On The Security of RFID-based Monitoring Mechanism for Retail Inventory Management

Yu Yi Chen[1], Jinn Ke Jan[2], Meng Lin Tsai[2] , Chun Ching Ku[2] and Der Chen Huang[2]
[1] Department of Management Information System, National Chung Hsing University
Taiwan, R.O.C.
[e-mail: chenyuyi@nchu.edu.tw]
[2] Department of Computer Science and Engineering, National Chung Hsing University
Taiwan, R.O.C.
[e-mail: {jkjan, huangdc}@cs.nchu.edu.tw]
[e-mail: morning529@gmail.com]
[e-mail: ccku2001@hotmail.com]
*Corresponding author: Yu-Yi Chen

Received September 15, 2011; revised October 25, 2011; accepted November 2, 2011; published February 28, 2012

Abstract

The aim of this article is to provide a study on the issue of inventory inaccuracy and to show the manner in which RFID technology can improve the inventory management performance. The objective of inventory control is to monitor the stock flow of merchandises in order to understand the operating profit and loss. A proper mechanism of inventory control could be made to help the profitability. As RFID is applied to inventory control, it can improve efficiency, enhance accuracy and achieve security. In this paper, we introduce the evolution of different mechanisms of inventory control with RFID system - counting method, collect-all method, and continuous monitoring method. As for improving the accuracy of inventory check during business hours, continuous monitoring is the solution. We introduce the infrastructure of the RFID inventory management system based on M2M architecture can make the inventory be efficiently monitored with instant warnings.

Keywords: Inventory Control, inventory check, RFID, security, M2M

DOI: 10.3837/tiis.2012.02.004

1. Introduction

The inventory inaccuracy occurs when the inventory level in the information system is inconsistent with the actually available inventory. Although the automation is adopted to improve the inventory management processes, inventory information system and actual inventory are rarely consistent [1]. In the survey researches, Gruen et al. [2] found that 55% of product records were inaccurate and Raman et al. [1] found 65% inaccuracy in their study. The current researches address that retailer inventory records are inaccurate based on the difference between system inventory record and actual inventory [1][2][3]. In general, inventory record accuracy is a critical issue for efficient replenishment and the inventory inaccuracy may make the company perfoemance inefficiently [4]. The factors of the inventory inaccurancy can be classified into five categories: transaction errors, misplacement errors, damage and spoilage, theft, and supply errors [5][6][7]. Misplaced inventory have a significant impact on the inventory to cause profit reduced by 25% at the retailer [1]. For the US retail industry, internal and external theft, administrative errors and vendor cheating resulting in loss of USD 33 billion, about 1.8% of sales in 2001 [8]. Based on the NSRG (National Supermarket Research Group) survey, internal and external theft, receving errors, damage, accounting errors and retail pricing error are estimated at 2.3% of sales [9]. According to the NRSS retail industry survey [10], throughout the year of 2008, the loss of up to 36 billion dollars of which 80% arose from commodities theft and supplier frauds. It is known that inventory control is related directly to retailer's profit. A proper mechanism of inventory control could be made to improve profitability of enterprise.

The objective of inventory control is to monitor the stock flow of merchandises in order to understand the operating profit and loss. In traditional, it is performed by using paper and pen to write down the type and quantity of stock. It takes a lot of manpower and processing time, the accuracy is dependent on the proper execution of manual counting and logging at the inventory check. In the 40s', bar-codes began to emerge [11] for inventory control with less manpower and processing time, and this activity makes the inventory stork information more accurate. For the World-wide market, over 5 billion barcodes are scanned daily [12].

In recent years, a new technology for inventory control has arisen - Radio Frequency Identification. The RFID reader has the ability to interrogate multiple RFID tags at the same time without line of slight. Retail inventory labeled with RFID tags could be checked more efficiently [13]. As the RFID applied as an anti-theft device, this provides retailers with an important additional business benefit from item-level tagging [12]. Several major retailers, such as Wal-Mart and Target in the U.S. and Metro and TESCO in Europe, are making major investments in RFID technology, which is believed as the future of retail inventory control [14][15]. The most benefit is to improve inventory management for many potential advantages from implementing RFID in the supply chain [17]. In the survey research proposed by Delen et al. [18], the accuracy of inventory records can be improved after RFID technology is applied [19][20]. In the research proposed by DeHoratius et al. [21], seven determinants of inventory record inaccuracy are: item cost, quantity sold, sales volume, audit frequency, inventory density, product variety, and the distribution structure. As the result analyzed by Hardgrave et al. [20], there are five determinants of inventory record inaccuracy (item cost, sales velocity, sales volume, inventory density and product variety) can be improved by RFID tagging. Inventory shrinkages can be avoided by continuously monitoring using RFID technology [22]. The potential benefits of RFID system are enormous.

2. Survey of RFID-based Monitoring Mechanisms

Besides the improvement brought by new technologies, the timing of inventory check is also an important consideration from the management point of view. It can be divided into three kinds, during business hours, before (after) business hours, and at the closure of business [21]. However, only the kind of inventory check during business hours can be applied to the 24 hrs opening retailers. The problem of inventory check during business-hours is the ongoing customer shopping, which can cause incorrect result. At such kind of timing, the stock not on the shelves might have been picked up but yet to be checked out, or probably even be stolen. Regarding how to improve the accuracy of inventory check during business hours, continuous monitoring [23] is one possible solution. The deployment of RFID system is necessary based on such kind of monitoring mechanism [24]. Equipped with sensible tags, assimilating and transmitting data contained within those readers and tags autonomously.

RFID applications in business can be classified into two types [26]: the history-oriented tracking application and the real-time-oriented monitoring application. In case RFID is applied to monitor the stock [26][27][28], the efficiency and accuracy of checking stock should be improve as well as the security. It has the potential to build an efficient real-time monitoring system to process large volumes of RFID data and extract useful information [30][31]. The following will introduce and analysis the evolution of different mechanisms of inventory control with RFID system.

The first approach is called counting method. The reader broadcasts the query message to the tags. Then the tags which match the query condition should response to the reader. After receiving the tags' responses, the reader sends the counting result to the server **Fig. 1**.

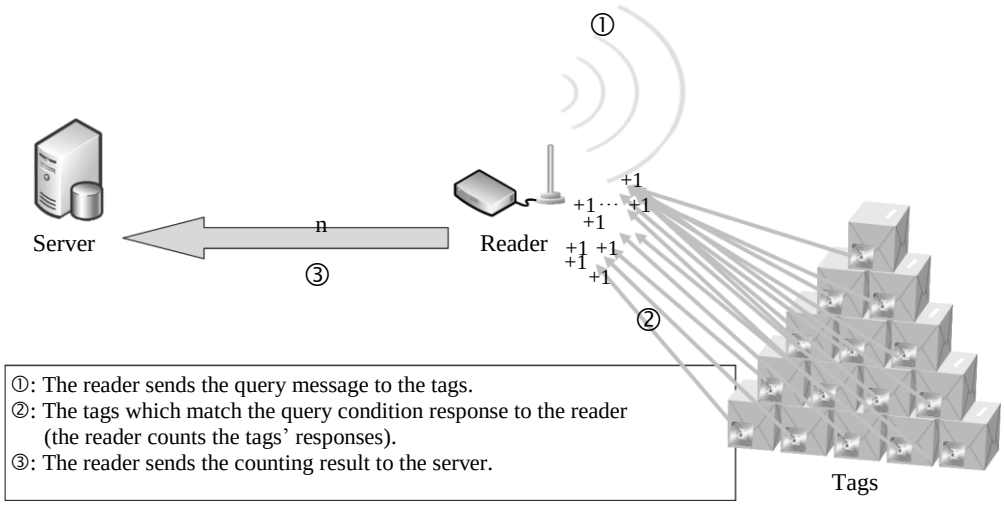

Fig. 1. Counting method

This method is simple and efficient, but the counting result can be tampered easily. The thief has the opportunity to tamper the counting result before it is transferred to the server **Fig. 2**.

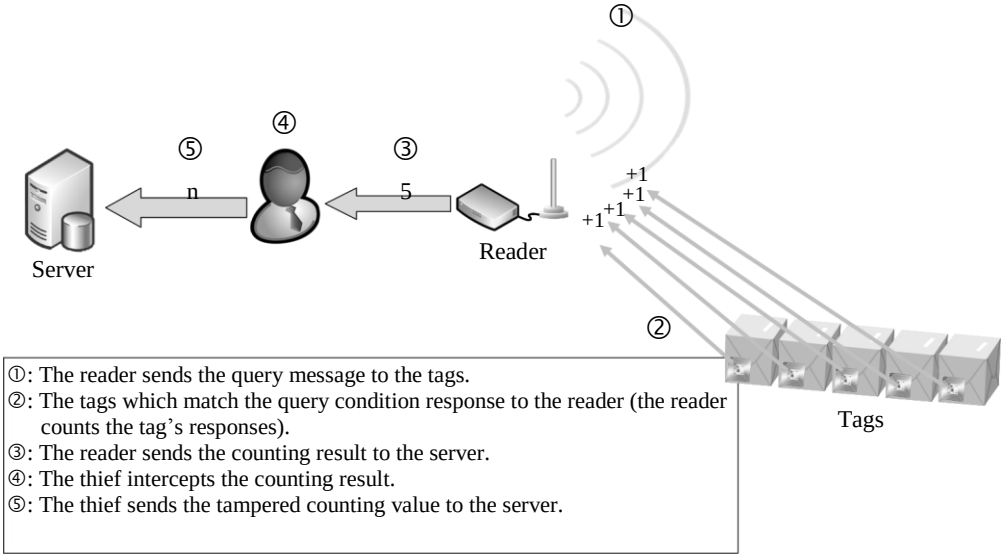

Fig. 2. The vulnerability of counting method

The second approach is called collect-all method [25]. It requires the reader send the identifiable information of each tag to the server for authentication **Fig. 3**. The security of such design is equivalent to the RFID authentication mechanism [32]. However, the authentication requires larger amount of data transferring in between the tags, the reader, and the server. If the number of the monitoring products is large, each product can be monitored exactly but a lot of challenge-response messages makes the performance is not acceptable. The security mechanism should be designed carefully, otherwise the replay attack may be raised.

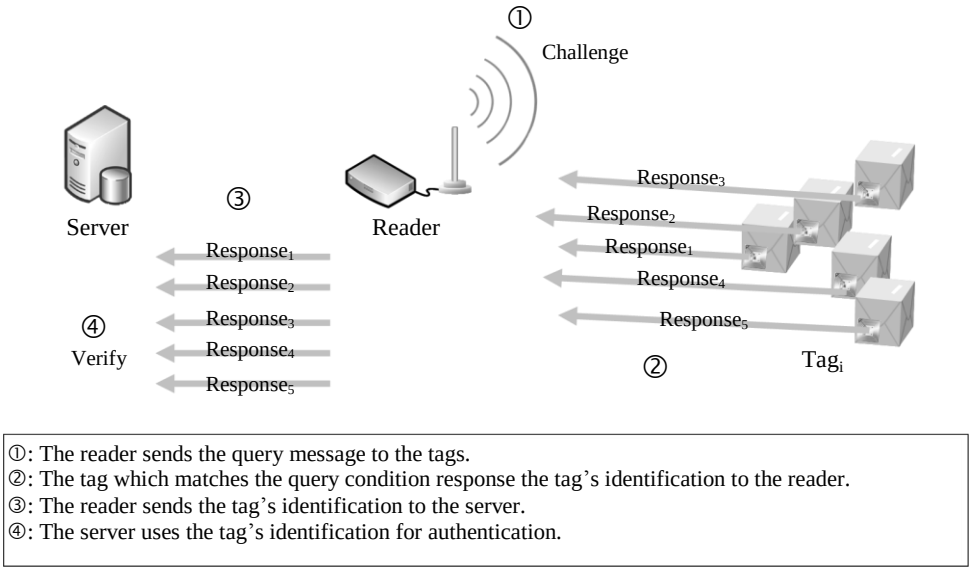

Fig. 3. Collect-all method

The third approach is to use RFID on instant monitoring of stock. For the collect-all method,

each tag can be monitored exactly but a lot of challenge-response messages make the performance not acceptable. Therefore, Tan et al. [25] proposed TRP **Fig. 4** which uses hash function to digest the responses as a verifiable bit stream for the server. The first phase is the server defines a seed and transmits it to the reader. Then the seed is the challenge to be broadcasted to all tags, and each tag can make its hash value according to its key and the seed. The second phase is the reader issues a serious of queries, and is based on the tags' responses to decide the bit stream. The bit stream is equivalent to the digest of all tags' responses according to the server's challenge. The digest value is verifiable by the server.

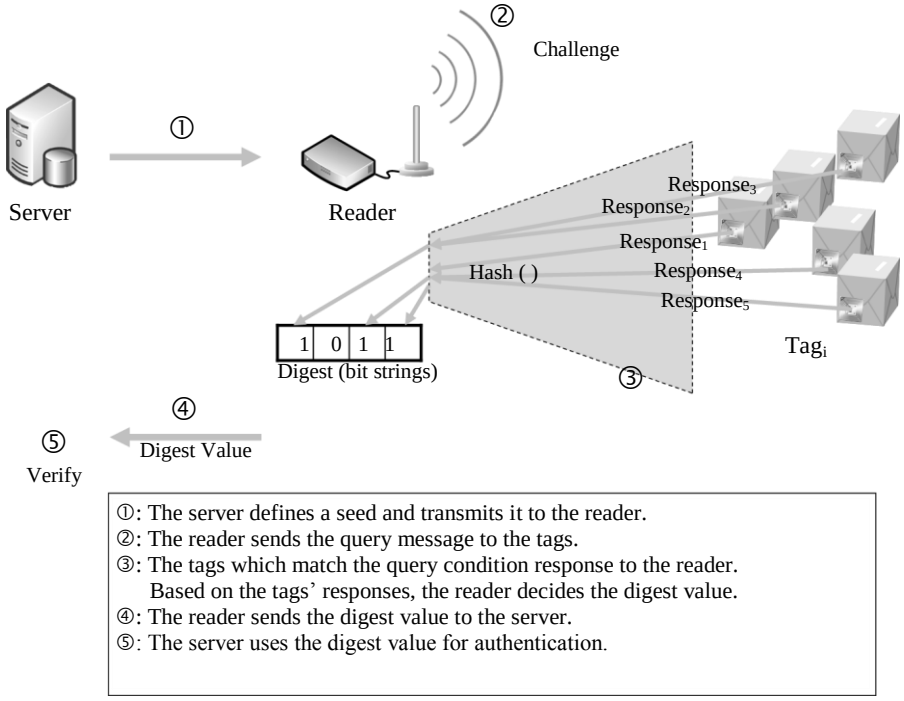

Fig. 4. TRP method

In TRP scheme, the authors found out the internal theft problem. For a set of products, they can be located in two locations and the fake proof is just the combination of two bit streams. As the example **Fig. 5**, the bit streams of two sets are bs_1 and bs_2 which can be combined as the original bit stream bs. Then the separate set of products may be unpacked and tag-removed in an occult room. Therefore, TRP will be failed to monitor the moved products.

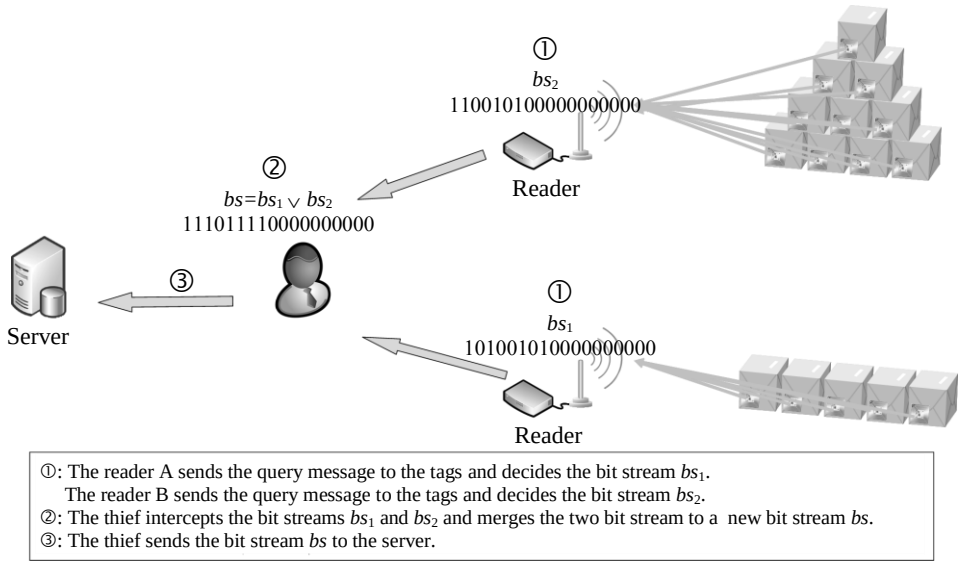

Fig. 5. TRP's insurmountable problems

For theft-prevention, the tags' responses of the separate set should be different as challenged by another reader. Then the combination of two bit streams will not be a valid proof. Such a kind of design was also proposed by Tan et al. [25]. The refined method called UTRP (UnTrusted Reader Protocol) **Fig. 6**. The details of UTRP method are listed in the appendix. However, UTRP is out of performance.

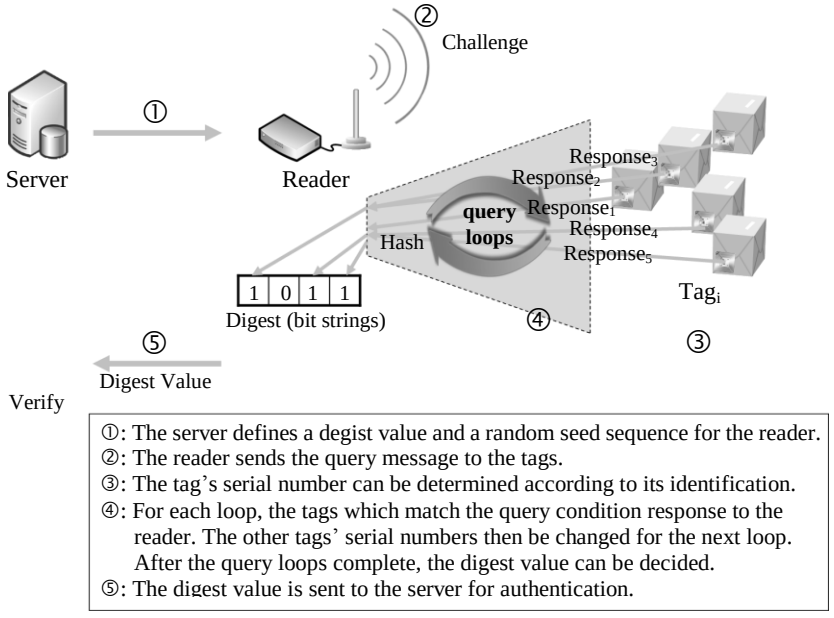

Fig. 6. UTRP method

3. Analysis of RFID-based Monitoring Mechanisms

Tan et al. constructed an RFID application in monitoring, the stock can be real-time monitored. However, there are some disadvantages in Tan's design. We analyze and summarize the following criteria for a RFID monitoring mechanism system.

3.1 Anti-loss

In TRP and UTRP, the tolerance is defined by the parameter m which can be adjusted by the administrator. However, the loss is possibly far greater than this value. Suppose there are 10 tags to be monitored, the frame size f is set to be 18, the maximum value of tolerable missing tags is set to be 2 If the tags' serial numbers are unfortunately collided in high ratio - $sn_i = 1$ for 5 tags, $sn_i = 2$ for another 5 tags. The result of the bit stream should be 110000000000000000. However, just remaining one tag $sn_i = 1$ and another tag $sn_i = 2$ can be interrogated, the result of the bit stream still is 110000000000000000. Therefore, no warning message would be issued even if the actual loss could reach 80%.
As the above mentioned, TRP and UTRP may be fail and cause a lot of loss. To avoid such problem, the variance between the stock and the database records should be exactly checked. Therefore, the tolerance can be defined and the loss can be controlled.

3.2 Accuracy and efficiency

For the counting method, it can work efficiently but the counting result can be tampered easily. For the collection of all method, each tag can be monitored exactly but a lot of challenge-response messages make the performance is not acceptable. In consideration of balancing the efficiency and the accuracy, the challenge-response messages are reduced and only a bit stream is necessary for the server's authentication. However, the price for improving the efficiency is the raising of losses problem in TRP and UTRP.

3.3 Tag privacy

The tags' identifications is not transmitted. It will be secured to against the intercept attack.

3.4 Flexible tolerance

In TRP and UTRP, the tolerance is defined by the parameter m which can be adjusted by the administrator. All kinds of products should be setted to reasonable values to allowing the number of products to be picked up but not yet checked out. Such a design will be useful for the "vacant time" of inventory check, which is caused by the ongoing customer shopping. The threshold of alarm for different products can be adjusted as reference for the inventory control practice.

3.5 Theft-prevention

As TRP had been proposed, the authors found out the internal theft problem. For a set of products, they can be located in two locations and the fake proof is just the combination of two bit streams. Then the separate set of products may be unpacked and tag-removed in an occult room. Therefore, TRP will be failed to monitor the moved products.
For theft-prevention, the moved tags' responses of the separate set should be different as challenged by another reader. Based on this designing mechanism, the internal theft problem mentioned by Tan et al. will not happen.

3.6 Practicality and Scalability

In TRP and UTRP, the parameter f is adjusted for suiting any amount of the monitoring products. Therefore, this mechanism is scalable for inventory control.

4. Improvement of RFID-based Monitoring Mechanism

In this section, we redefine an RFID inventory monitoring system extended to work under Machine-to-Machine (M2M) architecture **Fig. 7**. Based on M2M architecture, the major challenges of M2M design are in the areas of security, privacy, reliability, robustness, latency, and cost-effectiveness [33]. We conduct the improvement of inventory monitoring mechanism, it provides the variety of devices can be connected to share information for obtaining data and transmit through a network to applications [34][35]. The M2M gateway is responsible for extracting raw data from the intelligent readers. The application at end users can analyze data to achieve inventory control. Moreover, the M2M application can query the sensing information of a certain region to the M2M gateway, the server requests the specific reader cover the requested region to route the request to those tags. In M2M network, readers interact with tags and transmit data autonomously. As the reader broadcasts the parameters defined by the server, each tag's serial number can be determined. Then the reader sends out a series of queries, and counts the tags' responses with the bit stream. The bit stream is transmitted to the M2M gateway for authentication.

Step 1. The M2M gateway defines the frame size of the digest value, a random seed, and the bit length of counter for the reader.

Step 2. According to the random seed, the query seed is generated by the reader's secret key. Then the frame size and the query seed are broadcasted to all tags.

Step 3. Each tag's serial number can be determined according to it secret key.

Step 4. For each loop, the tags which match the query condition response to the reader.All responses are counted by the reader to be appended to the bit stream. After the query loops complete, the complete bit stream can be decided.

Step 5. The complete bit stream is transmitted to the M2M gateway for authentication. After the process of efficient hashing and exact counting, the monitor data can be authenticated and evaluated in real time.

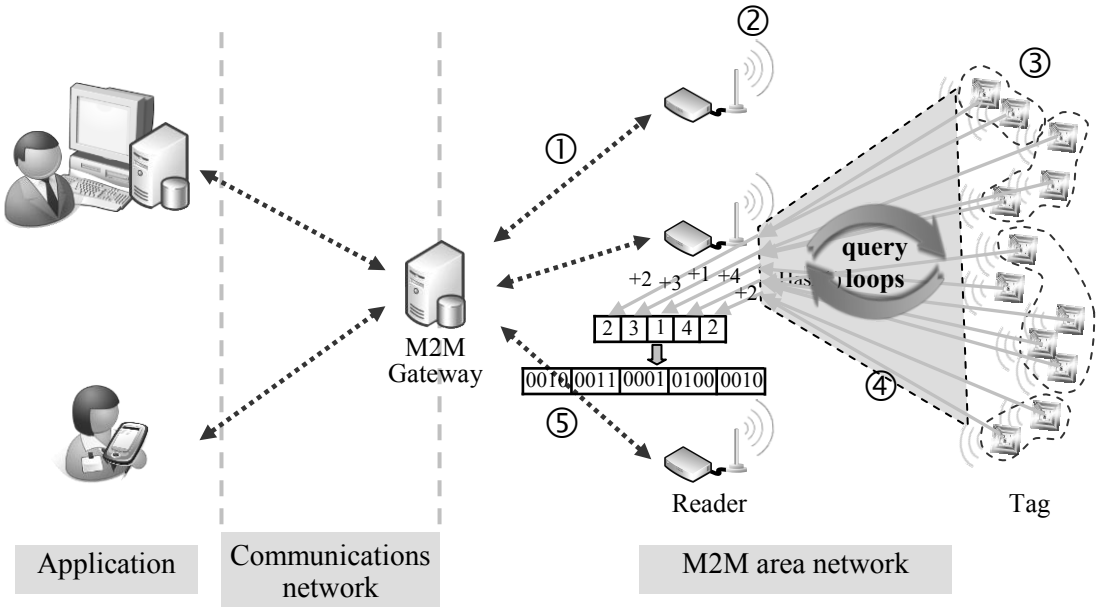

Fig. 7. The M2M architecture of Inventory Monitoring

More details are listed in the appendix. Based on this designing mechanism, any abnormal situation of inventory can be monitored with instant warnings. Configuring enough RFID readers in the retailer, a complete real-time secure mornitoring system can be implemented by the following protocol while combing robust communication network and information system.

5. Conclusions

Applying RFID and M2M technology to develop a proper inventory control has a definite practical value. In this paper, we introduce the inventory record accuracy before and after implementing RFID-enabled adjustments to the inventory monitoring system.We overcome the weakness of TRP and UTRP. We have proposed a continuous monitoring scheme for inventory control based on RFID and M2M technology. The system structure is introduced and some details are discussed. Comparing with TRP and UTRP, the time complexity is listed in the following table. Clearly, our design is much more efficient than UTRP. According to the concepts mentioned above, the improvement of inventory monitoring mechanism achieves anti-loss, accuracy and efficiency, tag privacy, flexible tolerance, theft-prevention, practicality and scalability. Hopefully, it will meet the demands of the future. The inventory can be monitored with instant warnings. The managers can monitor, diagnose, and manage inventory in real time from any location at any time. It will lead to reduced costs and increase of inventory accuracy. The future research in RFID-enabled adjustments to the inventory monitoring includes further warehouse management, production line monitoring, workshop management, and sales monitoring to perform a integration framework of monitoring platform [36]. More RFID applications in various industries will be proposed as technical, privacy, and security issues are resolved. We hope that this paper will be helpful for anyone who is interested in RFID-based monitoring research, including both academic researcher and industry practitioner, and will help to stimulate further interest in this area.

Table 1. The Comparison of time complexity

		TRP	UTRP	Our Scheme
Tag	hash	1	f	1
	xor	1	f	1
	mod	1	f	1
	count	-	f	-
Reader	hash	-	-	1
	xor	-	-	1
	mod	-	-	-
	count	-	-	f
Server	hash	n	n*f	n+1
	xor	n	n*f	n+1
	mod	n	n*f	n
	count	-	n*f	f

References

[1] A. Raman, N. DeHoratius and Z. Ton, "Execution: The missing link in retail operations," *Calif Manage Review*, vol.43, no.3, pp.136-152, 2001.

[2] T. W. Gruen and D. S. Corsten, "A comprehensive guide to retail out of stock reduction in the fast-moving consumer goods industry," *Grocery Manufacturers of America*, 2007.

[3] Y. Kang and S. B. Gershwin, "Information inaccuracy in inventory systems: Stock loss and stockout," *IIE Tranactions*, vol.37, no.9, pp.843–859, 2005. Article (CrossRef Link)

[4] A. G. Kök and K. H Shang, "Replenishment and inspection policies for systems with inventory record inaccuracy," *Manuf Serv Operat Manage*, vol.9, pp.185–205, 2007. Article (CrossRef Link)

[5] Y. Rekik, "An analysis of the impact of RFID technology on inventory systems," in *Proc. of Unique Radio Innovation for The 21st Century*, pp.435-450, 2010.

[6] H. S. Heese, "Inventory record inaccuracy, double marginalization and RFID adoption," *Production and Operations Management*, vol.16, no.5, pp.542–553, 2007. Article (CrossRef Link)

[7] Y. Rekik, E. Sahin and Y. Dallery, "Analysis of the impact of the RFID technology on reducing product misplacement errors at retail stores," *International Journal of Production Economics*, vol.112, no.1, pp.264-278, 2008. Article (CrossRef Link)

[8] Supermarket, "Supermarket shrink survey," *National Supermarket Research Group*, 2001. Article (CrossRef Link)

[9] R. C. Hollinger and J. L.Davis, "National retail security survey," *Department of Sociology and the Center for Studies in Criminology and Law*, Article (CrossRef Link)

[10] R. Hollinger, "2008 National retail security survey: Preliminary results," A Town Hall Meeting with Dr. Richard Hollinger. Article (CrossRef Link)

[11] Wikipedia, "Barcode", http://en.wikipedia.org/wiki/Barcode.

[12] EAN International and the Uniform Code Council, http://www.ean-int.org.

[13] D. C. Wyld and M. C. Budden, "Upping the Ante: using RFID as a competitive weapon to fight shoplifting and improve business intelligence," *The International Journal of Managing Information Technology (IJMIT)*, vol.1, no.1, Nov.2009.

[14] M. C. O'Connor, "Retailers see RFID's potential to fight shrinkage," *RFID Journal*, Aug.2008. Article (CrossRef Link)

[15] R. Wessel, "To future-proof its future store," *RFID Journal*, Sep. 2008. Article (CrossRef Link)

[16] D.C. Wyld, "RFID 101: The next big thing for management," *The Engineering Management Review*, vol.35, no.2, pp.3-19, May.2007. Article (CrossRef Link)

[17] M. Bhattacharya, C.-H. Chu, J. Hayya and T. Mullen, "An exploratory study of RFID adoption in the retail sector," in *Proc. of Oper Manag Res*, vol.3, pp.80–89, 2010. Article (CrossRef Link)

[18] D. Delen, B. C. Hardgrave and R. Sharda, "RFID for better supply chain management through enhanced information visibility," *Production Operations Management*, vol.16, no.5, pp.613–624, 2007. Article (CrossRef Link)
[19] B. C. Hardgrave, J. Aloysius and S. Goyal, "Does RFID improve inventory accuracy? A preliminary analysis," *International Journal of RF Technologies: Research and Applications*, vol.1, no.1, pp.44–56, 2009. Article (CrossRef Link)
[20] B. Hardgrave, S. Goyal and J. A. Aloysius, "RFID-Enabled visibility and retail inventory record inaccuracy: Experiments in the field," *University of Arkansas Working paper*, 2010.
[21] N. DeHoratius and A. Raman, "Inventory record inaccuracy: An empirical analysis," *Management Science*, vol.54, no.4, pp.627–641, 2008. Article (CrossRef Link)
[22] de A. G. Kok, van K. H. Donselaar, and van T. Woensel, "A break-even analysis of RFID technology for inventory sensitive to shrinkage," *International Journal of Production Economics*, vol.112, no.2, pp.521-531, 2008. Article (CrossRef Link)
[23] W.-C. Hsu, "A study of applying mobile wireless communication on the inventory process for the retailing industry-Using the bakery retailing as an example," *Master Thesis*, *Tamkang University*, 2003.
[24] Asiainfo, "The concept of distributed control system", http://www.asia-info.net/detail_mech.asp ?id=919.
[25] C. C. Tan, B. Sheng, and Q. Li, "How to monitor for missing RFID tags," in *Proc. of The 28th International Conference on Distributed Computing Systems*, 2008.
[26] F. Wang, S. Liu and P. Liu, "Complex RFID event processing," *The International Journal on Very Large Data Bases*, vol.18, no.4, pp.913–931, 2009. Article (CrossRef Link)
[27] M.C. O'Connor, "Outdoor clothing and equipment retailer tests RFID-EAS tags," *RFID Journal*, Aug.2008. Article (CrossRef Link)
[28] J. Patton and B. C. Hardgrave, "RFID as electronic article surveillance: Technology performs well in feasibility study," *Information Technology Research Institute*, 2008. Article (CrossRef Link)
[29] C. Swedberg, "Raflatac releases RFID tags with built-in EAS," *RFID Journal*, Dec.2007. Article (CrossRef Link)
[30] G. R. Paul, "An introduction to Radio Frequency Identification (RFID) methods and solutions," *Assembly Automation*, vol.26, no.1, pp.28–33, 2006. Article (CrossRef Link)
[31] Yi Huang, Brian C. Williams and Li Zheng, "Reactive, model-based monitoring in RFID-enabled manufacturing," *Computers in Industry*, In Press.
[32] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *Proc. of Conference on Computer and Communication Security*, pp.210-219, 2004.
[33] Neyre Tekbiyik and Elif Uysal-Biyikoglu, "Energy efficient wireless unicast routing alternatives for Machine-to-Machine networks," *Journal of Network and Computer Applications*, 2011.
[34] Krishnan V and Bhaswar Sanyal, "M2M technology: Challenges and opportunities," *Tech Mahindra*, 2010.
[35] Lantronix, "Enabling business intelligence with M2M: An introduction to device networking solutions," *Lantronix*, 2005.
[36] Shouqin Zhou, Weiqing Ling, and Zhongxiao Peng, "An RFID-based remote monitoring system for enterprise internal production management," *The International Journal of Advanced Manufacturing Technology*, vol.33, no.7-8, pp.837-844, 2007.

Appendix

Algorithm of UTRP method

Step 1. The server defines the frame size f of the digest value and a sequence of random seeds $r_1, r_2, ..., r_f$. The message ($f, r_1, r_2, ..., r_f$) is transmitted to the reader.

Step 2. The reader sets another variable $f' = f$. According to the value f, the reader prepares a empty f -length bit stream. The reader broadcasts the message (f, r_1) to all tags.

Step 3. Based on the message (f, r_1) and the tag's counter ct_i = 0, each tag's serial number sn_i can be determined according to its identification id_i.

$$sn_i = h(id_i \oplus r_1 \oplus ct_i) \bmod f \quad (1)$$

Step 4. The reader sequentially broadcasts the query message $qm - f + f'$, where $qm = 0$ to $f - 1$. For each loop, the following interactions will be executed:

Step 4.1. As any tag's serial number sn_i is equal to the query message $qm - f + f'$, it responds an acknowledgement to the reader.

If no response comes from the tags, this loop is end.

Otherwise, the qm-th bit of the bit stream is set and the variable f' is updated as $f' = f - qm$. Then the reader broadcasts the new seed (f', r_k) to the tags. In this situation, the never responded tags' serial numbers should be re-determined. It increases the work load of each tag, the time complexity of a tag will be O(n) in the worst case.

Step 4.2. The other tags which never responded should increase its own counter ct_i.

$$ct_i = ct_i + 1 \quad (2)$$

According to the tag's identification id_i, counter ct_i and the seed (f', r_k), the tag's serial number sn_i is changed for the next loop.

$$sn_i = h(id_i \oplus r_k \oplus ct_i) \bmod f' \quad (3)$$

Step 5. After the above query loops, the complete bit stream is transmitted to the server for authentication. Another bit stream is generated by the server using the stock records, the parameters (f , r_1 , r_2 , ..., r_f), and the same function. Any variance between those two bit streams means it is inconsistency between the stock and the database records.

Algorithm of Inventory Monitoring based on M2M architecture

Step 1. For querying the sensing information of a certain region, the M2M gateway defines the frame size f of the digest value, a random seed value r needed for hash function, and the bit length $u = \log_2 n$ of counter.

The message (f, r, u) is transmitted to the reader.

Step 2. Upon receiving of the random number r, the reader should generate a query seed x by its secret key Key_R as follows.

$$x = h(r \oplus Key_R) \quad (4)$$

Then the message (f, x) is broadcasted to all tags.

Step 3. Based on the query seed x and the value f, each tag's serial number sn_i can be determined according to its secret key Key_i.

$$sn_i = h(Key_i \oplus x) \bmod f \quad (5)$$

Step 4. The reader sequentially broadcast the query message qm from 0 to $f - 1$. For each loop, the following interactions will be executed:

Step 4.1. As any tag's serial number sn_i is equal to the query message qm, it responds an acknowledgement to the reader.

Step 4.2. All responses are counted by the reader. And the counting value is appended to the bit stream bs.

Step 5. After the above query loops, the complete bit stream is transmitted to the M2M gateway for authentication.

auth ($f, r, u, bs, Key_R, missing\_threshold$) (6)
{
$q \leftarrow h(r \oplus Key_R)$
for all tags' records in the database
{
access Key_i

$sn_i \leftarrow h(Key_i \oplus x) \bmod f$
}
$missing\_value \leftarrow 0$
for $j = 0$ to $f - 1$
{
$sc \leftarrow$ count for those records $sn_i = j$
$rc \leftarrow$ get_the_ j -th_value_from_the_
bitstream $(bs, j*u, (j+1)*u-1)$
$missing\_value \leftarrow missing\_value + (sc - rc)$
}
if ($missing\_value > missing\_threshold$)
return MISSING_ALARM
else
return MISSING_PASS
}

By connecting to the application, the data can be accessed, evaluated, and utilized in real time. It means that managers can monitor, diagnose, and manage inventory from any location at any time.

Yu-Yi Chen is currently an associate professor of the Department of Management Information Systems, National Chung Hsing University, Taiwan. He received the B.S., M.S., and Ph.D. in Applied Mathematics from the National Chung Hsing University in 1991, 1993, and 1998, respectively. His research interests include computer cryptography, network security, and e-commerce.

Jinn-Ke Jan received the B.S. degree in physics from the Catholic Fu Jen University in 1974 and the M.S. degree in information and computer science from University of Tokyo in 1980. He studied Software Engineering and Human-Computer Interface in the University of Maryland, College Park, MD, during 1984-1986. He is presently a professor in the institute of Computer Science at National Chung Hsing University. He is currently also an editor of Information and Education, an editor of Journal of Computers, and an executive member of the Chinese Association for Information Security. He is a member of IACR and member of IEEE. From 1995 to 1997, he was the Director of the Counseling Office for Overseas Chinese and Foreign Students. From 1997 to 2000, he was the Director of the Computer Center at National Chung Hsing University. His research interests include computer cryptography, human factors of designing software and information systems, ideograms I/O processing , data structures and coding theory.

Meng-Lin Tsai received the B.S. degree in International Business from the Providence University in 2007 and the M.S. degree in Computer Science and Engineering from the National Chung Hsing University in 2009. She is currently pursuing her doctoral degree in Computer Science and Engineering at National Chung Hsing University. Her research interests include computer cryptography, network security, and e-commerce.

Chun-Ching Ku received the B.S. degree in Applied Mathematics from the National Chung Hsing University in 1995 and the M.S. degree in Computer Science and Engineering from the National Chung Hsing University in 2010. Her research interests include computer cryptography and network security.

Der-Chen Huang received the BS degree in electronic engineering from Fung- Chia University, Taiwan, in 1983, the MS degree in computer engineering from Florida Institute of Technology, U.S.A, in 1991, and the PhD degree in computer engineering from the Department of Computer Science and Information Engineering, Chung- Cheng University, Chiayi, Taiwan, R.O.C. in 2000. From 1983 to 1989, he worked as a design engineer with the Computer Communication Lab. (CCL)/Industrial Technology Research Institute (ITRI) and Chung-Shan Institute and Science of Technology (CSIST) when he was assigned to a partnership project at General Dynamics, Fort Worth, Texas. U.S.A. He was an associate professor with the Department of Electronic Engineering, National Chinyi Institute of Technology, Taichung, Taiwan, R.O.C. from 1991 to 2004. In 2004, he joined the Department of Computer Science and Engineering, National Chung Hsing University, Taichung, Taiwan, R.O.C.. He was director of Computer and Information Network Center of Chung Hsing University from 2007 to 2011. Currently, he is an associate professor Chung Hsing University. Dr, Huang served as a reviewer for various technical journal and conferences and a member of editorial board of Journal of Internet Technology. Meanwhile, he is also a CFO of Academia-Industry Consortium for Science Parks in Central Taiwan and Secretary-General to the Association of National Chung Hsing University Alumni since 2007. He received the Best Paper Award from the 5th International Conference on Future Information Technology, Korea, in 2010. His research interests include VLSI design for testability and diagnosis, VLSI Digital Signal Process, Communication, Security and Medical Image.