An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection

Haowen Tan[1], Dongmin Choi[1], Pankoo Kim[1], Sungbum Pan[2], Ilyong Chung[1]

[1] Department of Computer Engineering, Chosun University, South Korea
[2] Department of Electronic Engineering, Chosun University, South Korea
tan_halloween@foxmail.com, {jdmcc, pkkim, sbpan, iyc}@chosun.ac.kr

Abstract

Radio Frequency Identification (RFID) is a promising technology which can be applied in many areas, including supply chains logistics and medical treatment. Due to practical requirements of verifying multiple objects simultaneously, the authentication towards large numbers of RFID tags or tag groups remains a hot topic. However, because of the resource limitation of low-cost RFID tags, only basic cryptographic encryptions can be applied on the tag sides. As a result, security and privacy risks towards the RFID system remain crucial issues to be solved. Additionally, in some complex scenarios such as factory or harbor, some tags may be missing or temporarily disabled due to environmental interference. In this paper, an efficient hash-based RFID grouping authentication protocol providing missing tags detection is proposed. In our assumption, each reader of the authentication system can verify large amounts of RFID tags within its ranges. Note that it is not necessary for the reader to predefine the tags into groups during large-scale authentication. Instead, the RFID system can automatically divide the tags into different groups according to the given slots and bitmap. Moreover, the proposed protocol can detect and reset the missing tags so that the missing tag can rejoin the system. Security analysis shows that this protocol can offer sufficient security assurances and resist various attacks. Subsequently, the performance analysis illustrates that the proposed protocol yields better performance than the state-of-the-art RFID grouping authentication protocols.

Keywords: RFID, Grouping authentication, Security, Missing tags

1 Introduction

Unlike barcodes, it is not necessary for RFID tag to conduct line-of-sight contact during the authentication. A basic RFID system is composed of three essential entities: backend process system, reader and RFID tag [1-3]. The reader is capable of communicating with multiple tags simultaneously so as to acquire relevant information from the tags. The BPS performs as the verifier with responsibility to determine authenticity of the proof acquired from the reader [4-5].

The group authentication towards multiple RFID tags or tag groups has become hot research topic due to requirement of real applications [7-9]. In specific scenarios with large numbers of tags and readers such as the production department of the factory [10], each reader should verify large amounts of RFID tags within its range [11]. Many research achievements have been made with the assumption that the tags are previously organized into certain groups with predefined reading sequence [7, 12-13]. However, in real applications, the authentication processes cannot be fixed. The reader may need to verify random and undetermined tags of the range whenever necessary.

Missing tag is another important factor that affects the regular operation of the entire RFID system [14-17]. In some complex scenarios such as factory or harbor, some tags may be missing or temporarily disabled due to environmental interference. In fact, these missing tags are revoked and cannot rejoin the RFID system due to desynchronization with the system [18].

On the other hand, due to practical requirements for large-scale implementation including big markets and harbors [2, 6, 18-19], the authentication on large numbers of RFID tags need to be accelerated. Moreover, due to the resource limitation of RFID tag, the adopted techniques should be lightweight and more efficient. Instead of authenticating all the tags one by one, parallel authentication provides a more practical way for real scenarios [10, 20-21].

With the above consideration, we propose an efficient hash-based RFID grouping authentication protocol providing missing tags detection. In our assumption, the RFID system can divide the tags into different groups according to the given slots and bitmap. Hence the reader could verify all the activated tag groups one after another, which is suitable for occasions with large amounts of tags to be verified. Moreover, the proposed protocol can detect and reset the missing tags. The security analysis and performance

*Corresponding Author: Ilyong Chung; E-mail: iyc@chosun.ac.kr
DOI: 10.3966/160792642018031902016

analysis prove that the proposed protocol could provide adequate security properties and efficiency.

2 Related Works

Several RFID authentication protocols for multiple tags have been proposed to provide enough security protection and resistance to various attacks [7-10]. In order to compensate for the weakness of yoking protocol presented by Juels [2], the original grouping proof using time stamp [7] is proposed by J. Saito and K. Sakurai, which is relatively the earliest proposed grouping authentication protocols on multiple RFID tags. In the protocols, the reader derives the time stamps from database and forwards it to all the RFID tags within its communication range. The tags is classified into two varieties: pallet tag and ordinary product tags. However, this protocol cannot provide the RFID system with resistance to replay attack [3, 22-23].

The chaining proof [10] protocol is proposed in 2007. The key point of this protocol is to associate all the intended tags together and build a chain to provide integrity preservation. Reading-order independent grouping protocol [8] is presented in 2008. In this protocol, the pallet tag and the reader are combined together and perform as a single entity. In 2013, H. Liu proposed grouping proofs based authentication protocol for distributed RFID systems [9, 11, 24]. The tags are classified into groups and are verified sequentially. The RFID system also needs to previously arrange all the tags to be verified [5, 25-26].

3 System Model

In this section, we describe the system model and the missing tag detection problem. We assume the occasion containing large amounts of RFID tags to be verified. Each reader in the system need to verify all the RFID tags as required [11, 27-28]. We would like to emphasize that the RFID system will not predefine the reading process for certain tag groups. Instead, all the tags appear randomly on the authentication range of each reader. At the same time, due to the environmental interference, some RFID tags may lose contact with the RFID system and are missing for some sessions. In this case, it is necessary for the missing tags to rejoin the system.

The whole structure of the RFID system applied in our protocol is introduced in Figure 1. The communication between the BPS and the reader is through wired connection and is considered to be secure. Each reader is responsible for all tags in its effective areas. Note that some tags may be in the overlapping range. Additionally, there are some missing tags existing randomly in the entire area. These missing tags are revoked and cannot rejoin the RFID system due to desynchronization with the system [2, 12, 29]. As illustrated above, secure and efficient RFID grouping authentication protocol is required with the purpose of making these missing tags useful, which is a good way to reduce the cost for system maintenance.

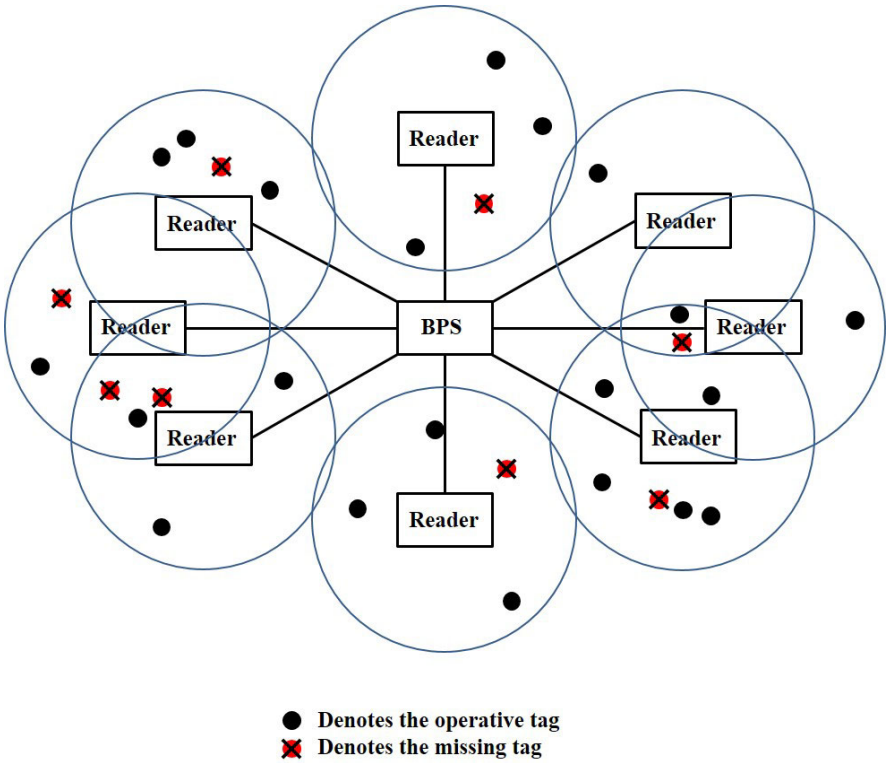


Figure 1. Structure of RFID system

4 Proposed Authentication Protocol

In this section, we describe the proposed protocol. The protocol can be divided into three parts including initialization, authentication scheme, key update and reset. The detailed description is given below. The notations are presented in Table 1.

Table 1. Notations

Symbol	Description
BPS	Back Processing System
ID_{Rm}	Identifier of Reader R_m
ID_{Ti}	Identifier of Tag T_i
S_{Ti}	Secret Key of Tag T_i
$H()$	Hash Function
$N_{T_i}^0$	Initial Value of N_{Ti}
r, r_{Rm}	Random Numbers

4.1 Initialization

In this phase, the BPS will generate a bitmap including f slots ($bitmap = \{slot_i \mid i = 1, 2, 3, \ldots, f\text{-}1\}$). All these slots perform as temporary tag identity and will be broadcasted to all the tags and readers. Note that the value of f and length of each slot can be decided according to real requirement. The brief description of the applied bitmap and slots is shown in Figure 2.

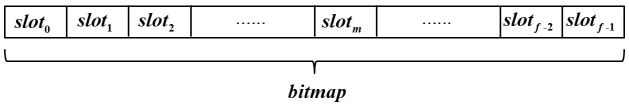


Figure 2. The applied bitmap and slots

4.2 Authentication Scheme

In this subsection, main authentication scheme is introduced. Brief description is shown in Figure 3. Detailed steps are as follows:

- The BPS generates r and broadcasts (r, f, $bitmap$) to all the devices within its range.
- Reader R_m computes $m=f$ *random(), and chooses $slot_m$ from the received bitmap. At the same time, it generates r_{Rm}.
- At the tag side, tag T_i computes $x=H(ID_{Ti}, r) \bmod f$. Each tag will select $slot_x$ as their own group identifier.
- Reader R_m sends (1, $slot_m$, ID_{Rm}, r_{Rm}) to all the tags in his range. Only the relevant tags with $slot_m$ will compute $G_{Ti}=ID_{Ti} \oplus ID_{Rm} \oplus r_{Rm}$ and $Q_{Ti}=H(S_{Ti}, r) \vee G_{Ti}$. (2, $slot_m$, G_{Ti}, Q_{Ti}, N_{Ti}) will then be sent back to reader R_m. Other tags will be activated only when reader choose their *slots* in the next.
- Reader R_m derives $ID_{Ti}=G_{Ti} \oplus ID_{Rm} \oplus r_{Rm}$ and stores ($slot_m$, ID_{Ti}, G_{Ti}, Q_{Ti}, N_{Ti}). BPS then sends $(ID_{T_i}, S_{T_i}, N_{T_i}^0)$ to reader R_m.
- Reader R_m checks Q_{Ti} and computes $W_{Ti}=H(S_{Ti}, N_{Ti})$. Then R_m checks if $N_{T_i}^0=N_{T_i}$ establishes. Reader R_m sends different requests to both the BPS and tag T_i according to different results.

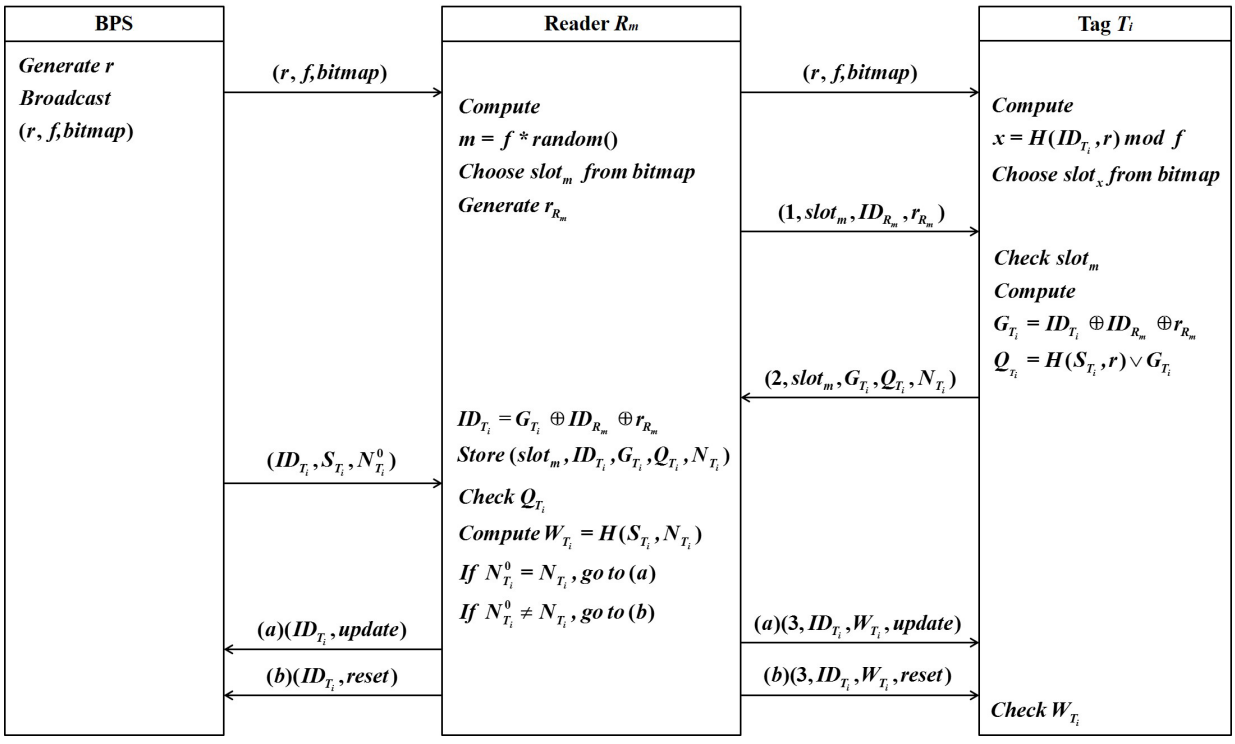


Figure 3. Authentication scheme

4.3 Key Update and Reset

In this phase, the secret key of the tags will be updated or reset according to different situations:

$(a)update:$

$Compute\ N_{T_i} = N_{T_i} + 1$

$S_{T_i} = H(S_{T_i}, N_{T_i})$

$(b)reset:$

$Compute\ N_{T_i} = N_{T_i}^0$

$S_{T_i} = H(S_{T_i}^0, N_{T_i}^0)$

5 Security Analysis

In this section, we analyze the proposed protocol briefly. It is proved that our proposed protocol can provide resistance to replay attack, and all the tags are independently verified. Additionally, mutual authentication and missing tag detection are also provided, which improves the security level of the proposed grouping authentication protocol [4, 30-32].

5.1 Resistance to Replay Attack

In the proposed protocol, pseudo random numbers are applied. The slots are randomly selected by readers and tags [33]. Moreover, secret key of the tag is updated after every successful session. In this way, it is difficult for the active adversary to conduct replay attack by reusing the previous acquired messages.

5.2 Reading Independence

In this protocol, the authentication towards every tag is irrelevant. It is not necessary for the RFID system to predefine the reading sequence and tag groups for tags to be authenticated [5, 34]. Each reader is capable of identifying random tags at any time, which is practical for real applications.

5.3 Mutual Authentication

As illustrated in the system model, the communication between readers and tags are through insecure wireless channel [7, 19, 35-37]. In our proposed protocol, the reader and tag authenticate the received message every time in order to guarantee the received message comes from legitimate entity. In this way, the mutual authentication can be provided.

5.4 Missing Tag Detection

The proposed protocol can provide missing tag detection, which is efficient for RFID system. Assuming tag T_y is disconnected from the system at time T due to environmental interference. At time $T+\triangle t$, T_y receives (1, $slot_m$, ID_{Rm}, r_{Rm}) and want to rejoin the system. Reader R_m checks value of N_{Ti} and sends reset request to both tag and reader. After reset, T_y can join the system in next session.

6 Performance Analysis

In this section, we present the performance analysis towards the proposed protocol. The corresponding simulation experiments are presented in order to prove the efficiency of the proposed protocol. Note that the authentication time is the most concerned factor, which is of great importance in RFID authentication scenarios with large number of RFID tags [38-40].

The experiments are conducted on Windows 10 with a 2.70 GHz Intel(R) Core i7-6820HK CPU and 16GB memory. The time consumption on BPS, reader, and tags are considered respectively. Note that the time consumption on BPS is considered as the total time for the entire authentication of all the participating RFID tags. The experiments are performed in Visual Studio 2015 with C++ language on socket. Moreover, the related figures are drawn in MATLAB R2014a.

It is worth emphasizing that we compare our protocol with two state-of-the-art authentication protocols employing lightweight cryptographic techniques, namely the LGAP [12] protocol and GUPA [9] protocol. The simulation of LGAP and GUPA are conducted for several times so as to compare with the proposed protocol. The comparison results and brief description on different devices are respectively presented as follows.

First, the comparison of authentication time on RFID tag is presented as shown in Figure 4. As we can see from the figure, the key size is taken into consideration. The experiments are conducted respectively under the condition that the key size is 64, 128, 256, 512 bits. It is obvious that the authentication time for each RFID tag increases dramatically as illustrated in Figure 4. The proposed protocol requires less time than LGAP. Additionally, the experiment on different requesting tags are also conducted. However, the time consumption on single RFID tag is not strictly relevant with the number of tag groups.

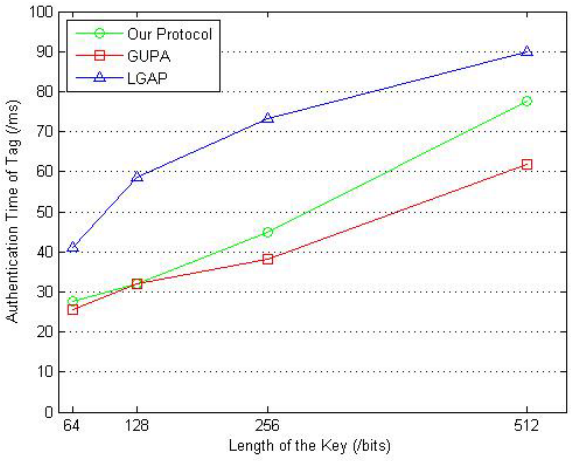


Figure 4. Comparison of authentication time on tag

Subsequently, the comparison of running time on reader side with LGAP and GUPA is displayed in Figure 5. Apparently, as the number of participating RFID tags increases, the running times on LGAP and GUPA both increases fast, which results from the certain reading order for all the tags. However, the communication between reader and tags is through parallel communication, which matches the presented simulation result. Note that we set the key size to be 512bits.

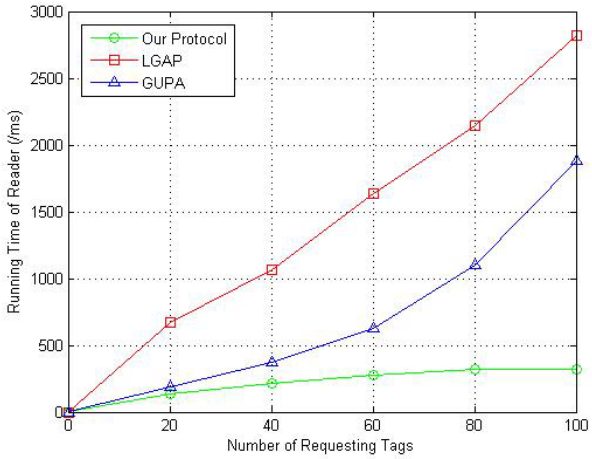


Figure 5. Comparison of running time on reader

Next, we focus on the effect of different key size under the assumption that the number of requesting tags is 100. In this way, the processing time for each tag increases with larger key size. Hence, the authentication time on reader side is effected accordingly. The result is given in Figure 6. Our protocol yields better performance than the LGAP and GUPA.

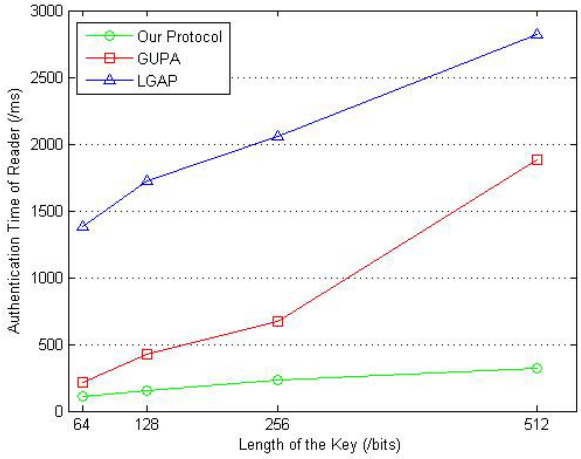


Figure 6. Comparison of authentication time on reader with different key size

At last, the operating time for the BPS to manage the authentication of all the tags is given in Figure 7. It is worth noting that we consider the BPS running time to be the system authentication time since all the identification starts and ends on the BPS side. Similarly, the key size is set to be 512bits. From Figure 7, we can see the number of participating RFID tags has a significant effect on the efficiency of the entire authentication process. Hence the authentication on large numbers of RFID tags remains the hotspot in practical scenarios.

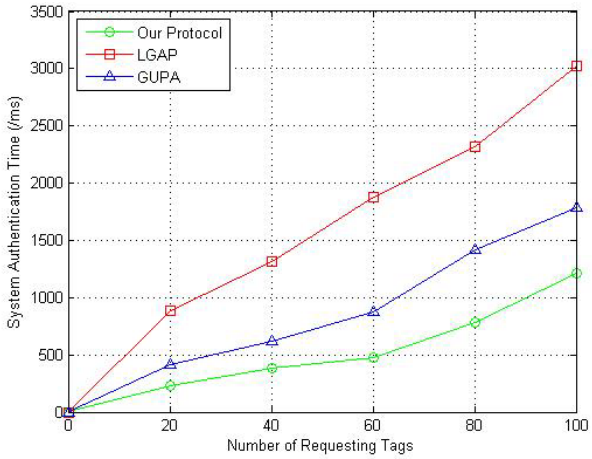


Figure 7. Comparison of system authentication time

Additionally, the effect of the key size on authentication efficiency is taken into consideration under the assumption that the number of the participating RFID tags is 100. In this occasion, the experiment result is given in Figure 8. We can see in our protocol the BPS requires less time for tag authentication.

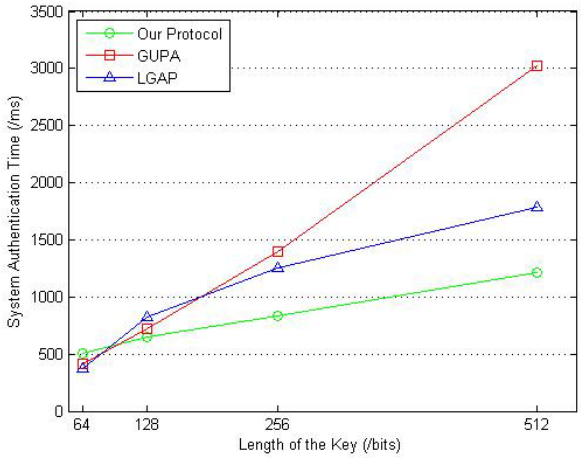


Figure 8. Comparison of system authentication time with different key size

In conclusion, the key size and number of RFID tags are the two main factors which affect the entire group authentication process. For this consideration, the simulation results prove that the proposed protocol has better performance than the state-of-the-art RFID authentication protocol.

7 Conclusion

In this paper, we propose an efficient hash-based RFID grouping authentication protocol providing missing tags detection. Each reader of the authentication system can verify large amounts of RFID tags within its ranges. The RFID system can automatically divide the tags into different groups according to the given slots and bitmap. In addition, the proposed protocol can detect and reset the missing tags. Security analysis shows that this protocol can resist various attacks. The performance analysis is given in the next, where the comparison with two state-of-the-art RFID group authentication protocols on authentication time is presented. Note that we mainly considerate the key size and number of tags as two variables affecting the RFID authentication system. According to the experiment results, the proposed protocol could provide better performance. Hence the proposed protocol achieves both the security and performance properties.

Acknowledgements

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-0-00390) supervised by the IITP, and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017-R1D1A3B03034005).

References

[1] A. Juels, RFID Security and Privacy: A Research Survey, *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 381-394, February, 2006.

[2] A. Juels, Yoking-Proofs for RFID Tags, *Proc. of Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, Orlando, FL, 2004, pp. 138-143.

[3] S. Piramuthu, On Existence Proofs for Multiple RFID Tags, *Proc. of IEEE International Conference on Pervasive Services*, Lyon, France, 2006, pp. 317-320.

[4] H. Y. Chien, S. B. Liu, Tree-Based RFID Yoking Proof, *Proc. of 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, China, 2009, pp. 550-553.

[5] L. Bolotnyy, G. Robins, Generalized Yoking-Proofs for A Group of RFID Tags, *Proc. of 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, San Jose, CA, 2006, pp. 1-4.

[6] D. Sun, J. Zhong, A Hash-Based RFID Security Protocol for Strong Privacy Protection, *IEEE Transactions on Consumer Electronics*, Vol. 58, No. 4, pp. 1246-1252, November, 2012.

[7] J. Saito, K. Sakurai, Grouping Proof for RFID Tags, *Proc. of 19th International Conference on Advanced Information Networking and Applications*, Taipei, Taiwan, 2005, pp. 621-624.

[8] Y. Lien, X. Leng, K. Mayes, J. Chiu, Reading Order Independent Grouping Proof for RFID Tags, *Proc. of IEEE International Conference on Intelligence and Security Informatics*, Taipei, Taiwan, 2008, pp. 128-136.

[9] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, L. Yang, Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, No. 7, pp. 1321-1330, July, 2013.

[10] C. Lin, Y. Lai, J. D. Tygar, C. Yang, C. Chiang, Coexistence Proof Using Chain of Timestamps for Multiple RFID Tags, *Proc. of Advances in Web and Network Technologies, and Information Management*, Huang Shan, China, 2007, pp. 634-643.

[11] J. Shen, H. Tan, Y. Wang, S. Ji, J. Wang, An Enhanced Grouping Proof for Multiple RFID Readers & Tag Groups, *International Journal of Control and Automation*, Vol. 7, No. 12, pp. 239-246, December, 2014.

[12] J. Shen, H. Tan, S. Chang, Y. Ren, Q. Liu, A Lightweight and Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangements, *Proc. of 17th IEEE International Conference on Advanced Communication Technology*, Seoul, South Korea, 2015, pp. 681-686.

[13] M. Chen, S. Chen, An Efficient Anonymous Authentication Protocol for RFID Systems Using Dynamic Tokens, *Proc. of IEEE 35th International Conference on Distributed Computing Systems (ICDCS)*, Columbus, OH, 2015, pp. 756-757.

[14] Y. J. Huang, W. C. Lin, H. L. Li, Efficient Implementation of RFID Mutual Authentication Protocol, *IEEE Transactions on Industrial Electronics*, Vol. 59, No. 12, pp. 4784-4791, December, 2012.

[15] W. Yue, C. Wu, Z. Chen, Cooperative Spectrum Sensing Based on Side Information for Cognitive Radio Sensor Networks in Internet of Thing Applications, *International Journal of Internet Protocol Technology*, Vol. 9, No. 2, pp. 121-128, January, 2016.

[16] X. Liu, B. Xiao, S. Zhang, K. Bu, Unknown Tag Identification in Large RFID Systems: An Efficient and Complete Solution, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 6, pp. 1775-1788, June, 2015.

[17] L. Ruan, M. P. I. Dias, E. Wong, SmartBAN with Periodic Monitoring Traffic: A Performance Study on Low-Delay and High Energy-Efficiency, *IEEE Journal of Biomedical and Health Informatics*, Vol. PP, No. 99, pp. 1-1, December, 2016.

[18] P. Gope, T. Hwang, A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks, *IEEE Transactions on Industrial Electronics*, Vol. 63, No. 11, pp. 7124-7132, November, 2016.

[19] R. Acierno, M. Maffia, L. Mainetti, L. Patrono, E. Urso, A Multidisciplinary Approach to Investigate Potential Exposure

Risks on Drugs of RFID Systems, *Proc. of 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, Rome, Italy, 2010, pp. 1-5.

[20] B. Vaidya, D. Makrakis, H. T. Mouftah, Authentication Mechanism for Mobile RFID Based Smart Grid Network, *Proc. of 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Toronto, Canada, 2014, pp. 1-6.

[21] J. Qiao, W. Wang, Y. Zhang, S. Niu, Code Division Cooperative Identification Reader Anti-Collision Protocol in Smart RFID Systems, *Proc. of 2012 19th International Conference on Telecommunications (ICT)*, Jounieh, Lebanon, 2012, pp. 1-6.

[22] A. Almaaitah, H. S. Hassanein, M. Ibnkahla, Tag Modulation Silencing: Design and Application in RFID Anti-Collision Protocols, *IEEE Transactions on Communications*, Vol. 62, No. 11, pp. 4068-4079, November, 2014.

[23] T. Zhang, Y. Yin, D. Yue, Q. Ma, G. Yu, A Simulation Platform for RFID Application Deployment Supporting Multiple Scenarios, *Proc. of 2012 Eighth International Conference on Computational Intelligence and Security*, Guangzhou, China, 2012, pp. 563-567.

[24] N. Lo, S. Ruan, T. Wu, Ownership Transfer Protocol for RFID Objects Using Lightweight Computing Operators, *Proc. of 2011 International Conference for Internet Technology and Secured Transactions*, Abu Dhabi, United Arab Emirates, 2011, pp. 484-489.

[25] E. Karbab, D. Djenouri, S. Boulkaboul, A. Bagula, Car Park Management with Networked Wireless Sensors and Active RFID, *Proc. of 2015 IEEE International Conference on Electro/Information Technology (EIT)*, Dekalb, IL, 2015, pp. 373-378.

[26] F. Ouakasse, S. Rakrak, From RFID Tag ID to IPv6 Address Mapping Mechanism, *Proc. of 2015 Third International Workshop on RFID And Adaptive Wireless Sensor Networks (RAWSN2015)*, Agadir, Morocco, 2015, pp. 63-67.

[27] S. Pudasaini, K. S. Kwak, S. Shin, On Maximising Tag Reading Efficiency of A Multi-Packet Reception Capable Radio Frequency Identification Reader, *IET Communications*, Vol. 9, No. 5, pp. 701-706, March, 2015.

[28] D. B. Arbia, M. M. Alam, R. Attia, E. B. Hamida, Behavior of Wireless Body-To-Body Networks Routing Strategies for Public Protection and Disaster Relief, *Proc. of 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Abu Dhabi, United Arab Emirates, 2015, pp. 117-124.

[29] A. M. Ortiz, T. Olivares, F. Royo, N. Crespi, L. Orozco-Barbosa, Smart Cross-Layer Protocol Integration for Efficient Wireless Communications, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 20, No. 3, pp. 148-158, November, 2015.

[30] C. Zhu, H. Nicanfar, V. C. M. Leung, L. T. Yang, An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 1, pp. 118-131, January, 2015.

[31] J. Shen, H. Tan, J. Wang, J. Wang, S. Lee, A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks, *Journal of Internet Technology*, Vol. 16, No. 1, pp. 171-178, January, 2015.

[32] R. Colella, L. Catarinucci, L. Tarricone, Improved Battery-Less Augmented RFID Tag: Application on Ambient Sensing and Control, *IEEE Sensors Journal*, Vol. 16, No. 10, pp. 3484-3485, March, 2016.

[33] R. Bhattacharyya, C. Floerkemeier, S. Sarma, Low-Cost, Ubiquitous RFID-Tag-Antenna-Based Sensing, *Proceedings of the IEEE*, Vol. 98, No. 9, pp. 1593-1600, September, 2010.

[34] C. Qian, H. Ngan, Y. Liu, L. M. Ni, Cardinality Estimation for Large-Scale RFID Systems, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 9, pp. 1441-1454, September, 2011.

[35] H. Xiong, Z. Qin, Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 7, pp. 1442-1455, July, 2015.

[36] M. Kathuria, S. Gambhir, Reliable Delay Sensitive Loss Recovery Protocol for Critical Health Data Transmission System, *Proc. of 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, Noida, India, 2015, pp. 333-339.

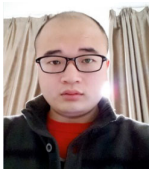
[37] J. Shen, H. Tan, S. Moh, I. Chung, J. Wang, An Efficient RFID Authentication Protocol Providing Strong Privacy and Security, *Journal of Internet Technology*, Vol. 17, No. 3, pp. 443-455, May, 2016.

[38] M. T. I. Huque, K. S. Munasinghe, A. Jamalipour, A Probabilistic Energy-Aware Routing Protocol for Wireless Body Area Networks, *Proc. of 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, Vancouver, Canada, 2014, pp. 1-5.

[39] L. Wei, C. Yang, R. Chen, RFID-Based Stent-Graft Dynamic Assessment for Health Cares, *IET Networks*, Vol. 6, No. 1, pp. 1-4, January, 2017.

[40] E. Sarra, T. Ezzedine, Performance Improvement of the Wireless Body Area Network (WBAN) Under Interferences, *Proc. of 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, 2016, pp. 1-6.

Biographies

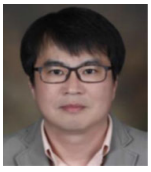


Haowen Tan received the B.E. degree and the M.E. degrees in computer science from Nanjing University of Information Science and Technology, Nanjing, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in Department of Computer Engineering, Chosun University, Gwangju, Korea. His research interests include information security, wireless body area

networks, radio frequency identification, and vehicular ad-hoc networks.

Dongmin Choi received his B.E. degree from the Kyunghee University in 2003 and M.S. and Ph.D. degrees in computer science from Chosun University in 2007 and 2011, respectively. Since 2014, he has been a professor in Department of Computer Science, Chosun University, Gwangju, Korea. His research interests are in information security, sensor network systems, mobile ad-hoc systems, smart grid home network systems and internet ethics.

Pankoo Kim received the BS degree in computer engineering from Chosun University of Korea and the MS and Ph.D. degrees in computer engineering from Seoul National University of Korea. He is a full professor in the Department of Computer Engineering at Chosun University. His specific research interests include semantic web techniques, semantic information processing and retrieval, and semantic multimedia processing. He is a member of the IEEE.



Sungbum Pan received his Ph.D. degrees in Electronics Engineering from Sogang University, Korea, in 1999, respectively. He was a team leader at Biometric Technology Research Team of ETRI from 1999 to 2005. He is now professor at Chosun University. His current research interests are biometrics, security, and VLSI architectures for real-time image processing.

Ilyong Chung received the B.E. degree from Hanyang University, Seoul, Korea, in 1983 and the M.S. and Ph.D. degrees in Computer Science from City University of New York, in 1987 and 1991, respectively. From 1991 to 1994, he was a senior technical staff of Electronic and Telecommunication Research Institute (ETRI), Dajeon, Korea. Since 1994, he has been a Professor in Department of Computer Science, Chosun University, Gwangju, Korea. His research interests are in computer networking, security systems and coding theory.