBECOM 2011), IEEE Communications Society, pp. 1–5.