Mobile Networks and Applications (2021) 26:1407–1411
https://doi.org/10.1007/s11036-020-01683-4

Editorial: Security and Privacy in Computing and Communications

Zheli Liu[1] · Jin Li[2] · Ilsun You[3] · Siu-Ming Yiu[4]

Published online: 11 November 2020

Editorial:

The computing models and communication environments are changed tremendously because of the rapid development for real-world application. With the advances in information systems and technologies, we are witnessing the advent of novel challenges on security and privacy in computing and communications for mobile devices, cloud and Internet application, IoT service and application, big data application, etc. The new requirements for security and privacy have been brought by the new technologies and applications. Traditional security and privacy cannot be completely suitable for the new environment. There exist some limitations to the real-world application by the traditional methods. The researchers have tried to explore new methods to solve the security and privacy problems in computing and communication by the usage of machine learning and optimization strategies. The special issue solicits contributions of novel methods to provide security and privacy in computing and communications for real-world application.

This special issue features thirty selected papers with high quality. The first article, "A Revocable Group Signatures Scheme to Provide Privacy-Preserving Authentications", authored by Xiaohan Yue, introduced a security model that contains the definition of backward security, and propose a revocable group signatures scheme that is more efficient and scalable compared to previous ones, especially for Sign and Verify algorithms, which are performed much more frequently than others. In addition, considering the heavy workload of the group manager, they divide the whole group into groups by employing a decentralized model to make their scheme more scalable, and thus more practical in real-life applications.

The second article titled "Privacy-Preserving Top-k Location-based Services Retrieval in Mobile Internet" provided a secure and efficient service retrieval scheme in cloud computing. Specifically, a novel encrypted index structure is designed by taking both service texts and locations into consideration. Moreover, a depth-first search algorithm is created for the index and it can efficiently return query results. Theoretical analysis and simulation results illustrate security and efficiency of their scheme.

In the next article with the title "Throughput Analysis of Smart Buildings-oriented Wireless Networks under Jamming Attacks", the authors investigated the throughput of IEEE 802.11 enabled IoT, where a ring model is put forward to capture the distribution of legitimate nodes and jammers. Afterwards, the collision probability of wireless transmission is derived from the perspective of both physical layer and MAC layer. Then, the throughput of each IoT node is calculated. To validate their models, numerical tests as well as simulation results derived on NS3 are provided with various parameter settings. Simulation results show that their models could accurately characterize the performance of IEEE 802.11-enabled wireless networks under jamming attacks.

The use of nodes with different sensing capabilities is pervasive. This leads to many environments capable of monitoring human activity for security, comfort, and connectivity applications among others. The fourth article titled "Dynamic Spectrum Access Algorithm Based on Game Theory in Cognitive Radio Networks" focused on a covert channel communication system based on sound waves with cognitive radio capabilities. In such system, the mobile nodes are infected with malware that allows the attacker to obtain information from the devices, sending data using a covert channel (hidden communications) to neighbor sensor nodes used for IoT applications through sound waves imperceptible to human ears. A cognitive radio design is based on allowing such hidden communications to occur when the primary channel is unused (i.e., when the user is not using or handling its device).

With the acceleration of the Internet of things (IoT) construction, the security and energy consumption of IoT will

✉ Zheli Liu
liuzheli1978@163.com

[1] Nankai University, 94 Weijin Rd, Nankai District, Tianjin 300071, China

[2] Guangzhou University, Guangzhou, China

[3] Department of Information Security Engineering, Soonchunhyang University, 22 Suncheonhyang-ro, Sinchang-myeon, Asan-si, Chungcheongnam-do, South Korea

[4] The University of Hong Kong, Pok Fu Lam, Hong Kong

become an import factor restricting the overall development of the IoT. The fifth article, "Intrusion Detection System for IoT Heterogeneous Perceptual Network" proposed the placement strategy of the intrusion detection system (IDS) described in this paper is to place the IDS on the cluster head nodes selected by the clustering algorithm called ULEACH. By optimizing the calculation of the node threshold, the ULEACH clustering algorithm will comprehensively consider the heterogeneity of the perceptual nodes and take the residual energy, energy consumption rate, and overall performance of the nodes into account. As a result, the strategy improves the utilization of the nodes to enhance the performance of heterogeneous perceptual network and extend the lifetime of the system. Furthermore, the paper proposes a intrusion detection system framework and establishes dynamic intrusion detection model for IoT heterogeneous perceptual network based on game theory, by applying modified particle swarm optimization, the optimal defense strategy that could balance the detection efficiency and energy consumption of the system is obtained.

As the security of cloud storage cannot be effectively guaranteed, many users are reluctant to upload their key data to the cloud for storage, which seriously hinders the development of cloud storage. The sixth article, "Role-Based Access Control Model for Cloud Storage Using Identity-Based Cryptosystem" proposed an RBAC scheme for ciphertext in cloud storage. They also give the formal definitions of their scheme, a detailed description of four tuple used to represent access control strategy, the hybrid encryption strategy and write-time re-encryption strategy, which are designed for improving the system efficiency. The detailed construction processes of their scheme which. Include system initialization, add and delete users, add and delete permissions, add and delete roles, add and delete role inheritance, assign and remove user, assign and remove permission, read and write file algorithm are also given.

Covert channels are widely used for secret message transmission on networks, and they are constantly changing and updating to adapt to the new network and communication environment. The seventh article, "A Timestamp-Regulating VoLTE Covert Channel against Statistical Analysis" designed a secure covert storage channel for VoLTE via regulating timestamp of VoLTE packets. First, they analyze the data captured in the real environment and find out two statistical patterns for the timestamp of the video packets. Then, they build the covert channel by modifying timestamp to carry the covert message in the case of maintaining these two patterns.

With the development of service-oriented architecture, Web service composition has become more important for mitigating potential security vulnerabilities. The eighth article, "An Efficient Bounded Model Checking Approach for Web Service Composition" verified the composition of semantic Web services described by OWL-S and proposes a timed service model (TSM) to formally model the service composition system. Furthermore, the auto-mapping relationship between the OWL-S service description and the model is established. For more efficient verification, this study uses SMT-based (SMT: satisfiability modulo theory) encoding in the TSM. Finally, a public emergency service composition system was built to verify the proposed model and the efficiency of the proposed algorithm.

The spread of Internet rumors and viruses has caused great hidden dangers to the safety of human life. The ninth article, "PRIA: a Multi-source Recognition Method Based on Partial Observation in SIR Model" proposed a novel PRIA algorithm to locate multiple propagation sources. Firstly, they propose a new partitioning method based on effective distance, which transforms the source problem into a single source problem in multiple partitions. Secondly, they propose a single source algorithm based on SIR propagation model, which uses reverse infection algorithm to locate suspicious sources. Finally, they evaluate their approach in real network topology.

The tenth article, "A Privacy-sensitive Service Selection Method Based on Artificial Fish Swarm Algorithm in the Internet of Things" proposed a privacy-sensitive service selection algorithm based on the Artificial Fish Swarm Algorithm (ASFA). It aims to choose the service with the best Quality of Experience (QoE) which includes privacy preferences as one of its primary factors so as to reduce the risk of privacy exposure and to pick up the service that satisfies all the requirements of users. Specifically, QoE model with privacy preferences is established and relevant constraints as well as quantitative methods are given firstly. Secondly, the proposed algorithm is constructed to select specific services based on the above model. Finally, the proposed method is verified through simulations.

The reliability performance analysis of coupled cyber-physical systems under different network types is investigated. The eleventh article, "Security Assessment for Interdependent Heterogeneous Cyber Physical Systems" proposed a practical model for interdependent cyber-physical systems using network percolation theory. Besides, for different network models, they also study the effect of cascading failures effect and reveal mathematical analysis of failure propagation in such systems. Then they analyze the reliability of their proposed model caused by random attacks or failures by calculating the size of giant functioning components in interdependent cyber-physical systems. In order to gain an insight into the proposed analysis model, numerical simulation analysis is also provided.

The Internet of Things (IoT) has become a research hotspot in recent years. With the increase of smart devices which are connected in IoT, the privacy of IoT has become an important problem. The twelfth article, "Correction to: Identity-based Multi-Recipient Public Key Encryption Scheme and Its Application in IoT" constructed a new ID-MRPKE by using the programmable hash function from multilinear maps. The security of the novel scheme can be proven in the standard

model, instead of the random oracle. Furthermore, based on the k-level Multilinear-maps Decisional Deffie-Hellman (MDDH) assumption, they prove that the proposed scheme has the indistinguishability under the selective multi-identity attack and chosen plaintext attack (IND-sMID-CPA).

Reversible watermarking is an important method of information hiding, which has been widely used in copyright protection of relational data. The thirteenth article, "A Graded Reversible Watermarking Scheme for Relational Data" proposed a graded reversible watermarking scheme for relational data. By removing the arbitrary portion of the watermark, data quality can be enhanced incrementally. The notion of data quality grade is defined to describe the impact of watermark embedding on the usability of data. Four fundamental algorithms are designed to facilitate the processes of watermark embedding, data quality grade detection, watermark detection, and data quality grade enhancement. Before data distribution, numbers of data quality grades can be predefined.

The fourteenth article, "A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks" proposed a malicious node detection model based on reputation with enhanced low energy adaptive clustering hierarchy (Enhanced LEACH) routing protocol (MNDREL). MNDREL is a novel algorithm, which is aimed at identifying malicious nodes in the wireless sensor network (WSN) more efficiently. Cluster-head nodes are first selected based on the enhanced LEACH routing protocol. Other nodes in WSN then form different clusters by selecting corresponding cluster-head nodes and determine the packets delivery paths. Each node then adds its node number and reputation evaluation value to the packet before sending it to the sink node. A list of suspicious nodes is then formed by comparing the node numbers, obtained through parsing with the packets by the sink node, with the source node numbers. To determine the malicious nodes in the network, the ratio of the suspect value to the trusted value of each node is further calculated and compared with a predefined threshold.

Fuzzy keyword search is a necessary and important feature of information retrieval in modern cloud storage services since users with insufficient knowledge may input typos or keywords with inconsistent formats. The fifteenth article, "A Privacy-preserving Fuzzy Search Scheme Supporting Logic Query over Encrypted Cloud Data" proposed a new secure multi-keyword fuzzy search scheme for encrypted cloud data, their scheme leverages random redundancy method to handle the deterministic of bloom filter to resist SNMF attack. Besides the privacy, their scheme uses tree-based index construction to improve search efficiency and allows users to conduct complicated fuzzy search with logic operations "AND", "OR" and "NOT", which can meet more flexible and fine-grained query demands.

The sixteenth article, "Quadratic Poly Certificateless Inductive Signcryption for Network Security" presented Quadratic Poly Certificateless Inductive Signcryption (QPCIS) for network security in WSN without using bilinear pairing. The QPCIS scheme inherits the security of quadratic polynomial that possesses lower computation complexity than bilinear pairing. In QPCIS scheme, only designated receiver node recovers the data packet via base station by verifying validity of signcrypted data packet using Inductive Probability theorem.

With the rapid development of cloud storage technology, cloud data assured deletion has received extensive attention. The seventeenth article, "An Efficient Scheme of Cloud Data Assured Deletion" proposed an efficient scheme of cloud data assured deletion. The scheme replaces complicated bilinear pairing with simple scalar multiplication on elliptic curves to realize ciphertext policy attribute-based encryption of cloud data, while solving the security problem of shared data. In addition, the efficiency of encryption and decryption is improved, and fine-grained access of ciphertext is realized. The scheme designs an attribute key management system that employs a dual-server to solve system flaws caused by single point failure.

Shor presented a quantum algorithm to factor large integers and compute discrete logarithms in polynomial time. The eighteenth article, "Cryptanalysis of a Public Key Cryptosystem Based on Data Complexity under Quantum Environment" breaked Wu's public key cryptosystem and signature scheme by directly solving the private key from the public key. Therefore, their public key cryptosystem and signature scheme are insecure in a quantum computer.

The nineteenth article, "An Evolutionary-Based Black-Box Attack to Deep Neural Network Classifiers" introduced a new black-box adversarial attack based on evolutionary method and bisection method, which can greatly reduce the L0 distance while limiting the L2 distance. By flipping pixels of the target image, an adversarial example is generated, in which a small number of pixels come from the target image and the rest pixels are from the source image.

With the increasingly extensive applications of the network, the security of internal network of enterprises is facing more and more threats from the outside world, which implies the importance to master the network risk assessment skills. The twentieth article, "Network Risk Assessment Based on Baum Welch Algorithm and HMM" used the Baum Welch algorithm to optimize the risk assessment process by establishing the HMM model, which can improve the accuracy of the evaluation value. Firstly, behavior of the attacker is described in-depth by the attack graph generated through MulVAL framework. Then, the nodes on the attack path can will be evaluated and the value will be further evaluated by the Bayesian model. Finally, by establishing the hidden Markov model, the corresponding parameters can be defined and the most likely probabilistic state transition sequence can be calculated by using the Viterbi algorithm and Baum Welch algorithm to deduce the attack intent with the highest possibility.

The twenty-first article, "A Confidence-Guided Evaluation for Log Parsers Inner Quality" presented a p_value-guided inner quality assessment on multiple log parsing algorithms. This method uses conformal evaluation to gain a deep insight of log parser quality. In this method, they choose the string edit distance algorithm as underlying non-conformity measure for conformal evaluation. They introduce two quality indicators to evaluate log parsers: credibility and confidence. The credibility reflects how conformal a log message to a event template generated by a log parser whereas the confidence reflects how non-conformal this log message to all other event templates. In order to demonstrate the inherent difference among different log parsers, they display the distribution of credibility and confidence of each prediction on tSNE 2D space.

Generally, the 5th Generation (5G) network will be soon available in the near future. It will be one with the feature that some of its network functions are handled by Virtual Machines (VMs), rather than by a dedicated one (like that in the 4th generation (4G) networks). The twenty- second article, "A Fault Tolerant Mechanism for UE Authentication in 5G Networks" proposed a fault tolerant mechanism for 5G end-device authentication, named Fault Tolerant 5G Authentication Scheme (FT5AS), in which a machine, named Mediator, is added to manage and keep track of authentication steps for end devices. The purpose is that when a VM fails, other AUSFs can successfully take over its authentication tasks on UEs. Also, the FT5AS can detect this failure immediately and react properly, aiming to increase the Quality of Service (QoS) that an UE can receive from 5G networks.

The twenty-third article, "Malware Detection Based on Multilevel and Dynamic Multi-feature Using Ensemble Learning at Hypervisor" proposed a new malware detection method to improve virtual machine security performance and ensure the security of the entire cloud platform. This paper used the virtual machine introspection(VMI) combined with the memory forensics analysis(MFA) technology to extract multiple types of dynamic features from the virtual machine memory, the hypervisor layer and the hardware layer. Furthermore, this paper proposed an adaptive feature selection method. By combining three different search strategies, three types of features are compared and analyzed from three aspects: effectiveness, system load and security. By adjusting the weight of each feature, it meets the detection requirements of different malware in the cloud environment as expected. Finally, the detection method improved the detection accuracy and generalization ability of the overall classifier using the AdaBoost ensemble learning method with Voting's combination strategy.

Deduplication eliminates duplicated data copies and reduces storage costs of cloud service providers. The twenty-fourth article, "Secure Encrypted Data Deduplication Based on Data Popularity" proposed a secure encrypted data deduplication scheme based on data popularity. Tags are calculated via bilinear mapping to determine whether different encrypted data originate from the same plaintext. Ciphertext policy attribute-based encryption is used to protect the tags. A secure key delivery scheme is designed to pass the data encryption key from an initial data uploader to subsequent uploaders via the cloud server in an offline manner. The cloud server can perform deduplication without the assistance of any online third party.

The twenty-fifth article, "Accurate and Cognitive Intrusion Detection System (ACIDS): a Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks" developed an intrusion detection system called 'Accurate and Cognitive Intrusion Detection System' (ACIDS) for detecting the most vulnerable packet dropping attack known as black hole attack. This system takes the parameters such as Destination Sequence Number (DSN) and Route Reply (RREP) into consideration for detecting the intruders by identifying the deviation of the chosen parameters from the normal behavior. The proposed system has been simulated using NS2 and the analysis of the results attest to the efficacy of ACIDS over AODV routing protocol in detecting packet dropping scenarios of the black hole attack.

Low-rate denial-of-service (LDoS) attack reduce the performance of network services by periodically sending short-term and high-pulse packets. The twenty-sixth article, "MF-CNN: a New Approach for LDoS Attack Detection Based on Multi-feature Fusion and CNN" proposed a LDoS attack detection method based on multi-feature fusion and convolution neural network(CNN). In this method, they compute a variety of network features and fuse them into a feature map, which will be used to characterize the state of the network. CNN model is an excellent classification algorithm for image recognition in the field of deep learning. It can distinguish the difference between feature maps and detect the feature maps which contain LDoS attack.

The twenty-seventh article, "Research on Intelligent Detection of Command Level Stack Pollution for Binary Program Analysis" introduced a technique for intelligently detecting the stack space and operating its readable and writable area (referred to as stack pollution). They innovatively defined the concept of "stack pollution" and raised the level of analysis from byte level to instruction level: Control flow recovery and instruction promotion based on the McSema tool. The "stack pollution" technology is a process of intelligently and intact "polluting" the required research space objects, solving the three stack space constraints by modifying SEM (semantic functions) interpretation of the instructions in the promotion process.

The last article titled "ShadowFPE: New Encrypted Web Application Solution Based on Shadow DOM" investigated efficient trust prediction in a large-scale social network. The authors proposed ShadowFPE, a novel format-preserving encryption that makes use of a robust property in Shadow DOM to obtain a feasible solution. Compared with ShadowCrypt, ShadowFPE does not destroy the data format and makes the

data usable in most of cloud web applications. They confirmed the effectiveness and security of ShadowFPE through case studies on web applications.

Acknowledgements The guest editors are thankful to our reviewers for their effort in reviewing the manuscripts. We also thank the authors of the EAI SPNCE conference for their support and MoNET journals for their support.

Zheli Liu received the BSc and MSc degrees in computer science from Jilin University, China, in 2002 and 2005, respectively. He received the PhD degree in computer application from Jilin University in 2009. After a postdoctoral fellowship in Nankai University, he joined the College of Computer and Control Engineering of Nankai University in 2011. Currently, he works at Nankai University as a Professor. His current research interests include applied cryptography and data privacy protection.

Jin Li received the BS degree inmathematics from Southwest, University, in 2002 and the PhD degree in information security from Sun Yat-sen University, in 2007. Currently, he works at Guangzhou University as a Professor. He has been selected as one of science and technology new star in Guangdong province. His research interests include applied cryptography and security in cloud computing. He has published over 50 research papers in refereed international conferences and journals and has served as the program chair or program committee member in many international conferences.

Ilsun You received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with THINmultimedia Inc., Internet Security Company Ltd., and Hanjo Engineering Company Ltd., as a Research Engineer. He is currently a Full Professor with the Department of Information Security Engineering, Soonchunhyang University. He is a Fellow of the IET. He has served or is currently serving as a General Chair or a Program Chair for international conferences and workshops, such as WISA'19–20, MobiSec'16–19, AsiaARES'13–15, MIST'09–17, MobiWorld'08–17, and so forth. He is the Editor-in-Chief of the Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). He is in the Editorial Board for Information Sciences (INS), the Journal of Network and Computer Applications (JNCA), IEEE ACCESS, Intelligent Automation & Soft Computing (AutoSoft), the International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), and the Journal of High Speed Networks (JHSN). Especially, he has focused on 4/5G security, security for wireless networks & mobile internet, IoT security, and so forth while publishing more than 180 articles in these areas

Siu-Ming Yiu received the BSc degree in computer science from the Chinese University of Hong Kong, the MS degree in computer and information science from Temple University, Philadelphia, Pennsylvania, and the PhD degree in computer science from The University of Hong Kong. He received two research output prizes, one from the department, in 2013 and one from the faculty, in 2006. He was selected for Outstanding Teaching Award by the University, in 2009, the Teaching Excellence Award in the Department in 2001, 2003, 2004, 2005, 2007, 2009, and 2010. He also received the Best Teacher Award of the Faculty of Engineering twice (2005 and 2009). Before he joined the Department as a faculty member, he has worked as an analyst programmer for a couple of years. Besides basic research, he has been involving in various industrial projects involved in quite a number of industrial projects.(Based on document published on 24 December 2019).