A Lightweight and Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangements

Jian Shen*†‡§, Haowen Tan*§, Shaohua Chang*§, Yongjun Ren*§, Qi Liu*§
*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China
†Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Nanjing University of Information Science & Technology, China
‡Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, China
§School of Computer & Software, Nanjing University of Information Science & Technology, China
s_shenjian@126.com, tan_halloween@foxmail.com, casaha@126.com, renyj100@126.com, qrankl@163.com

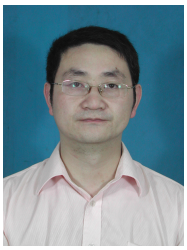
Abstract—Radio Frequency Identification (RFID) is a potential technology with the purpose of replacing the barcodes. The authentication towards multiple tags and tag groups has become the research hotspot considering of practical prospects of low-cost RFID tags. However, there are many concerns about the security risks and privacy issues due to the lightweight authentication property of the RFID tags. Many researches achievements have been made focusing on the existence of single tag in an object, while the arrangement that multiple tags attached to one object is out of consideration. In this paper, we propose a lightweight and practical RFID grouping authentication protocol in multiple-tag arrangement. In our assumption, one object to be authenticated is attached with a group of RFID tags. The backend process system (BPS) is able to take full control of the entire authentication process. The feedback towards various cases of the RFID tags is timely provided, which is available for practical situations. Additionally, the accurate position and status of the object can be ascertained with a number of tags combined with the object. Moreover, the protocol is proved to offer enough security assurances and have resistance to various attacks under the security analysis. The regular operation of RFID system will not be affected or damaged by the incidents occurred during the authentication process.

Keywords—RFID, lightweight, grouping authentication, multiple tag, security.

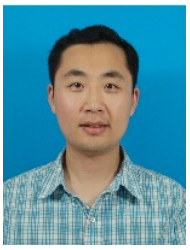
Jian Shen received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School 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.

Haowen Tan 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 authentication protocol design, and security formal modeling and analysis.

Ms. Chang received the B.E. degree from Nanjing University of Information Science and Technology, in 2013, and studying for the M.E. degree there. She focus on Body Sensor Network security. Her research interests include key management, authentication protocol design, and security analysis.



Yongjun Ren obtained the PhD degree in the computer and science department at the NanJing University of Aeronautics and Astronautics, China, in 2008. Now he is serving as a full time faculty in the NanJing University of Information science and Technology. His research interests include network security and applied cryptography.



Qi Liu received his BSc degree in Computer Science and Technology from Zhuzhou Institute of Technology, China in 2003, and his MSc and PhD in Data Telecommunications and Networks from the University of Salford, UK in 2006 and 2010. His research interests include context awareness, data communication in MANET and WSN, and smart grid. His recent research work focuses on intelligent agriculture and meteorological observation systems based on WSN.