Agenda

IEEE Workshop "Intelligent and secure wireless communications"

July 15th, 2021 10:00 am-12:10 pm (America-Toronto Time)

	Speaker	Talk title
10:00-10:25 am	Prof. Jianting Ning	Towards Efficient Privacy-Preserving Inspection of TLS Encrypted Traffic
10:26-10:50 am	Prof. Stefano Tomasin	User authentication by received radio signals
10:51-11:05 am	Shengmin Xu	Expressive Bilateral Access Control for Internet-of-Things in Cloud-Fog Computing
11:06-11:20 am	Min Gao	Seed-based density clustering method for community detection in social networks
11:21-11:35 am	Huanchi Wang	Edge Intelligence Enabled Soft Authentication in UAV Swarm
11:36-11:50 am	Jiazhi Chen	An Efficient Trust Establishment Model for Developing Collaboration Efficiency in Internet of Vehicles
11:51-12:10 pm	Mouhamed Abdulla	Latency of Concatenating Unlicensed LPWAN with Cellular IoT: An Experimental QoE Study

IEEE Communication/Broadcasting Joint Chapter

IEEE London Section

IEEE ComSoc™ IEEE Communications Society

BTS IEEE Broadcast Technology Society

Join Zoom Meeting

https://westernuniversity.zoom.us/j/94840797738

Meeting ID: 948 4079 7738

Passcode: 643735

One tap mobile

+16699006833,,94840797738#,,,,*643735# US (San Jose)

+19292056099,,94840797738#,,,,*643735# US (New York)

Dial by your location

+1 669 900 6833 US (San Jose)

+1 929 205 6099 US (New York)

Meeting ID: 948 4079 7738

Passcode: 643735

Find your local number: https://westernuniversity.zoom.us/u/abJ7NTfNt7

Join by SIP

94840797738@zoomcrc.com

Join by H.323

162.255.37.11 (US West)

162.255.36.11 (US East)

69.174.57.160 (Canada Toronto)

65.39.152.160 (Canada Vancouver)

Meeting ID: 948 4079 7738

Passcode: 643735

10:00-10:25 am

Title: Towards Efficient Privacy-Preserving Inspection of TLS Encrypted Traffic

Abstract: Network middleboxes perform deep packet inspection to detect anomalies and suspicious activities in network traffic. However, increasingly these traffic are encrypted and middleboxes can no longer make sense of them. This raises the problem of privacy-preserving inspection on TLS encrypted traffic. In this talk, I will first introduce the need for TLS traffic inspection and the problem with the existing approach. Three recent proposals, namely Blindbox, PrivDPI and Pine, will be then introduced. Finally, I will present conclusion and future direction.

Biography: ***Jianting Ning*** received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University in 2016. He is currently a Professor with the Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, China. Previously, he was a research scientist at School of Information Systems, Singapore Management University and a research fellow at Department of Computer Science, National University of Singapore. His research interests include applied cryptography and information security. He has published papers in major conferences/journals such as ACM CCS, ESORICS, ACSAC, IEEE TIFS, IEEE TDSC, etc.

10:26-10:50 am

Title: User authentication by received radio signals

Abstract: Ensuring that a received message comes from the declared sender and has not been generated by an attacker impersonating the sender is an essential security feature, denoted authentication. Due to the growing number of connected devices with several computational and energy limitations, new authentication techniques can integrate cryptography approaches. In a wireless network, the features of the received radio signal (such as intensity, presence of echoes, and Doppler) are characteristics of the transmitter and receiver positions, and may be exploited for user authentication purposes. We will define the authentication problem by radio signal and see the main directions used to solve it, considering the specific characteristics of signal propagation.

Biography: ***Stefano Tomasin*** (Senior Member, IEEE) received the Ph.D. degree in telecommunications engineering from the University of Padua, Italy, in 2003. He is currently an Associate Professor with the University of Padua. He has been on leave at Philips Research, Eindhoven, The Netherlands, in 2002; Qualcomm Research Laboratories, San Diego, CA, USA, in 2004; Polytechnic University, Brooklyn, NY, USA, in 2007; and the Huawei Mathematical and Algorithmic Sciences Laboratory, Boulogne-Billancourt, France, in 2015. His current research interests include physical layer security and signal processing for wireless communications, with application to 5th generation cellular systems. Since 2011, he has been an Editor of the EURASIP Journal on Wireless Communications and Networking. From 2011 to 2017, he was an Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. Since 2016, he has been an Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING. Since 2020, he has been an Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

10:51-11:05 am

Title: Expressive Bilateral Access Control for Internet-of-Things in Cloud-Fog Computing

Abstract: As a versatile system architecture, cloud-fog Internet-of-Things (IoT) enables multiple resource-constrained devices to communicate and collaborate with each other. By outsourcing local data and immigrating expensive workloads to cloud service providers and fog nodes, resource-constrained devices can enjoy data services with low latency and minimal cost. To protect data security and privacy in the untrusted cloud-fog environment, many cryptographic mechanisms have been invented. Unfortunately, most of them are impractical when directly applied to cloud-fog IoT computing, mainly due to the large number of resource-constrained end-devices. In this talk, we present a secure cloud-fog IoT data sharing system with bilateral access control based on a new cryptographic tool called lightweight matchmaking encryption. This system enforces both sender access control and receiver access control simultaneously and adapts to resource-constrained end devices by outsourcing costly workloads to fog nodes.

Biography: ***Shengmin Xu*** received the Ph.D. degree in Cryptography from University of Wollongong, Australia, in 2018. He is currently a research scientist at Singapore Management University, Singapore. Previously, he was a research fellow at Singapore University of Technology and Design, Singapore. He has published over 30 research papers in top international conferences and journals, including ESORICS, ACSAC, ACM ASIACCS, IEEE TIFS, IEEE TDSC, etc. His research interests include information security, cloud computing and blockchain.

11:06-11:20 am

Title: Seed-based density clustering method for community detection in social networks

Abstract: Social networks are a kind of complex networks including individuals and their social interactions, such as online social networks (Facebook, Wechat), the collaboration network from Google Scholar. There are some research hotspots, i.e., viral marketing, community detection, and recommendation systems, in this background. We focus on the problem of community detection, and propose a seed-based density clustering method for community detection in social networks. This method combines user attributes from three perspectives to select the seed nodes and achieves a higher modularity value of the result of community division.

Biography: ***Min Gao*** received the B.S. degree in computer application technology from Anshan Normal University, China, in 2018 and the M.S. degree in computer application technology from Fujian Normal University, China, in 2019. She is now a PhD student majoring in computer architecture, with Fudan University, China. Her research interest is social computing, machine learning and malicious user detection.

11:21-11:35 am

Title: Edge Intelligence Enabled Soft Authentication in UAV Swarm

Abstract: With the increased deployment of the Unmanned Aerial Vehicles (UAVs) in both military and civilian fields, the authentication of the UAV surveillance and controlling data

becomes critical due to the severe consequences of any forged data. The conventional centralized authentication schemes suffer from the single-point failure due to the attacks initiated by the spoofing devices with high computational capability. To compensate for the challenge, the decentralized authentication scheme has been studied where no static infrastructure is required. By utilizing different authentication nodes which identifies the suspicious device from multiple angles, the difficulty for impersonating the legitimate device has been significantly increased. Despite the advantages of the decentralized authentication schemes, it increases the computational cost as well as the ambiguity for the final authentication decision if the edge authentication decision is unreliable. Hence, in this work, we utilize the physical-layer fingerprints to increase the difficulty for the attackers to impersonate the legitimate UAVs. A decentralized authentication scheme is proposed to avoid the single-point failure at the cluster head (CH) caused by the imperfect estimations. Furthermore, we propose a situational-aware authentication customization algorithm at each authentication node to compute the reliability of different attributes. Only the authentication node with reliable attributes observations will contribute to the decentralized authentication process. Moreover, a soft authentication decision algorithm, which is compatible with customized regression models at each authentication, is proposed to further improve the system robustness.

Biography: ***HUANCHI WANG*** (Graduate Student Member, IEEE) received the B.E.Sc degree major in electrical engineering from Western University, Canada, in 2019, where he is currently pursuing the M.E.Sc. degree with the Department of Electrical and Computer Engineering. His research interests include the intelligent authentication and distributed security provisioning.

11:36-11:50 am

Title: An Efficient Trust Establishment Model for Developing Collaboration Efficiency in Internet of Vehicles

Abstract: Internet of Vehicles (IoV) is an emerging technology to provide efficient and safe transportation by enabling vehicles to cooperate with each other or infrastructures through vehicle-to-everything (V2X) communications. However, cooperation among moving vehicles usually

requires complex decision-making schemes to choose cooperative vehicles for security and quality guarantee, thus leading to a long time delay, which directly reduce collaboration efficiency among vehicles. In this regard, trust among vehicles can be utilized as a lightweight decision criterion to accelerate collaboration among moving vehicles and we propose a novel trust establishment model for IoV to select best cooperative vehicles in an efficient way.

Biography: ***JIAZHI CHEN*** is currently a M.E.Sc. candidate in the Department of Electrical and Computer Engineering at Western University. Since September 2020, she has worked under the supervision of Dr. Xianbin Wang; Her research interests include network security, trust management in Vehicular Ad hoc Network (VANET), Internet of Things (IoT), and machine learning.

11:51-12:10 pm

Title: Latency of Concatenating Unlicensed LPWAN with Cellular IoT: An Experimental QoE Study

Abstract: Developing low-power wide-area network (LPWAN) solutions that are efficient to adopt, deploy and maintain are vital for smart cities. The poor quality-of-service of unlicensed LPWAN, and the high service cost of LTE-M/NB-IoT are key disadvantages of these technologies. Interfacing unlicensed with licensed LPWANs can overcome these limitations and harness their benefits. However, a concatenated LPWAN architecture will inevitably result in excess latency which may impact users' quality-of-experience (QoE). To evaluate the real-life feasibility of this system, we first propose a concatenated LPWAN architecture and experimentally measure the statistics of endto-end (E2E) latencies. The concatenated delay margin is determined by benchmarking the latencies with different LPWAN architecture schemes, namely with unlicensed IoT (standalone LoRa), cellular IoT (standalone LTE-M), and concatenated IoT (LoRa interfaced with LTE-M). Through extensive experimental measurement campaigns of 30,000 data points of E2E latencies, we show that the excess delay due to LPWAN interfacing introduces on average less than 300 milliseconds. We also found that concatenated LPWAN outperforms unlicensed IoT by roughly 1.5 seconds at the typical QoE threshold for users' satisfaction. Overall, the

experimental study suggests that a concatenated LPWAN is technically feasible and offers an affordable alternative for real-world smart city deployment. Keywords: LPWAN, Cellular IoT, Latency, QoE, Smart Cities. Link: https://arxiv.org/pdf/2105.10852.pdf

Biography: ***Mouhamed Abdulla*** is a professor of Electrical Engineering at Sheridan. Since the fall-2015 he was an EU Marie Skłodowska-Curie Individual Fellow (H2020-MSCA-IF) at Chalmers University of Technology in Sweden. In Europe, his research was funded by the European Commission and Ericsson Research Foundation. In 2017, he was a Visiting Fellow with the Dept. of Electronic Engineering of Tsinghua University in Beijing, China. Until 2015, he was an NSERC PDF with the Dept. of Electrical Engineering of the University of Québec. Before that, he worked as a Systems Engineering Researcher in the Wireless Design Laboratory of the Dept. of ECE of Concordia University. Moreover, for nearly 7 years since 2003, he was with IBM Canada Ltd. as a Senior Technical Specialist. He received, respectively in 2003, 2006, and 2012, a B.Eng. (with Distinction) in Electrical Eng., an M.Eng. in Aerospace Eng., and a Ph.D. in Electrical Eng. all at Concordia University in Montréal. Currently, he is a member of the IEEE Connected, Automated and Intelligent Vehicles Working Group mandated to draft the "IEEE P2040 Standard". He was an IEEE Executive Committee member of the Montréal Section, where he held the Secretary position in 2013 and the Treasurer in 2014-2015. Since 2020, he is appointed by IEEE Canada Board (R7) as a member of the IEEE Industry Committee with the mandate to strengthen partnership with Industry by promoting IEEE Standards on emerging technologies.