CHEMICAL ENGINEERING TRANSACTIONS
VOL. 46, 2015
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Peiyu Ren, Yancang Li, Huiping Song
Copyright © 2015, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-37-2; **ISSN** 2283-9216
DOI: 10.3303/CET1546227

Research on Authentication Technology of Agriculture Products Traceability System Based on RFID

Bin Wang[a], Jian Zhang[a], Xiaohua Sun[b], Na Wang[c], Yan Zhao*[d], Fushun Wang[d]

[a] College of Information Science and Technology, Agricultural University of Hebei, Baoding, China,
[b] Department of Digital Media, Hebei Software Institute, Baoding, China,
[c] Department Economics and Management, Baoding Vocational and Technical College, Baoding, China,
[d] College of Information Science and Technology, Agricultural University of Hebei, Baoding, China.
wb900@126.com

A secure mutual authentication protocol named DRHSAP (Dynamic Refresh ID and Hash-based the Security authentication protocol) is presented. It can guarantee that the agriculture products in the process of productivity and circulation are not counterfeit. Based on the deficiencies of the low cost RFID (Radio Frequency Identification) system, the DRHSAP protocol has kept the last and present identities of each label on server to effectively solve the synchronization issue between the server and the label, thus further enhances the overall safety of the system. After using BAN logic and several comparative analysis of the authentication protocol, it can prove that the DRHSAP can effectively ensure the security and privacy issues faced by RFID technology and achieve higher security in RFID system.

1. Introduction

The current agriculture products quality security incident sometimes occurs; the agriculture products security problem is day by day serious and is prominent. Modern technologies are being incorporated to cope with the increasing complexity, and such innovations cost substantial amounts of money. Radio frequency identification (RFID) technology is a type of wireless, contactless auto identification technology. Its core is EPC and electronic tag. The techniques have been applied to various products traceability systems. However, the RFID system faces with traditional security threats such as forgery, eavesdropping, replay attacks, tampering with information in tags, and the ability of tracking targets is more likely to cause serious privacy problems which was confirmed (Martin Feldhofer, et al. (2004); Dirk Henrici, et al. (2004); Sarmas. E, et al. (2003); S.K. Kwok, et al. (2010); Chen H Y, et al. (2007); Ha J, et al. (2007)). The current systems based on RFID have security shortcomings which was confirmed (Avoine G, et al. (2005); Thompson, et al. (2006); Kfir, Z, et al. (2005); Sarma, et al. (2003); Chien-Chang Hsu, et al. (2011); Myung, J.H, et al. (2006)). Aiming at this problem, a large number of studies have been launched and a set of assumptions has been put forward about security authentication protocol which was confirmed (Oh, R, et al. (2008); Gu, H, et al. (2009); Chen, S.C, et al. (2008); C. Berbain, et al. (2009)). But there are more weaknesses with these present protocols. The research of efficient, safe and practical security problem of RFID hasn't formed its unified concept and theoretical system so far which was confirmed Oscar Ortiz.et al. (2013); Sen A, et al. (2013); Chaudhry, et al. (2009); BEIER S, et al. (2006)).. In the paper aiming at the demand of privacy protection and practical security, a mutual authentication protocol named DRHSAP is presented based on unilateral hashing function, pseudo-random number generator and dynamic update RFID. By Using BAN logic, the objective and the security of this protocol are proved by formal analysis process.

2. DRHSAP protocol

Aimed to the deficiencies of security authentication protocol, a new authentication protocol named DRHSAP (dynamic refresh ID and hash-based security authentication protocol) is proposed. The RFID information is stored in back server database of the protocol. A Pseudo Random Number Generator is fixed in read-write device. By the pseudo random number generator, the RFID label can deal with the hash function algorithm

Please cite this article as: Wang B., Zhang J., Sun X.H., Wang N., Zhao Y., Wang F.S., 2015, Research on authentication technology of agriculture products traceability system based on rfid, Chemical Engineering Transactions, 46, 1357-1362 DOI:10.3303/CET1546227

and logic operation, and has certain storage capacity. Suppose that there is wired connections between the reader and back-end database, and the communication security can be guaranteed.
The implementation process of the protocol is illustrated on fig.1.Here is the explanation of some symbols of parameters about DRHSAP.
Query: the authentication request from read-write device to the RFID label.
D_r: the 18bit all states pseudo-random sequence produced by read-write device.
D_t: the 12bit all states pseudo-random sequence produced by the RFID label.
SIGNi: the 60 bit binary sequence allocated by severity is unique identifier of each label.
$TSIGN_i$: the hash value of $SIGN_i$, T_i is the pseudonym of a label.
Last $SIGN_i$: a prescribed value of $SIGN_i$ in the previous authentication.
Last $TSIGN_i$: a prescribed value of $TSIGN_i$ in the previous authentication.
Present $SIGN_i$: a prescribed value of $SIGN_i$ in the current authentication.
Present $TSIGN_i$: a prescribed value of $TSIGN_i$ in the current authentication.
hk: an one-way hash function for hash arithmetic with the secret key k and message x.
⊕: a boolean operator for xor operation.
==: to test whether or not the two are equal.
The authentication protocol is described in detail in fig 1.

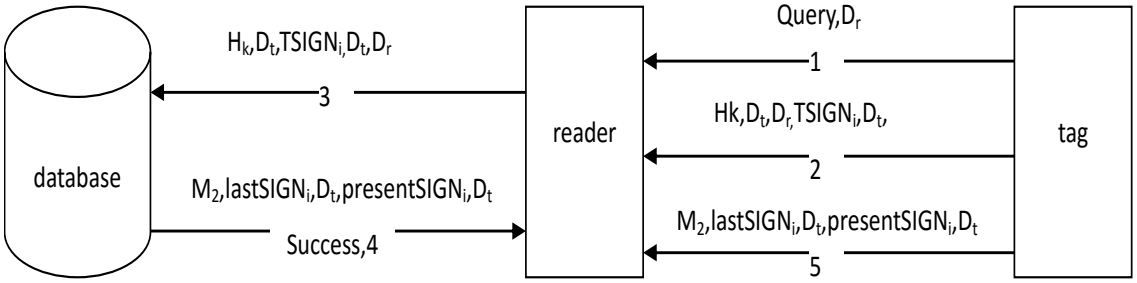

Figure 1: DRHSAP protocol operation procedure

(1) Initial condition
The information of each label is stored to back-end database. The information includes:
$[lastSIGN_i, lastTSIGN_i, presentSIGN_i, presentTSIGN_i]$.
The value of parameters last $SIGN_i$ and last $TSIGN_i$ in the initialization condition is distributed. And present $SIGN_i$ and present $TSIGN_i$ are both of null value. They share a secret key with each legitimacy label. $TSIGN_i = h_k(SIGN_i)$ is stored in label T_i(Tag), and it can be used for a pseudonym of the label.
(2) Authentication process
The reader creates a random number D_r and sends request to T_i for query.
When receiving the query request from reader, Ti generates a binary random number D_t. Then it calculates the $M_1 = h_k(D_t \oplus D_d \oplus TSIGN_i)$ and sends the value of M_1 and Dt to R.
M_1, D_t and D_r are sent to back-end database by R.
last $TSIGN_i$ is selected by database from [last $SIGN_i$,last $TSIGN_i$,present $SIGN_i$, present $TSIGN_i$],and $M' = h_k(D_t \oplus D_d \oplus lastTSIGN_i)$ is calculated.
Then judge whether $M_1 == M'$.
If they are accurately equal, identify and authenticate T_i.If there is no accordant object, select present $TSIGN_i$ from storage space and calculate $M'' = h_k(D_t \oplus D_d \oplus presentTSIGN_i)$. Judge whether $M_1 == M'$ again. If they are accurately equal, identify and authenticate T_i and go to the next step. If the two are not equal, send authentication failure information to R and terminate the sessions.
Calculate the $M_2 = lastSIGN_i \oplus D_t$ or $M_2 = presentSIGN_i \oplus D_t$. Then the success information and relevant information about the label is sent to reader. At the same time, M_2 is sent to Reader by R.
Then last $SIGN_i$ and last $TSIGN_i$ are covered by present $SIGN_i$ and present $TSIGN_i$ which are successfully authenticated.
And $lastSIGN_i \oplus lastTSIGN_i \oplus D_t$ is calculated and present $SIGN_i$ is covered by it. $h_k = presentSIGN_i$ is calculated and present $TSIGN_i$ is covered by it.
Ti is sent to M_2 by the Reader. The logical exclusion or operation is executed with M_2 and D_t, and $SIGN_i$' is obtained. Then judge whether $h_k(SIGN'_i) = TSIGN_i$. If they are equal, the identification has been completed

and $TSIGN_i$ is covered by $h_k(SIGN' \oplus TSIGN \oplus D_t)$. If they are not equal, the identification is failure and the $TSIGN_i$ remains the same value.

3. BAN logical analysis

In order to verify the security of DRHSAP protocol, a formal method is used with the BAN logical analysis about goals, assumptions, and message delivery. BAN logical analysis is given to prove that DRHSAP protocol can achieve the predetermined target from assumption. There are three kinds of treatment object in BAN logical analysis which is called as subject, key and formula. The formula is also known as proposition or statement. The main variable is represented as P and Q. The common theme is represented as A and B. The shared secret variable is represented as S. The temporary value is represented as Na and Nb.
The logical expression of BAN is described as:

$P \mid\equiv X$: P regarded X as a true value.

$P < X$: P has received the message of X.

$P \mid\sim X$: P has sent information about X at some moment.

$P \mid\Rightarrow X$: P has the jurisdiction to X.

$\#(X)$: X is a new object.

$P \overset{s}{\leftrightarrow} Q$: P and Q are sharing a secret about S.

$\{X\}_s$: X is encrypted by the key S.

A total of 19 logic rules are managed by BAN. The rules used here are listed below.
(1) Message meaning rule:

$$\frac{P \mid\equiv P \overset{s}{\leftrightarrow} Q, P < \{X\}_s}{P \mid\equiv Q \mid\sim X}$$

(2) Random number verification rule:

$$\frac{P \mid\equiv \# X, P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

(3) Jurisdiction rule:

$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

(4) Message fresh rule:

$$\frac{P \mid\equiv \# X}{P \mid\equiv \#(X, Y)}$$

In the basic model, the label is regarded as subject A, the reader and backend server are regarded as B. In the DRHSAP protocol, the unique identifier of each label is $SIGN_i$. Therefore, in the DRHSAP authentication system, $TSIGN_i$ is regarded as an Identity authentication of subject A and similarly, $SIGN_i$ is regarded as an Identity authentication of subject B.
When executing formally BAN, the process of key generation and identity authentication are omitted. Only the logical part directly related to the security problems are conserved. The definite formalization of the protocol is:
Message1:

$A \rightarrow B: N_a, N_b, \{N_a, N_b, TSIGN_i\}_k$.

Message2:

$B \to A: \{N_a, SIGN_i\}_k$.

The security goals are:
(1) $B \mid\equiv TSIGN_i$
(2) $A \mid\equiv SIGN_i$
The initial hypotheses are:

$P1: B \mid\equiv A \overset{k}{\leftrightarrow} B$

$P2: A \mid\equiv A \overset{k}{\leftrightarrow} B$

$P3: B \mid\equiv \#(N_b)$

$P4: A \mid\equiv \#(N_a)$

$P5: B \mid\equiv A \mid\Rightarrow TSIGN_i$

$P6: A \mid\equiv B \mid\Rightarrow SIGN_i$

The pragmatic logical reasoning of BAN about DRHSAP protocol is:
When $B < N_a, N_b, \{N_a, N_b, TSIGN_i\}_k$ are met, according to the initial hypothesis P_1 and message meaning rule, It is deduced that $\frac{P \mid\equiv P \overset{s}{\leftrightarrow} Q, P < \{X\}_s}{P \mid\equiv Q \mid\sim X}$. From this, $B \mid\equiv A \mid\sim TSIGN_i$.
According to the initial hypothesis P_3, with $B \mid\equiv \#(N_b)$ and the message fresh rule $\frac{P \mid\equiv \# X}{P \mid\equiv \#(X, Y)}$. It is deduced that $B \mid\equiv \#(TSIGN_i)$.
According to the random number verification rule $\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$. It is deduced that $B \mid\equiv A \mid\equiv \#(TSIGN_i)$.
According to the Initial hypothesis $B \mid\equiv A \mid\Rightarrow TSIGN_i$ and jurisdiction rule $\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$, It is deduced that $B \mid\equiv TSIGN_i$. In the same sense, when $A < \{N_a, SIGN_i\}_k$ It is deduced that $A \mid\equiv TSIGN_i$.
Through the content above about the DRHSAP based on BAN, the security goals can be deduced.
The results show that the present DRHSAP protocol is reliable. It can effectively realize the target of two-way legal identity security authentication.
The traceability system based on RFID will receive security threat in many ways, including spoofing, replay attacks, tracking attack, tampering with data and repudiation, QOS and blocking attack, system attack and virus. The method presents by this paper is contrasted with the common protocols about countering the security threats above. As shown in table 1.

Table 1: Security agreement

	hash	hash-chain	reverse--chain	random--chain	DRHSAP
spoofing	√	√	√	√	√
replay	√	√	√	√	√
tracking	√	√	√	×	√
blocking\qos	×	×	×	-	√
system\ virus	×	×	×	×	√
tampering\	×	√	√	√	√

Therefore, the proposed DRHSAP is well suitable for security communication of the low cost traceability system of agriculture products.

4. Conclusions

It is very import to establish farm product traceability system for ensuring safety of farm product. As the popularization of Internet of thing and RFID technologies, through RFID technology combined with the existing information security technologies, realization of supply chain security and traceability of goods, low cost, and high-tech features, that can ensure the safety of goods in circulation. It is concluded that the application of RFID technology to agricultural products is quite critical to the foodstuff safety of our country, and will plays important role in the agricultural development and 21st century society stability.

Acknowledgments

This work is supported by rural informatization engineering technology research center of Hebei province, 2014 annual plan for scientific research and development of Baoding support project (Grant No.14ZS004) and 2015 annual plan for scientific research and development of Baoding support project (Project: Agricultural products traceability management system based on IOT) and 2013 annual Science and Engineering Foundation of Hebei Agricultural University, China. (Grant No. LG201308).

References

Avoine G., Oechslin P., 2005, A Scalable and Provably Secure Hash Based RFID Protocol. In: Proceeding of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005) [C]. Washington DC, USA. pp. 125-140, DOI: 0.1109/PERCOMW.2005.12.

Berbain C., Billet O., Etrog J., Gilbert H., 2009, in An Efficient Forward Private RFID Protocol [J]. CCS'09: Proceedings of the 16th ACM conference on Computer and Communications Security. ACM, New York, NY. Vol. 7. pp. 43-53. DOI: 10.1145/1653662.1653669.

Chen H.Y., 2007, SASI: A new ultra light weight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Transactions on Dependable and Secure Computing, vol. 4 PP. 337 2340.

Chen S.C, & Chen C.H., 2008, Developing an applied RFID program and curriculum of aquatic products logistics and supply chain [J]. In Proceedings of IEEE international conference on service operations and logistics, and informatics. Vol. 4: 2433-2438.

Hsu C.C., Yuan P.C., 2011, The design and implementation of an intelligent deployment system for RFID readers [J] Expert Systems with Applications. C. -C. Hsu. vol. 4. pp. 122-134.

Henrici D., Muller P., 2004, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifier. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops PERCOMW. vol. 10 pp. 28-34. DOI: 10.1109/PERCOMW.2004.1276922

Gu H., & Wang D., 2009, A content-aware fridge based on RFID in smart home for home-healthcare [J]. In Proceedings of 11th international conference on advanced communication technology. Vol. 4 pp. 987-990.

Ha J., Kim H., Park J., et al., 2007, HGLAP-hierarchical group-index based light weight authentication protocol for distributed RFID system [C] RFID International Conference Embedded and Ubiquitous Computing. TAIWAN: Taipei, pp. 557-567.

Kfir Z. and Wool A., 2005, Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems.in 1st International Conference on Security and Privacy for Emerging Aeas in Communication Networks. pp. 33-35.

Feldhofer M., 2004, A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags. IEEE Proceedings of MELECON, vol. 2, pp. 759-762.

Myung J.H, & Lee W.J., 2006, Adaptive splitting protocols for RFID tag collision arbitration [J]. In Proceedings of the 7th ACM international symposium on mobile ad-hoc networking and computing. pp. 202-213.

Oh R, & Park J., 2008, A development of active monitoring system for intelligent [J]. In Proceedings of international conference on advanced language processing and web information technology. vol. 5: pp. 358-361.

Sarma S.E., Weis S.A., and Engels D.W., 2003, RFID Systems and Security and Privacy Implications.in Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523.Springer-Verlag Berlin. pp. 45-50. DOI: 10.1007/3-540-36400-5_33.

Sarmas. E, Weis S.A., Engels D.W., 2003, RFID Systems And Security And Privacy Implications. In: Proceedings Of The 4th International Workshop On Cryptographic Hard-ware And Embedded Systems. Springer-Verlag Berlin, pp. 454-469, DOI: 10.1007/3-540-36400-5_33.

Kwok S.K., Ting J.S.L., et al. 2010, Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication [J]. Computers in Industry, vol. 61: PP: 624-635.

Thompson D.R, Chaudhry N., and Thompson C.W., 2006, RFID security threat model, in Conference on Applied Research in Information Technology. Conway, Arkansas. pp. 100-102

Ortiz O., 2006, E volution of agricultural extension and information dissemination in Peru: An historical perspective focusing on potato-related pest control [J]. Agriculture and Human Values, 23: 477-489.

Sen A., Chander M., 2013, Privatization of veterinary services in developing countries: a review [J]. Tropical Animal Health and Production, 35: 223-236.

Chaudhry, 2009, A Simple Multi-sensor Data Fusion Algorithm Based on Principal Component Analysis [J]. International Colloquium on Computing, Communication, Control, and Management Proceedings. 91-94.

Uan Rijswijk W., Frewer L.J., Menozzi D., et al., 2008, Consumer Perceptions of Traceability: A Cross-national Comparison of the Associated Benefits. Food Quality and Preference, 19: 88-91.

Beier S., Grandison T., Kailing K., et al., 2006, Discovery services renabling RFID traceability in EPC global networks [C]. Intemational Conference on Management of Data. Delhijndia: Indian Institute of Technology (IIT), 14-16.