International Journal of Control and Automation
Vol. 7, No. 12 (2014), pp. 239-246
http://dx.doi.org/10.14257/ijca.2014.7.12.22

An Enhanced Grouping Proof for Multiple RFID Readers and Tag Groups

Jian Shen*[1,2,3], Haowen Tan[1,3], Yang Wang[1,3], Sai Ji[1,3] and Jin Wang[1,3]

[1]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science &Technology, Nanjing, 210044, China
[2] Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Nanjing University of Information Science & Technology, Nanjing, 210044, China
[3] School of Computer & Software, Nanjing University of Information Science &Technology, Nanjing , 210044, China

Abstract

RFID authentication on large numbers of tags or tag groups has attracted many researchers' attention as an extension of initial one-or-two-tags scenarios. Due to demands of RFID application in supply chain, various proofs are proposed in the purpose of solving existing problems of grouping tags identification. However, it is proved that verifiers in these proofs are not aware of abnormal relating devices instantly, which may cause both security and technical risks and lie heavy upon identification of the problematic tags and readers. In this paper, we propose an enhanced grouping proof for multiple RFID readers and tag groups, according to which the verifier is able to cope with multiple readers and tag groups simultaneously and know the detailed status of the problematic tags. In addition, privacy protection is provided by offering mutual authentication between the readers and tags. Moreover, it is hard for the malicious tags to pass the verification in the proposed proof.

Keywords: *Grouping proof; multiple readers; tag groups*

1. Introduction

Radio Frequency Identification (RFID), confirmed to have great potential in many applications, is basically composed of the backend processing system (BPS), readers and tags. Through radio communication, the whole RFID system is capable of identifying large amounts of goods with tags attached on them. In general, the RFID tag is expected to be made as cheap as it can be so that the barcode will be replaced. At the same time, privacy and security issues remain hot topics [1, 2].

Under normal circumstances, communication between the verifier and readers is set to be completely secure in many RFID authentication proofs. As a matter of fact, portable readers can be produced very small in size. Instead of traditional wired connection, portable readers communicate with the verifier in wireless way. As a result, it is necessary for the verifier to check out the validity of readers in case of forgery attack, which is taken into consideration in the proposed proof. We would like to emphasize that the verifier must be trustworthy in order to protect the entire RFID system [3]. In this paper, we propose an enhanced grouping proof for multiple RFID readers and tag groups. In our scheme, the verifier is able to cope with multiple readers and tag groups.

* The corresponding author

ISSN: 2005-4297 IJCA

This paper is arranged as followed: in the following section, some related works about RFID authentication proofs are introduced. Our proposed proof is described in detail in section 3. Security analysis of the proof is shown in section 4. Performance analysis of the proof is shown in section 5. Finally, the conclusion of this paper is covered in section 6.

2. Related Work

2.1 Grouping Proofs for Two Tags

In 2004, A. Juels proposed yoking proof to solve the simultaneously scanning problem of two tags [4]. The key idea of yoking proof is to link the two tags together to generate a proof with the help of random number generator in order to keep freshness of data in each session. Yoking proof is very important because it is the first time that simultaneously scanning issue is introduced. After that, many researchers were inspired and created their own grouping proofs. J. Saito and K. Sakurai [5] pointed out that the original yoking proof is vulnerable to replay attack and gave out “yoking proof using timestamp” to prevent the reuse of previous messages. In 2006, S. Piramuthu claimed that J. Satio and K. Sakurai’s proof still showed no resistance against replay attack and presented a novel proof to withstand the replay attack [6]. In 2008, Lien et al. proposed “reading order independent yoking proof” where the verifier does not need to predefine the reading order of tags before verification [7].

All the above proofs suffer from many shared issues coming from their property of linking proof together. Note that the verifier is not capable of knowing the detailed reason of the failure when the verification fails. In particular, the verifier cannot judge what situation the whole RFID system is in because communication blocks, transmission errors, missing of the tags or something else may result in the verification failure. On the other hand, these proofs are not efficient enough and some of which are only applicable in one-reader and one-tag-groups circumstances. In the complex situation with more readers and groups of tags, these proofs may not perform as well as they are designed to be [8].

2.2 Grouping Proofs for Multiple Tags

As extensions of two tags proofs, grouping proofs aim to generate a proof of multiple tags simultaneously, which is the hotspot of RFID authentication area. In 2006, L. Bolotnyy and G. Robins extended A. Juels’s work and proposed generalized yoking proof in [9]. However, identities of individual tags in [9] are not hidden, which may cause privacy leaking. After that, anonymous yoking proof is introduced in order to preserve the privacy of tags [10]. Considering of threat of certain reading order of the tags, reading order independent grouping proof is proposed by Y. Lien, *et al.*, [7]. In 2009, select-response grouping proof is designed by the method of letting the verifier be involved in the authentication instead of letting the verifier wait for the proof generated by the reader passively [11]. However, if the number of readers and tags increases, the computation cost in the verifier will be very large. In addition, in this proof, the reader only performs as a communicating channel between the tags and verifier and does not deal with any passing message.

We classified all the grouping proofs mentioned above into two families from the way the reader communicates with tags: the serial family and the parallel family. In the serial family, the reader exchanges information with each tag one by one and links them like a chain, which guarantees the integrity of the message [12, 13]. One broken tag of the chain will affect the whole authentication process, which is not efficient in practical applications. In the parallel family, the entire RFID system broadcasts messages to every tag at the same time. The proofs in the parallel family are more efficient than that in the serial family but may cause communication block [14].

3. The Proposed Proof

3.1 Detailed Design of the Proof

We propose an enhanced grouping proof for multiple RFID readers and tag groups in this paper. In our design, mutual authentication between the readers and tags is used to identify the tags. In this case, the incorrect message will be abandon so as to reduce the communication and computational cost of the entire RFID system as well as protect privacy and security. The notations used in the proposed proof are shown in Table 1.

Table 1. Notations used in the Proposed Proof

Symbol	Description
V	Verifier[1]
R_i	Reader *i*
T_i	Tag *i*
g_i	Tag group *i*
GID_i	Identifier of tag group *i*
ID_i	Identifier of tag *i*
r_i , r_{R_i} , r_{R_i}'	Random numbers
S_{g_i}	Secret of tag group *i*
MAC	Message Authentication Code
ID_{R_i}	Identifier of reader *i*
S_{R_i}	Secret of reader *i*

It is assumed that the entire RFID system has large amounts of readers and tag groups. The verifier knows the secret of all the tags groups and readers. The proposed grouping proof is shown in Figure 1.

[1] In general, the backend processing system (BPS) and the verifier are considered as one entity.

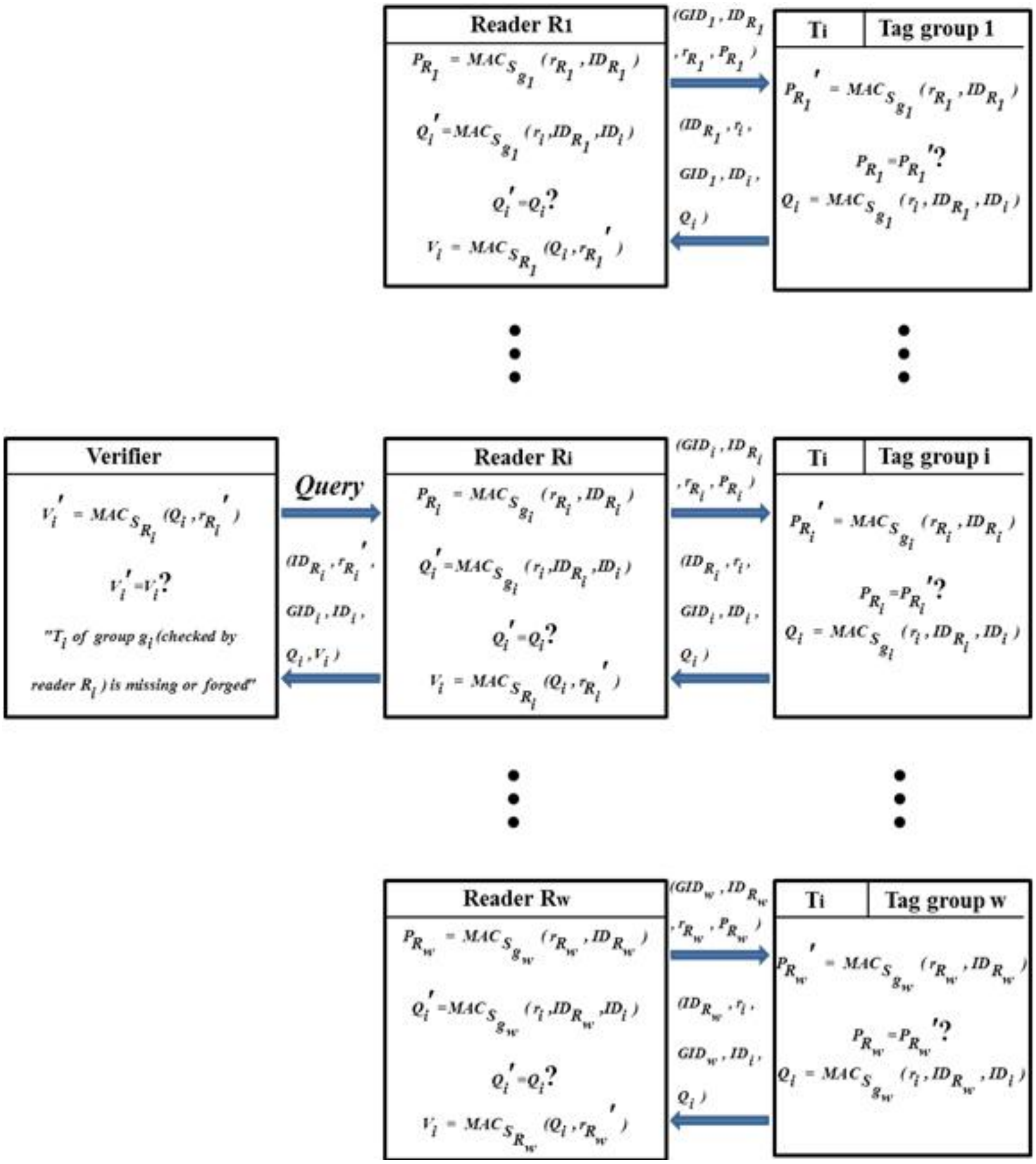
Reader R1
Ti
Tag group 1
Verifier
Query
Reader Ri
Ti
Tag group i
Reader Rw
Ti
Tag group w
$V_i' = MAC_{S_{R_i}}(Q_i, r_{R_i}')$
$V_i' = V_i$?
"T_i of group g_i (checked by reader R_i) is missing or forged"
$(ID_{R_i}, r_{R_i}', GID_i, ID_i, Q_i, V_i)$
$P_{R_i} = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$
$Q_i' = MAC_{S_{g_i}}(r_i, ID_{R_i}, ID_i)$
$Q_i' = Q_i$?
$V_i = MAC_{S_{R_i}}(Q_i, r_{R_i}')$
$(GID_i, ID_{R_i}, r_{R_i}, P_{R_i})$
$(ID_{R_i}, r_i, GID_i, ID_i, Q_i)$
$P_{R_i}' = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$
$P_{R_i} = P_{R_i}'$?
$Q_i = MAC_{S_{g_i}}(r_i, ID_{R_i}, ID_i)$

Figure 1. An Enhanced Grouping Proof for Multiple RFID Readers and Tag Groups

The process of the proof is described in detail as follows:

1) The verifier V sends the query to all the readers.

2) The reader R_i generates a random number r_{R_i} on receiving the query. R_i computes $P_{R_i} = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$ and broadcasts $(GID_i, ID_{R_i}, r_{R_i}, P_{R_i})$ to all the tag groups.

3) The tag group g_i wakes up. Note that group g_i is assumed to have k tags from T_1 to T_k. These k tags begin to compute $P_{R_i}{}' = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$ and compare with the received P_{R_i} to ensure the validity of R_i. After the authentication, each tag T_i generates a random number r_i

using r_{R_i} as a seed and computes $Q_i = MAC_{S_{gi}}(r_i, ID_{R_i}, ID_i)$. Then the tag T_i sends $(ID_{R_i}, r_i, GID_i, ID_i, Q_i)$ to R_i.

4) The reader R_i computes $Q_i^{'} = MAC_{S_{gi}}(r_i, ID_{R_i}, ID_i)$ and checks it with Q_i to guarantee identities of tags. Then R_i identifies and abandons incorrect message and collects all the remaining tags into groups by its GID_i. R_i generates a random number $r_{R_i}{}^{'}$ and computes $V_i = MAC_{S_{R_i}}(Q_i, r_{R_i}{}^{'})$ for each tag. At last, R_i adds V_i to the message received from T_i and relays $(ID_{R_i}, r_{R_i}{}^{'}, GID_i, ID_i, Q_i, V_i)$ to the verifier *V*.

5) The verifier computes $V_i^{'} = MAC_{S_{R_i}}(Q_i, r_{R_i}{}^{'})$ and compares it with V_i. If $V_i^{'} = V_i$, authentication completes. If not, the verifier *V* terminates the proof and shows “Tag T_i of group g_i (checked by reader R_i) is missing or forged”.

3.2 Key Properties of the Proof

The Mutual Authentication: Mutual authentication is an important factor in grouping proof verification. In order to protect the security and privacy of both tags and readers, mutual authentication between the readers and tags is required in our paper. In addition, due to the vulnerability of radio communication, it is also significant for the verifier to check the validity of the readers. In our proposed proof, the readers and tags authenticate with each other in the first time to guarantee the communicating entities are valid [11, 15].

Reading Order Independence: Some grouping proofs arrange certain order for the tags to be checked. In this circumstance, the entire verification process will be affected by unexpected events. Moreover, the adversary may know the reading order of the tags and damage the RFID system. Hence, it is important to have the proofs independent on reading order. In the proposed proof, it is not necessary for the tags to reply to the reader in a predefined reading order as our proof belongs to the parallel family [7, 16].

4. Security Analysis

4.1 Resistance to Replay Attack

Mutual authentication is provided between the readers and tags, which strengthens the verification. Note that random numbers are used in every step of the proof to prevent replay attack, which keeps the message fresh. In addition, the proof encrypts the message with MAC computation and secret keys so as to defend against replay attack [7, 14, 17].

4.2 Maintenance of Abnormal Tag Feedback

Our proof can identify the abnormal tag and provide security protection. In our proof, the verifier is able to acquire the detailed records of adversary’s forgery attacks and finds out which tag is missing instantly [11], which is very important in practical situation. In other word, abnormal tag feedback improves the maintenance of tag groups, where the RFID system can manage to check or replace the suspicious tags in time to preserve its integrity [18].

4.3 Ensuring of Reading Order Independent

The proposed proof is independent of the reading sequence of RFID tags, which is a crucial feature for a practical grouping proof. In our scheme, the readers send information to all the tag groups at the same time and are capable of obtaining message from the specific tag groups whose GID_i are in accordance with the received group identifiers. Moreover, identities of the tags are involved in the verification so that the corresponding readers are able to identify the tags in any order. Without requiring a predefined sequence of tags, the entire RFID system in our proof is efficient.

4.4 Against Clandestine Scan

In the proposed proof, it is difficult for the adversary to obtain privacy information of the tags through clandestine scan. The tags will check GID_i and group secret before responding anything to ensure the validity of the readers [11]. As a result, malicious readers are refused to continue the communications since they are unknown of the GID_i and corresponding secret keys. Therefore, privacy is protected in the proof [11, 20, 21].

5. Performance Analysis

In our proof, the verification process is simple. Note that only MAC functions are included in the computational operations, which is appropriate for low-price tags. In addition, the reader can identify the message intended to be sent to the verifier, which is applicable in practical situation and reduces computation cost of the verifier. Moreover, it needs to be stressed that most of the previous proposed grouping proofs are only good for single-reader occasion and do not take multiple-readers into consideration [5-7 10, 11], while our proof is capable of dealing with large amounts of tag groups and readers at the same time. The fact that massive tag groups and readers are under verification process simultaneously improves the speed of the whole system so the proof is more efficient than aforementioned proofs. Our proposed proof has vast potential for future development in the real application. For example, it can be applied to automobile factories with many departments to maintain the order of production and generates inventories of automobile parts so as to bring convenience to overall management of the entire factories.

6. Conclusion

In this paper we propose an enhanced grouping proof for multiple RFID readers and tag groups to verify groups of tags, where the verifier is able to know the detailed status of ineffective tags. The proof is reading order independent and more efficient and secure than previous proofs. Furthermore, the entire RFID system is available to scan several readers and tag groups, which is very useful in RFID applications.

Acknowledgements

This paper is a revised and expanded version of a paper entitled “A Novel RFID Authentication Protocol for Multiple Readers and Tag Groups” presented at CST 2014, Indonesia, 19-22 June, 2014. This work is supported by the research fund from Nanjing University of Information Science and Technology under Grant No.S8113003001, the National Science Foundation of China under Grant (61300237, 61232016, 61402234), the National Basic Research Program 973 under Grant No.2011CB311808, the research fund from Jiangsu Technology & Engineering Center of Meteorological Sensor Network in NUIST under Grant No.KDXG1301, the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) under Grant No.2011-0030823, the Natural Science Foundation of Jiangsu Province under Grant No.BK2012461, the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, and the PAPD fund.

References

[1]. H. Y. Chien and S. B. Liu, "Tree-Based RFID Yoking Proof, International Conference on Networks Security," Proc. of Wireless Communications and Trusted Computing (NSWCTC'09), vol. 1, **(2009)** April, pp. 550-553.

[2]. D. Z. Sun and J. D. Zhong, "A Hash-Based RFID Security Protocol for Strong Privacy Protection," Proc. of IEEE Transactions on Consumer Electronics, vol. 58, **(2012)** November, pp. 1246-1252.

[3]. A. Jules, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)** February, pp. 381-394.

[4]. A. Juels, "Yoking-proofs for RFID tags," Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, **(2004)** March, pp. 138-143.

[5]. J. Satio and K. Sakurai, "Grouping proof for RFID tags," Proc. of the 19th International Conference on Advanced Information Networking and Applications, vol. 2, **(2005)** March, pp. 621-624.

[6]. S. Piramuthu, "On Existence for Multiple RFID Tags," Proc. of IEEE International Conference on Pervasive Services (ICPS'06), **(2006)** June, pp. 317-320.

[7]. Y. Lien, X. Leng, K. Mayes, and J. H. Chiu, "Reading Order Independent Grouping Proof for RFID Tags," Proc. of IEEE International Conference on Intelligence and Security Informatics (ISI'2008), **(2008)** June, pp. 128-136.

[8]. J. Cho, S. Yeo, S. Huang, S. Rhee, and S. Kim, "Enhanced Yoking Proof Protocols for RFID Tags and Tag Groups," Proc. of 22nd International Conference on AINA-Workshops, **(2008)** March, pp. 1591-1596.

[9]. L. Bolotnyy and G. Robins, "Generalized "Yoking-proofs" for a Group of RFID Tags," Proc. of International Conference on Mobile and Ubiquitous Systems, **(2006)** July, pp. 1-4.

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

[11]. X. Leng, Y. Lien, K. Mayes, and J. H. Chiu, "Select-Response Grouping Proof for RFID Tags," Proc. of First Asian Conference on Intelligent Information and Database Systems (ACIIDS 2009), **(2009)** April, pp. 73-77.

[12]. M. Burmester, B. D. Medeiros, and R. Motta, "Provably Secure Grouping-Proofs for RFID Tags," Proc. of International Federation for Information Processing, **(2008),** pp. 176-190.

[13]. C. Ma, J. Lin, Y. Wang, and M. Shang, "Offline RFID Grouping Proofs with Trusted Timestamps," Proc. of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, **(2012),** pp. 674-681.

[14]. N. W. Lo and K. H. Yeh, "Anonymous Coexistence Proofs for RFID Tags," Journal of Information Science and Engineering, vol. 26, **(2010),** pp. 1213-1230.

[15]. P. P. Lopez, A. Orfila, J. C. H. Castro and J. C. A. V. D. Lubbe, "Flaws on RFID grouping-proofs. Guidelines for future sound protocols," Journal of Network and Computer Applications, vol. 34, no. 3, **(2011),** pp. 833-845.

[16]. H. Lee and D. Hong, "The tag authentication scheme using self-shrinking generator on RFID system," Proc. of Transactions on Engineering, Computing and Technology, vol. 18, **(2006),** pp. 52-57.

[17]. H. Sun, W. Ting and S. Chang, "Offlined simultaneous grouping proof for RFID tags," Proc. of the 2nd International Conference on Computer Science and its Applications, **(2009),** pp. 1-6.

[18]. H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong and L. T. Yang, "Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems," Proc. of IEEE Transactions on Parallel and Distributed Systems, vol. 24, **(2013)** July, pp. 1321-1330.

[19]. H. Huang and C. Ku, "A RFID grouping proof protocol for medication safety of inpatient," Journal of medical systems, vol. 33, no. 6, **(2009),** pp. 467-474.

[20]. I. Yamada, S. Shiotsu, A. Itasaki, S. Inano, K. Yasaki and M. Takenaka, "Secure active RFID tag system," Proc. of the 4th Workshop on Ubi Comp Privacy, **(2005)**.

[21]. F. Costa, S. Genovesi, A. Monorchio and G. Manara, "Perfect metamaterial absorbers in the ultra-high frequency range," Proc. Int. Symp. Electromagn. Theory, **(2013),** pp. 701 -703.

Authors

Jian Shen, He received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

Yang Wang, He currently is a Bachlor student in School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China. His research interests include information security, system modelling and network computing.

Haowen Tan, He received the B.E. degree in 2013 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology, Nanjing, China. He focuses on the security and privacy issues in radio frequency identification. His research interests include RFID authentication, security design in BAN and security modeling.

Sai Ji, He is an associate professor in Nanjing University of Information Science & Technology, China. He received his Bachelor (NUIST, China, 1999), Master (NUAA, China, 2006). His research interests are in the areas of Computer Measurement and Control, structural health monitoring and WSNs. He has published more than 20 journal/conference papers. He is principle investigator of three NSF projects.

Jin Wang, He received the B.S. and M.S. degree in the Electronical Engineering from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree from the Computer Engineering Department of Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and Technology. His research interests mainly include routing protocol and algorithm design, network performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.