Guest Editorial: Special Issue on Advances in Internet Security and Technology[*]

Baokang Zhao[†] and Chunqing Wu
School of Computer Science
National University of Defense Technology
Changsha, Hunan, CHINA
{bkzhao, chunqingwu}@nudt.edu.cn

Qin Xin
Faculty of Science and Technology
University of the Faroe Islands, Denmark
qinx@setur.fo

Today's Internet has been considered as the largest engineered system ever created by mankind, which consists of hundreds of millions of connected individual computer hosts, communication links, and switches. It is a worldwide collection of connected networks that can be accessed by individual computer hosts through different ways, including gateways, routers and switches, dial-up connections, and Internet service providers. Combining with powerful capabilities of distributed computing and communications, the Internet has been serving as a new paradigm of information infrastructure, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals, government agencies, financial companies, academic institutions and businesses of all size without taking into account geographic locations. People and our societies have become increasingly dependent on the Internet for personal or professional uses regardless of whether it is for e-mail, file transfer, remote login, web page access or commercial transactions. Given that the Internet is so large and has so many diverse components and uses, it naturally brings lots of challenges on issues related to architecture, congestion, naming/addressing, interoperability, routing, resilience, dependability, fault tolerant, security and privacy. To achieve a good performance for Internet applications, all these addressed issues above should be considered.

This special issue on "Internet Security and Technology" attempts to highlight some of the latest research addressing those challenges. It collects a series of papers on the important topics, More specifically:

- The first paper, "Lattice Based Forward-Secure Identity Based Encryption Scheme with Shorter Ciphertext" by Singh et al. [7], proposes a novel identity based encryption scheme to reduce the size of the ciphertext. The delegation technique allows short basis (trapdoor) of a given lattice to derive short basis (trapdoor) of related lattice in a more secure way. However, it also needs to

[*]This special issue is financially supported by the Institute of Computer Networks and Information Security, School of Computer Science, National University of Defense Technology, and the grants of the National Basic Research Program of China (973 project) under Grant No.2009CB320503, 2012CB315906; and supported by Program for Changjiang Scholars and Innovative Research Team of the Ministry of Education ("Network Technology", NUDT), the Innovative Research Team of Hunan Province ("Network Technology", NUDT), the Innovative Research Team of Hunan Provincial natural science foundation of CHINA (11JJ7003).

[†]Corresponding author: Tel: +86-731-84575815

increase the size of the ciphertext. In this paper, the authors propose a new lattice based approach that significantly reduced the size of ciphertext.

- The paper of Allal and Boudjit [1], entitled “Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal” examines the geocast routing in VANETs(Vehicular Ad Hoc Networks). Geocast routing is an important technique used to route a message from an unique source vehicle to all vehicles located in a well geographically defined destination area. This paper provides a survey on existing geocast routing protocols for VANETs together with a classification based on the relay selection techniques. Furthermore, a new routing protocol named GeoSUZ is proposed to enhance the data efficiency of the geocast data dissemination.

- The paper of Dhurandher et al., “Energy-based Performance Evaluation of Various Routing Protocols in Infrastructure-less Opportunistic Networks” [4], focuses on the performance evaluation of various routing protocols in opportunistic Networks(Oppnets). Routing and forwarding are very challenging tasks in Oppnets due to the uncertain mobility and intermittent behavior of the nodes. Moreover, energy efficiency is another important concern in the performance evaluation of Oppnets Routing. In this paper, the authors have simulated, investigated and compared the performance of various already existing routing protocols for infrastructure-less Oppnets in terms of energy consumptions.

- The paper of Dabrowski et al. [3], entitled “A context-aware architecture for IPTV services personalization”,focuses on the personalization for the IPTV digital services and content distributions. Following the rapid expanding of IPTV, it becomes more and more critical to design efficient user interfaces for discovering the contents, as well as for manipulating associated interactive services. In this paper, the authors propose a novel UP-TO-US context-aware architecture for unified storage and processing situational data in IPTV service. Under such an architecture, the content personalization can be achieved by matching the users’ needs and current state of its surrounding environment.

- Sun, Song, Yang and Qin’s paper on “DHR-CCN, Distributed Hierarchical Routing for Content Centric Network” [8] presents a Distributed Hierarchical Routing for Content Centric Network (DHR-CCN). The Content Centric Network (CCN) is very useful since it provides a high-efficient mechanism to store the content at the network center and edge. Moreover, the design of efficient routing scheme becomes even more challenging because that the name of the corresponding content is used for the data transmission in CCN instead of the IP address. The distributed hierarchical routing scheme proposed in this paper provides the efficient information diffusion of the content names to reduce the overhead of the naming routing.

- Chen and Prokopi’s paper on “Enabling Resource-Aware Ubiquitous Applications for Personal Cloud with a Pairing Device Framework” [2] examines the problem of implementing ubiquitous computing in the context of cloud computing from the personal devices. With the increasing capability of these smart devices, such as smart phones and tablets, it enables to build a ubiquitous computing environment. The authors propose a common device framework that shall serve the underlying communication requirements, allowing personalized service innovation.

- The paper of Flores et al., “An Anti-Money Laundering Methodology: Financial Regulations, Information Security and Digital Forensics Working Together” [5], examines the problem of Anti-Money Laundering. In this paper, several issues including financial regulations, information security and digital forensics are carefully discussed. Moreover, an enhanced money laundering detection model and its related key features are proposed to provide a proper capability to identify, collect, acquire, and preserve admissible and reliable digital evidences, based on the BS ISO/IEC 27001, 27002 and 27035 standards.

- The final paper by Selvi, Vivek, Pradhan and Rangan [6] on "Efficient Certificateless Online/Offiine Signature with tight security" examines how light weight cryptography can be used in low power devices. The authors present a Online/Offine Signature (CLOOS) scheme and give a tight security reduction to the Gap Diffie-Hellman problem in the random oracle model. The CLOOS scheme provided is a light weight cryptography with the high security and the low communication overhead.

We believe that the papers included in this special issue illustrate some of the important issues investigated at the research of internet security and technology. We are happy and privileged to have been offered the opportunity to guest-edit this special issue of *Journal of Internet Services and Information Security (JISIS)*.

With the Editor-in Chief, Dr. Ilsun You, we wish to extend our special thanks to all authors, reviewers and editorial members for their invaluable contributions, without which this special issue would not have been possible.

References

[1] S. Allal and S. Boudjit. Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):20–36, February 2013.

[2] L. B. Chen and M. Prokopi. Enabling Resource-Aware Ubiquitous Applications for Personal Cloud with a Pairing Device Framework. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):83–100, February 2013.

[3] M. Dabrowski, J. Gromada, H. Moustafa, and J. Forestier. A context-aware architecture for IPTV services personalization. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):49–70, February 2013.

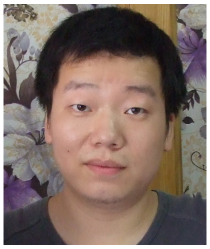
[4] S. K. Dhurandher, D. K. Sharma, and I. Woungang. Energy-based Performance Evaluation of Various Routing Protocols in Infrastructure-less Opportunistic Networks. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):37–48, February 2013.

[5] D. A. Flores, O. Angelopoulou, and R. J. Self. An Anti-Money Laundering Methodology: Financial Regulations, Information Security and Digital Forensics Working Together. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):101–114, February 2013.

[6] S. S. D. Selvi, S. S. Vivek, V. K. Pradhan, and C. P. Rangan. Efficient Certificateless Online/Offline Signature with tight security. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):115–137, February 2013.

[7] K. Singh, C. Pandurangan, and A.K.Banerjee. Lattice Based Forward-Secure Identity Based Encryption Scheme with Shorter Ciphertext. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):5–19, February 2013.

[8] L. Sun, F. Song, D. Yang, and Y. Qin. DHR-CCN, Distributed Hierarchical Routing for Content Centric Network. *Journal of Internet Services and Information Security (JISIS)*, 3(1/2):71–82, February 2013.



Baokang Zhao is an assistant Professor with the School of Computer Science, National University of Defense Technology. He received his B.S. and Ph.D. Degrees from the National University of Defense Technology, both in Computer Science. His current research interests include protocols, algorithms, and security issues in computer networks.

Chunqing Wu is a Professor with the School of Computer Science, National University of Defense Technology. She holds her B.S., M.S., and Ph.D. in Computer Science from the National University of Defense Technology. Her research interests are in computer networks and information security. She can be reached at *chunqingwu@nudt.edu.cn*.

Qin Xin is working in Faculty of Science and Technology at University of the Faroe Islands (UoFI), Faroe Islands as an associate professor. He obtains his Ph.D degree in Department of Computer Science at University of Liverpool, UK in December 2004. Prior to joining UoFI, he had held variant research positions in world leading universities and research laboratory including Senior Research Fellowship at Universitfi. Catholique de Louvain, Belgium, Research Scientist/Postdoctoral Research Fellowship at Simula Research Laboratory, Norway and Postdoctoral Research Fellowship at University of Bergen, Norway. His main research focus is on design and analysis of sequential, parallel and distributed algorithms for various communication and optimization problems in wireless networks and information management systems. Moreover, he also investigates the combinatorial optimization problems with applications in Bioinformatics, Data Mining and Space Research.