CIS-TC Newsletter

Communications and Information Security Technical Committee

http://cis.committees.comsoc.org/

Issue 2 – December 2017

cistc@comsoc.org

http://cis.committees.comsoc.org/newsletters/

Contents

Message from The Chair

I would like to wish everyone a great holiday season. As the end of the year is approaching, my term as the Chair of CIS-TC is coming to an end. I have enjoyed the privilege of working with all of you, and am happy to see our TC members attain abundant achievements in their respective research fields. My final job as chair of CIS-TC will be announcing the newly elected officers, who will take office starting in January 2018

Chair: Prof. Abderrahim Benslimane, University of Avignon, France

Vice Chair (Conference): Prof. Francesco Chiti, University of Florence, Italy

Vice Chair (Publication): Prof. Rongxing Lu, University of New Brunswick, Canada

Secretary: Prof. Bin Xiao, Hong Kong Polytechnic University, Hong Kong, China

Now, please give a warm welcome to them.

Happy New Year 2018!

Sincerely,
Xiaodong Lin
Chair of CIS-TC

Technical Recognition Award 2017

The Committee decided to give the CIS-TC Technical Recognition Award 2017 to Professor Kui Ren, University at Buffalo State University of New York (USA), for his contributions to security and privacy in cloud computing.

Prof. Ren has been awarded during the CIS-TC meeting held at ICC 2017 on May 24th, 2017 in Paris (France).

Kui Ren is SUNY Empire Innovation Professor and the director of the Ubiquitous Security and Privacy Research Laboratory (UbiSeC) in the Department of Computer Science and Engineering, University at Buffalo, State University of New York, where he joined in 2012 as an associate professor and was promoted to full professor in 2016. Previously, he has been with the Department of Electrical and Computer Engineering at Illinois Institute of Technology (IIT), where he received early tenure and promotion in five years starting 2007. He received degrees from three different majors, i.e., his Ph.D in Electrical and Computer Engineering from Worcester Polytechnic Institute, USA, in 2007, M.Eng in Materials Engineering in 2001, and B.Eng in Chemical Engineering in 1998, both from Zhejiang University, China. His current research interests include Data and Computation Outsourcing Security in the context of Cloud Computing, Wireless Systems Security in the context of Internet of Things, and Crowdsourcing-based Large-scale Data Acquisition. He has published frequently in peer-reviewed journal and conference papers. His H-index is 54, and his total citation has exceeded 19,000, according to Google Scholar (as of Aug. 2017). More than 10 of his publications have been each cited more than 600 times, with the highest exceeding 2,000. His research has also been widely covered by the media, including CBS News, Scientific American, NSF News, ACM TechNews, Science Daily, The Conversation, etc. He has delivered more than 100 keynote/invited talks at conferences and universities worldwide.

Technical Outstanding Service Award 2017

The Committee decided to give the CIS-TC Outstanding Service Award 2017 to Professor Hsiao-Hwa Chen, National Cheng Kung University (Taiwan), for his valuable and continuous contribution to our community.

Prof. Chen has been awarded during the CIS-TC meeting held at Globecom 2017 on December 6th, 2017 in Marina Bay Sands Hotel, Singapore.

Hsiao-Hwa Chen (S'89-M'91-SM'00-F'10) is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University, Taiwan. He obtained his BSc and MSc degrees from Zhejiang University, China, and a PhD degree from the University of Oulu, Finland, in 1982, 1985 and 1991, respectively. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books and more than ten book chapters in the areas of communications. He served as the general chair, TPC chair and symposium chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for numerous technical journals. He is the founding Editor-in-Chief of Wiley's Security and Communication Networks Journal. He is the recipient of the best paper award in IEEE WCNC 2008 and the recipient of IEEE 2016 Jack Neubauer Memorial Award. He served as the Editor-in-Chief for IEEE Wireless Communications from 2012 to 2015. He is a Fellow of IEEE, a Fellow of IET, and an elected Member at Large of IEEE ComSoc.

Forthcoming Meeting

The next IEEE ComSoc's Communication & Information Security TC (CISTC) meeting will be held at IEEE ICC 2018, May 20-24, 2018, Kansas City, MO, USA.

Scanning the World

"Opportunistic Networking shall not live by Routing alone"

Carlos Borrego Iglesias

dEIC - Departament d'Enginyeria de la Informació i de les Comunicacions - Universitat Autònoma de Barcelona

The Security of Networks and Distributed Applications group (SeNDA - *senda.uab.es*) from the Department of Information and Communications Engineering (dEIC - d*eic.uab.es)* is a teaching and research department within the Universitat Autònoma de Barcelona (*uab.es*). The **research** undertaken by the SeNDA group is focussed on

all aspects of **network** and distributed application **security**. Medical emergency situations and intelligent transport systems are the main scenarios the group is using for applied research, responding to current **society's needs.**

Among the different research topic the SeNDA group is interested in, the most challenging one is **Opportunistic Networking** (OppNet), a network paradigm where mobile nodes communicate with each other even when there is no end-to-end connectivity between them.

One of the most ardous and researched topics on OppNet is **routing**. Routing protocols designed to operate in DTN scenarios usually generate and use information about node behaviors, as the historic of contacts established with each other node. Then, they share this information with neighbours in order to improve the decision making. In some cases, a node is linked to a person. Therefore, the information that routing protocols use and share can be seen as private information about people's whereabouts or frequent behaviors. The more accurate and sensitive this information is, the more useful it is for the routing protocol and the more important is to protect its privacy. At SeNDA, we have developed different routing protocols like [1] that make use of **homomorphic encryption techniques** to preserve nodes' privacy.

However, **OppNet shall not live by routing alone.** We believe that in OppNet there are some other issues **as important as routing**. For example, available destination addresses are not always known by the sending applications. Profile-based network models, where the destination of a message is not identified by a network/transport address, are very useful in OppNet. In this case, applications send messages to nodes belonging to a profile defined by one or more **attributes** rather than to specific addresses.

However, there are strong limitations in OppNet profile-casting. In particular, there is no current way of representing profiles defined by delivery functions such as *best*, *maximum*, *over-the-average* or *k-best*. We call these profiles **relative profiles** [2]: nodes belong to these relative profiles taking into account not only attributes from the very same node but also relative to others from the same profile.

Nonetheless, this relative delivery decision is a complex task to perform. The reason for this is that intermittently connected OppNet nodes do not have access to the state of the network with regard to the attributes that define these relative profiles. **Broadcasting** messages to query the state of these attributes can be **inaccurate** and slow because of the characteristics of the network. Instead, sending **single** messages to the network to explore the network and afterwards deliver the message will imply a new problem: the problem of deciding **when to stop** exploring the network. Additionally, we have defined **Explore and Wait** [3], a composite routing-delivery scheme that uses **optimal stopping** theory-based delivery strategies.

At SeNDA we are developing *aDTN* [4], an OppNet **platform based on mobile code** that implements all of the network protocols above described.

References

[1] Sánchez-Carmona, Adrián, Sergi Robles, and Carlos Borrego. "PrivHab+: A secure geographic routing protocol for DTN." *Computer Communications* 78 (2016): 56-73.

[2] Borrego, Carlos, Gerard Garcia, and Sergi Robles. "Softwarecast: A code-based delivery Manycast scheme in heterogeneous and Opportunistic Ad Hoc Networks." *Ad Hoc Networks* 55 (2017): 72-86.

[3] Borrego, Carlos, Adrián Sánchez-Carmona, Zhiyuan Li, and Sergi Robles. "Explore and wait: A composite routing-delivery scheme for relative profile-casting in opportunistic networks." *Computer Networks* 123 (2017): 51-63.

[4] Borrego, Carlos, Sergi Robles, Angela Fabregues, and Adrián Sánchez-Carmona. "A mobile code bundle extension for application-defined routing in delay and disruption tolerant networking." *Computer Networks* 87 (2015): 59-77.

Contact

If you are interested on these topics, for research proposals or PhD candidates stays, please contact us at carlos.borrego@uab.cat

FEATURED TOPICS

"Network and Communication Security in Intelligent Connected Vehicular Systems"

Yiliang Liu[1] and Hsiao-Hwa Chen[2]

[1]Communications Research Center, Harbin Institute of Technology, China

[2]Department of Engineering Science, National Cheng Kung University, Taiwan

Intelligent connected vehicular (ICV) systems are implemented using sensors, automotive controllers, and other components based on advanced network and communication technologies, where the vehicles can exchange driving information with each other via both in-vehicle and out-vehicle network and communications technologies. ICV is one of the most fundamental units in autonomous vehicles, and it provides the automotive industry with a strategic opportunity for its transformation to fit in the future artificial intelligence (AI) based society.

In the development of ICV systems, different regions in the world may take somehow different approaches. For instance, USA and China adopted different paths for their car industries. The US Department of Transportation supports for automated roads based on DSRC (which works in a 75 MHz bandwidth in 5.85 - 5.925 GHz bands), which uses vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) techniques to provide safety road and value-added services. The Chinese government (as shown in its "Made-in-China 2025" road map) is promoting an intelligent connected vehicle system project that focuses on automated vehicles based on 5G cellular networks (i.e., LTE-V), where the ICV network and communication systems are implemented for driver-assist information exchange through vehicular on-board devices, networks, and clouds.

The ICV network and communication systems support information interoperability and connectivity, which is a critical component to achieve intelligent traffic management, intelligent dynamic information services, and vehicle intelligent control. Under 5G system infra-structure, device-to-device (D2D), machine-to-machine (M2M), new multiple access, massive MIMO technologies, and so on, are used for enhancing the performance of ICV network and communication systems. The information security of this system attracts a lot of attention due to the security risks in ICV network and communication systems, which may create serious consequences, such as traffic accidents, property loss, and driver casualties. Therefore, security is an extremely critical issue in the implementation of ICV systems.

We have been working in security of ICV systems for several years. In our previous works, we designed a prototype of ICV communication devices, which integrates various physical layer standards, such as Wi-Fi, WCDMA, DSRC, and GPS, into one on-board unit. The prototype can perform simple communication functions, but it does not support network and security protocols. In secure ICV communication research, we presented a proxy based authentication scheme [1] that makes use of vehicle's computational capabilities to increase vehicle authentication speeds. However, this cryptograph-based scheme is a time-consuming process and may fail to satisfy computational efficiency requirement in large-scale vehicular networks under 5G cellular systems. We also proactively studied some physical layer security schemes to use secure channels in wireless networks, such as an artificial noise-assisted MIMO technology [2] and a convex optimization-assisted relay technology [3]. These physical layer security investigations were independent without considering dynamic traffic patterns and system access capabilities. In terms of cloud security, we proposed an efficient and secure data de-duplication scheme [4] to support data upload confidentiality and dynamic ownership management.

Information security risks in ICV network and communication systems mainly include hardware intrusions, eavesdroppers, identification of theft/unauthorized accesses, and cloud service hacks. Especially, at hardware level, data storage security and access control are critical in on-board devices. However, the existing automobile electronic devices are unable to be re-designed for ICV security purposes. Hence, ICV hardware needs security protection of in-vehicle networks via multi-level security design of device configurations and interfaces. At the communication level, the physical layer channels are limited if using existing DSRC-based VANET technologies. In addition, cryptographic algorithms bring in much delay in the channels. D2D technologies of 5G networks are promising to provide large-scale communication interfaces and can also achieve security and short-delay communications via physical layer security. At the network level, the coexistence of heterogeneous networks and across-domain movement of vehicles are inconvenient for vehicle's control access and identity management. A uniform license-based identity authentication system is required to prevent across-domain forged identity attacks and unauthorized access. At the cloud service level, it is difficult to formalize a trusted vehicle-cloud security framework because vehicle-cloud services are diversified and decentralized, such that it is necessary to carry out a security collaborative format description of secure vehicle-cloud services, and then propose a scalable security service architecture and corresponding technologies. Besides, the attacks in ICV systems are mainly to illegally intrude and control vehicles rather than eavesdrop vehicular messages and data. Thus, the security framework should be established along with the streams of driver-assisted information.

To summarize, the main objective of ICV network and communication systems is to provide driver-assist information exchange among vehicles, pedestrians, and traffic managers. In addition, the ICV systems are required to offer secure interfaces for large-scale vehicle access. At the present, vehicular networking is evolving from informatization (for interconnections and communications) to intelligence (via cloud platforms, big data and artificial intelligence), which promotes the functional requirements of information security. We must pay enough attention to multi-domain (device-network-cloud) intelligent information security of vehicles rather than roadside information confidentiality and vehicle identity authentication. Specifically, the future research works include mainly five-fold as listed in the sequel. 1) The on-board unit security of vehicles should be designed independently without changing the existing automotive electronic systems. 2) A secure D2D-based ICV technology provides secure communication interfaces to realize short-range V2V communications. 3) Across-domain proxy and lightweight authentication algorithm is an effective way for bridging the gap between clouds and vehicles. 4) Cloud access control and secure vehicle-cloud computing should be provided to deal with security risks of comprehensive intelligent services. 5) A global framework with cross-level misbehavior detection and intrusion detection mechanisms is important for the protection of ICV communication security.

References

[1] Y. L. Liu, L. M. Wang, and H. H. Chen, "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 64, no.8, pp. 3697-3710, 2015.

[2] Y. L. Liu, H. H. Chen, and L. M. Wang, "Secrecy Capacity Analysis of Artificial Noisy MIMO Channels – an Approach Based on Ordered Eigenvalues of Wishart Matrices," IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, March 2017.

[3] P. Zhang, Y. L. Liu, J. M. Zhang, and L. M. Wang, "Power Allocation Design and Optimization for Secure Transmission in Cognitive Relay Networks," Security and Communication Networks, vol. 9, no. 18, pp. 5133-5142, Dec. 2016.

[4] S. R. Jiang, T. Jiang, and L. M. Wang, "Secure and Efficient Cloud Data Deduplication with Ownership Management," Accepted in IEEE Transaction on Services Computing, 2017.