GUEST EDITORIAL PREFACE

Emerging Security Threats and Defense Technologies in Mobile Computing and Networking

Ilsun You, Korean Bible University, Seoul, South Korea

Xianglin Wei, Nanjing Telecommunication Technology Research Institute, Nanjing, China

Chunfu Jia, Nankai University, Tianjin, China

With the rapid evolution of computing paradigms and the increasing popular of mobile devices, newly emerging mobile computing paradigms become more and more prevalent, such as crowd-souring computing, human-centred computing, mobile cloud computing etc. Moreover, with the emergence of new computing paradigms, communication networks experience unprecedented transformation which greatly improves their network capacity and thus Quality of Service. However, the newly developed computing and networking paradigms are also faced with many traditional security threats in the networking plane, as well as the computing knowledge plane, such as jammer attacks, wireless network intrusion, and those attacks on the content of the data, etc. Moreover, the newly emerging security threats such as network structure sniff, smart jammer attacks, and privacy leak also restrict the development of these new paradigms. The objective of this special issue is to collect different thoughts of the researchers and practitioners on the relevant topics. Given the current status, any enhanced technology addressing security issues arise in application layer, transmission layer and physical layer can be considered as the wide work space. In this issue, we mainly thought about getting some specific contributions on security issues in application and transmission layers.

Though there were other submissions with high quality, because of the restrictions of the number of papers in one special issue, we have accepted only 6 papers while each paper has been reviewed by at least three experts to ensure the quality of this special issue.

Let us give a brief introduction of the papers for a better understand of their contribution in this special issue's area.

Wang et al., in their work "Jammer Location-oriented Noise Node Elimination Method for MHWN" develop an algorithm to eliminate noise nodes based on the Mean of Squared Dis-

tance among the nodes for Multi-Hop Wireless Network to promote the localization accuracy of existing jammer localization algorithms. Through calculating the Mean of Squared Distance of each node, the algorithm can find out the noise nodes and remove them. Their simulation results in different jamming localization algorithms verify the correctness and effectiveness of the proposed algorithm. This work investigates the security issue at the transmission layer and is a good contribution to this special issue focusing on the main theme.

Liu et al. attempt to provide practitioners with a strategy on selecting performance metrics for classifier evaluation in their work "A Strategy on Selecting Performance Metrics for Classifier Evaluation". Firstly, they investigate seven widely used performance metrics, namely classification accuracy, F-measure, kappa statistic, root mean square error, mean absolute error, the area under the receiver operating curve, and the area under the precision-recall curve. Then, they resort to using Pearson linear correlation and Spearman rank correlation to analyze the potential relationship among these seven metrics. Experimental results show that these commonly used metrics can be divided into three groups. Finally, they give some suggestions on choosing adequate measures to evaluate a classifier's performance from a user perspective. Their work is helpful for the researchers to select appreciate metrics for evaluating various security technologies.

In an interesting work "What is New about the Internet Delay Space?", Zhang et al. carry out a large scale measurement to investigate the characters of Internet delay space from three aspects: the relationship between delay and geodistance, TIV severity and its dimensionality. It's found that as the evolvement of the Internet, the Internet delay space is transforming from a non-metric space into a metric space. To validate their observation, they perform a few simulation experiments.

Yang et al., in their work "Machine Learning Based Prediction and Prevention of Malicious Inventory Occupied Orders", aim to determine the best practice and model of the technical solutions that can effectively and systematically limit malicious inventory occupied orders (MIOOs), using the methods of analytical mining and case studies. They provide test and application of their model. This work considers the security issue in the viewpoint of application layer which is important for the mobile computing.

In "Interactive Multi-view Visualization for Fraud Detection in Mobile Money Transfer Services", Novikova et al. consider an interactive multi-view approach for detection of the fraudulent activity in the Mobile money transfer services (MMTS). This work considers a set of visualization techniques enabling comprehensive analysis of the MMTS subscriber behavior according to his/her transaction activity. They suggest a metaphoric visualization of the MMTS users' behavior based on RadViz visualization that is able to identify groups with similar behavior and outliers. The analysis of how transaction activity is changing over time is supported by heat map visualization of the transaction attributes. Then, they demonstrate how the proposed approach can be used to reveal money laundering scenarios, behavior frauds, present and discuss the results of the efficiency evaluation of the developed visualization techniques. The graphic demonstration in this work is interesting.

Finally, Borisenko et al., in their work "Framework for Infrastructure Attack Modeling in Hybrid Networks", consider a framework for modeling infrastructure attacks and protection mechanisms in hybrid networks. The developed framework saves time conducting tests and improves the accuracy of the experiments by connection the simulation system to real network nodes. They present formal description of the modeling system components and show modeling system architecture and implementation. Experimental results verify that the proposed hybrid modeling method can significantly improve the accuracy of the simulation of infrastructure attacks and defense mechanisms. This work could be beneficial when considering the security issues in the viewpoint of network.

Considering the target and the outcome, the Special issue has become a success. While we hope that the papers in this issue would be very helpful for the researchers working on the relevant fields. To this end, we would like to thank all the editors, authors and reviewers involved in the entire process. Especially, we are thankful to the Editors-in-Chief, Drs. Ismail Khalil and Edgar Weippl who approved the special issue and has guided us throughout the process.

Ilsun You
Xianglin Wei
Chunfu Jia
Guest Editors
IJMCMC