The Computer Journal Advance Access published August 28, 2013

doi:10.1093/comjnl/bxt085

Editorial

Advanced Security Technologies and Services for Future Computing Environments

YOUNG-SIK JEONG[1], DAMIEN SAUVERON[2] AND JONG HYUK PARK[3,*]

[1]*Dongguk University, Seoul, Republic of Korea*
[2]*University of Limoges, Limoges, France*
[3]*Seoul National University of Science and Technology, Seoul, Republic of Korea*
[*]*Corresponding author: jhpark1@snut.ac.kr*

The objectives of this special issue are advanced security technologies and services for future computing environments, including, but not limited to, security primitives, protocols and security applications and services. Recent advances in security technologies and services for future computing environments have created a new class of the following: (i) Wireless sensor networks and radio-frequency identification security and privacy; (ii) security architectures for distributed network systems, P2P systems, cloud and grid systems; and (iii) security in e-commerce, mobile and wireless networks, and finally, security standards and assurance methods. All papers are expected to focus on novel approaches for advanced security technologies and services for future computing environments and to present high-quality results for tackling problems arising from the ever-growing advanced security technologies and services for future computing environments.

Keywords: security, future computing, wireless sensor networks, RFID, cooperative intelligent transportation systems

1. INTRODUCTION

The development of computing environments, such as the smart grid, peer-to-peer, personal cloud, machine-to-machine, pervasive and ubiquitous computing, is changing our environment. The objectives of this special issue are advanced security technologies and services for future computing environments, including, but not limited to, security primitives, protocols and security applications and services. The published papers are expected to focus on novel approaches for advanced security technologies and services for future computing environments and to present high-quality results for tackling problems arising from the ever-growing advanced security technologies and services for future computing environments.

We have received many manuscripts. Only six manuscripts of high quality were finally selected for this special issue. Each manuscript selected was blind reviewed by at least three reviewers consisting of guest editors and external reviewers. We present a brief overview of each manuscript in the following.

2. RELATED WORKS

Recent advances in security technologies and services for future computing environments have created a new class of the following: (i) Wireless sensor networks (WSN) and radio-frequency identification (RFID) security and privacy; (ii) security architectures for distributed network systems, P2P systems, cloud and grid systems and (iii) security in e-commerce, mobile and wireless networks, and finally, security standards and assurance methods.

Sensors and RFIDs are usually densely deployed in a sensor field in order to continuously monitor surrounding areas. In a sensor application, each sensor and each RFID have the capability to collect data such as temperature, humidity, light condition and so on, depending on targeted applications. The lack of physical security combined with unattended operations make sensor nodes prone to a high risk of being captured and compromised. The wireless broadcast nature may result in privacy breaches of sensitive information during data

transmission. Therefore, security and privacy issues of WSNs have attracted a lot of research efforts. The pervasive nature of RFID systems make stored data increasingly distributed among different parties. This raises many new privacy and security concerns for RFID systems. Because a reader is not much more than a radio transceiver, it is thus relatively easy for attackers to obtain illegitimate readers and to query RFID tags for sensitive information. For solving these problems, some papers proposed the following: Alcaraz [1] developed a method that allows the network designers to select the most suitable key management schemes (KMS) for a specific WSN network setting. In addition, it also addressed the issues on the current state-of-the-art research on the KMS for homogeneous (i.e. non-hierarchical) networks to provide solutions for establishing link-layer keys in various WSN applications and scenarios. Sun *et al.* [2] proposed a Linear Congruential Generator-based lightweight block cipher that can meet security co-existence requirements of WSNs and RFID systems. Xiao *et al.* [3] explained the Security and Privacy in RFID and Applications in Telemedicine and so on.

There are many interesting issues in distributed network systems, P2P systems, cloud and grid systems. Recently, the security architecture and functions have highly depended on the reference architecture in the cloud computing field. Some papers proposed the reference architecture and the main security issues concerning distributed networks, P2P and cloud service architecture [4, 5].

Finally, there are the main issues in security research for e-commerce mobile and wireless networks, and finally, security standards and assurance methods. In WAP layers, protocols and functions, many researchers proposed the scheme within a security layer of WAP with respect to the wireless transaction protocol and the scheme of authentication and privacy. Some articles provided the strategy for QoS-Based Routing Protocols for Wireless Sensor Networks in order to improve the reliability and the security of the data transmission [6, 7].

The first paper entitled "A two-step secure localization for wireless sensor networks" by Han *et al.* [8] presents DCCI—a novel scheme called Two-Step Secure Localization (TSSL) stand against many typical malicious attacks, e.g. wormhole attack and location spoofing attack. TSSL detects malicious nodes step by step. First, anchor nodes collaborate with each other to identify suspicious nodes by checking their coordinates, identities (IDs) and time of sending information. Then, by using a modified mesh generation scheme, malicious nodes are isolated and the WSN is divided into areas with different trust grades. Finally, a novel localization algorithm based on the arrival time difference of localization information is adopted to calculate locations of unknown nodes. Simulation results show that the TSSL detects malicious nodes effectively and the localization algorithm accomplishes localization with high localization accuracy.

The second paper entitled "Using GHZ-state for multiparty quantum secret-sharing without code table" by Chou *et al.* [9] presents two multiparty quantum secret sharing schemes based on the n-particle Greenberger–Horne–Zeilinger-states (GHZ states), which are transformed from Einstein–Podolsky–Rosen (EPR) pairs by entanglement swapping. In their schemes, the dealer imposes messages by performing local unitary operations (I, σx, iσy, σz) on n-particle GHZ state she holds, and the agents collaborate to deduce the dealer's messages by performing local unitary operations on their own qubit. They propose two schemes to increase secret messages. In scheme (I), Alice needs to share the code table with n agents, where $n \geq 3$. In scheme (II), Alice does not necessarily have to share the code table with $2n + 1$ agents, where $n \geq 1$. The schemes they proposed always share $2n$ classical bits each time. Moreover, the security of their schemes is also analyzed.

Next paper entitled "MBST: detecting packet-level traffic anomalies by feature stability" by Zhang *et al.* [10] presents a statistical analysis of six traffic features based on entropy and a distinct feature number at the packet level, and they find that, although these traffic features are unstable and show seasonal patterns like traffic volume for a long period, they are stable and consistent with Gaussian distribution in a short time period. However, this equilibrium property will be violated by some anomalies. Based on this observation, they propose a Multidimensional box plot method for Short-time scale Traffic (MBST) to classify abnormal and normal traffic. They compare their new method with MCST with the well-known wavelet-based technique. The detection result on synthetic anomaly traffic shows that MBST can better detect the low-rate attacks than wavelet-based and MCST methods, and the detection result on real traffic demonstrates that MBST can detect more anomalies with low false alarm rate than the other two methods.

In the fourth paper entitled "IPv6 security issues in cooperative intelligent transportation systems", by Lee and Ernst [11] present positions on the emerging and urgent security issues of IPv6 communications at the ETSI/ISO ITS standardization level. Cooperative intelligent transportation systems (ITSs) are present to us with safe and efficient driving environments as well as convenient and infotainment features for future ITS stations. Significant progress has been made in the areas of cooperative ITS, but relatively little attention has been paid to the security issues of cooperative ITS in terms of ITS station architecture, security decision making, security credential management, communication type, communication overhead and location privacy [11].

The fifth paper entitled "A secure automatic fare collection system for time-based or distance-based services with revocable anonymity for user" by Isern-Deyà *et al.* [12] presents an electronic and secure automatic collection system that is adapted for massive user transport. They have achieved a system that can be adapted to time-based or distance-based fares with slight changes. The use of group signature schemes allows user authentication while preserving privacy [12].

The last paper entitled "A cryptanalysis attack on a family of Distance Bounding protocols" by Mitrokotsa *et al.* [13] presents

a detailed security analysis on a family of such protocols. More precisely, they describe a passive attack that can be launched against several distance bounding authentication protocols and may lead to a full disclosure of the secret key shared by the verifier and the proved. The main contribution is a high probability bound on the number of sessions required for the attacker to discover the secret key, as well as an experimental analysis of the efficiency of the attack under noisy conditions. Both of these show that the success probability of the attack mainly depends on the length of the used nonces rather than the length of the shared secret key. The theoretical bound could be used by practitioners to appropriately select their security parameters. Finally, they provide a countermeasure that could be used in order to combat it.

ACKNOWLEDGEMENTS

Our special thanks go to Prof. Fionn Murtagh who is Editor-in-Chief of *The Computer Journal* and all editorial staff for their valuable support throughout the preparation and publication of this special issue. We would like to thank all authors for their contributions to this special issue. We also extend our thanks to the external reviewers for their excellent help in reviewing the manuscripts.

REFERENCES

[1] Alcaraz, C., Lopez, J., Roman, R. and Chen, H.-H. (2012) Selecting key management schemes for WSN applications. *Comput. Secur.*, **31**, 956–966.

[2] Sun, B., Xiao, Y., Li, C.C. and Andrew Yang, T. (2008) Security co-existence of wireless sensor networks and RFID for pervasive computing. *Comput. Commun.*, **31**, 4294–4303.

[3] Xiao, Y., Shen, X., Sun, B. and Cai, L. (2006) Security and privacy in RFID and applications in telemedicine. *IEEE Commun. Mag.*, **44**, 64–72.

[4] Lee, K. (2012) Security threats in cloud computing environments. *Int. J. Sec. Appl.*, **6**, 25–32.

[5] Jeong, W.-H., Kim, S.-J., Park, D.-S. and Kwak, J. (2013) performance improvement of a movie recommendation system based on personal propensity and secure collaborative filtering. *J. Inf. Process. Syst.*, **9**, 157–172.

[6] Sumathi, R. and Srinivas, M.G. (2012) A survey of QoS based routing protocols for wireless sensor networks. *J. Inf. Process. Syst.*, **8**, 589–602.

[7] Varshney, U. and Vetter, R. (2000) Mobile and wireless networks. *Commun. ACM*, **43**, 73–81.

[8] Han, G., Jiang, J., Shu, L., Guizani, M., Nishio, S. (2012) A two-step secure localization for wireless sensor networks. *Comput. J.*, Online Published, doi:10.1093/comjnl/bxr138.

[9] Chou, Y.-H., Chen, S.-M., Lin, Y.-T., Chen, C.-Y. and Chao, H.-C. (2012) Using GHZ-state for multiparty quantum secret sharing without code table. *Comput. J.*, Online Published, doi:10.1093/comjnl/bxs005.

[10] Zhang, B., Yang, J., Wu, J. and Wang, Z. (2012) MBST: detecting packet-level traffic anomalies by feature stability. *Comput. J.*, Online Published, doi:10.1093/comjnl/bxr134.

[11] Lee, J.-H. and Ernst, T. (2012) IPv6 security issues in cooperative intelligent transportation systems. *Comput. J.*, Online Published, doi:10.1093/comjnl/bxs006.

[12] Isern-Deyà, A.P., Vives-Guasch, A., Mut-Puigserver, M., Payeras-Capellà, M. and Castellà-Roca, J. (2012) A secure automatic fare collection system for time-based or distance-based services with revocable anonymity for users. *Comput. J.*, Online Published, doi:10.1093/comjnl/bxs033.

[13] Mitrokotsa, A., Peris-Lopez, P., Dimitrakakis, C. and Vaudenay, S. (2012) On selecting the nonce length in distance-bounding protocols. *Comput. J.*, doi:10.1093/comjnl/bxt033.