Security Analysis of Social Networking Based Authentication in Infrastructureless PAC Networks

Nhu-Ngoc Dao and Sungrae Cho

***Abstract*—IEEE 802.15.8 standard defines specifications and characteristics of infrastructureless peer-aware communications (PACs) with fully coordination in an ad hoc environment. The PAC aims at supporting social connectivity for broad types of PAC devices, especially lightweight Internet of things. Since no coordinator exists in the PAC, security is considered as one of the main challenges for a successful communication between PAC devices. In this status quo, social networking based authentication (SNAuth) protocol proved its advances by supporting multi-security levels for diverse PAC devices. In this paper, we conduct a comprehensive security analysis of SNAuth protocol in order to provide a convenient reference for PAC users to select appropriate SNAuth configuration based on their demands.**

***Index Terms*—Security analysis, social networking based authentication, peer-aware communications.**

I. Introduction

The emerging Internet-of-Everything (IoE) paradigm has been characterized by a tremendous number of mobile equipments interconnected together through heterogeneous access mediums and technologies. Although the next-generation mobile networks, 5G, introduce a promising infrastructure for diverse IoE communications [1], [2], peer-to-peer networking remains its important role to compensate into various scenarios wherein the 5G infrastructure is unavailable and/or unnecessary, such as network overload, ultra-dense communications, local position-aware advertisements, and hazard notifications [3]. These scenarios are considered to be infrastructureless peer-aware communications (PACs) defined by the IEEE 802.15.8 standard [4], [5], which allow user devices to interconnect each other directly; see Fig. 1. Since no coordinator exists in the PAC networks, security is a serious problem. Moreover, multi-security-level support is required due to the broad diversity of PD applications and performances. It is worth noting that the infrastructureless and fully distributed coordinations are not comprehensively supported by the existing technologies (e.g., ProSe, WiFi Direct, Bluetooth, and ZigBee [6]).

Although a variety of effective security algorithms have been proposed in the literature, almost all of them are inapplicable to PAC since they are generally operated by a central entity such as an authentication server and an eNodeB coordinator; refer to [7], [8] for detailed surveys. It is widely recognized that three potential security approaches can be utilized in PAC networks, including (*i*) physical/direct key sharing among PDs' owners, (*ii*) physical (PHY) layer key generation based on the reciprocity and randomness of wireless fading channels, and (*iii*) the well-known Diffie-Hellman (D-H) key exchange protocols as well as their variants [9], [10]. Unfortunately, these existing algorithms mainly focus on the secret key agreement procedure without strictly considering PD characteristics. Moreover, the support of multi-level security levels has not been considered. These omissions might cause PAC to be vulnerable against recent attacks.

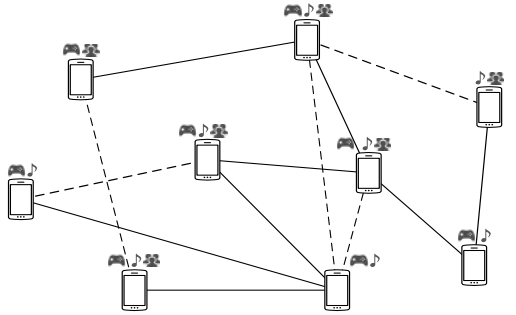

Fig. 1. Infrastructureless peer-aware communication networks [4].

To overcome these aforementioned challenges, a social networking based authentication protocol, namely SNAuth, has been proposed in [11]. The SNAuth protocol exploits the social networking feature of the PAC network to develop session key for PD communications. The PDs build their session key by using partial keys that are generated and delivered from a selected list of common neighbors of the PDs. The number of used partial keys determines the complexity of session key generation and the security levels. Larger number of partial keys are used, more secure PAC achieves, and vice versa.

Although the SNAuth protocol is potential and appropriate for diverse PDs, a comprehensive security analysis is needed to provide a convenient reference for PAC users to select appropriate SNAuth configuration based on their demands. In this paper, the SNAuth security performances are evaluated by adjusting the impacts of (*i*) the number of partial keys used, (*ii*) the number of possible eavesdropping devices, and (*iii*) the density of PDs in the networks. Finally, a reference table is developed for appropriate selection of the number of partial keys depending on a given security level.

Manuscript received September 15, 2018; revised January 27, 2019. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1A2B4009802).

The authors are with the School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, South Korea (e-mail: srcho@cau.ac.kr).

doi: 10.18178/ijfcc.2019.8.1.530

TABLE I: PRIME EXAMPLES OF PAC SERVICES AND THEIR SECURITY REQUIREMENTS [11]

Category	PAC services	Typical PDs	Security
User-centric services	Smart home, personalized tour guidance	Home appliances, kiosks	Data confidence, connection authentication
Local social services	Local gaming, content exchange	Smartphones, laptops	Data integrity, connection authentication
Advertisement	Commercial broadcast, pull-type advertisements	Smartphones, kiosks	Data integrity
Smart transportation	Traffic events, navigation assistant	In vehicle infotainment systems, smartphones	Multi-level security
Smart city	Tour information, local policy auto-instruction	Kiosks, smartphones	Multi-level security
Public safety	Hazard notification, public emergency	Smartphone, alarm systems	Multi-level security

II. PAC Security Challenge Analysis

A. Infrastructureless PAC Characteristics

As mentioned earlier in Section I, PAC networking supplements 5G communications with infrastructureless peer-to-peer communication supports, in which the PDs directly communicate with one another. Despite the diversity of the envisioned PAC services (see Table 1), their communications share the following common characteristics:

Fully distributed coordination: Since the PDs themselves manage all communication processes including synchronization, discovery, association, authentication, and channel access as well as wireless resource management and scheduling, equal roles are assigned to all PDs regardless of their performances and locations.

Infrastructureless architecture: In the PAC, all PDs directly communicate with another without the supervision of management and control entities. In other words, PDs play the roles of both client/server in service delivery and forwarding nodes in the network model; meanwhile, the PD connections form the links. No intermediate operator's equipment participates in the communications.

Mobile multi-hop support: Without networking infrastructure, the PDs require the mobile multi-hop feature to maintain their peer-to-peer communications connectivity over wireless interfaces among PDs in dense and scalable environments.

Diversity of PD performances and services: Table 1 summarizes the PAC services and their corresponding typical PDs. The performances of the PDs broadly stretch from IoE terminals (e.g., home appliances, information kiosks, and machinery) to high-power devices (e.g., smartphones, laptops, and portable servers [12], [13]). Accordingly, the PAC services require various communications features such as data rate, reliability, latency, and security level.

B. Security Problem Statement

Due to the PAC characteristics, although a variety of effective security algorithms have been proposed in the literature, three applicable security approaches show promise for PAC including physical/direct key sharing, PHY layer key generation, and the D-H key exchange protocol as well as their variants. These approaches are analyzed as follows.

Physical/direct key sharing: Historically, this straightforward key sharing approach is a traditional method where common pre-defined secret keys are exchanged via human negotiation activities (e.g., preinstallation on both devices, messaging, and physical meeting). One prime example of this approach is the personal identification number (PIN) based scheme. Although the PIN-based scheme has insignificant overhead in key generation and authentication, it is known to be vulnerable against various popular attacks, such as secret key guessing, stealing, spoofing, eavesdropping, and jamming. Moreover, the PIN materials have to be manually installed into the applications or devices for use.

PHY layer key generation: This method exploits the reciprocity and randomness of the fading occurring on the wireless channels operated between two devices [14]. Although the PHY-based method shows a potential secret key generation for PAC, its inadequate protection against eavesdropping and jamming attacks remains an open issue [15].

D-H key exchange protocols: The D-H protocols enable two devices to securely generate a common secret key by exchanging some open materials over an insecure channel [16]. The success of the D-H protocol has been proved in many variants in the literature during the last decades [17]-[19]. However, the D-H protocols cannot provide certification ability for ensuring authorization and privacy.

In summary, due to the strict constraint of infrastructureless and fully distributed coordination, PAC currently faces security problems in terms of authorization, privacy, and multi-security level dynamics, which remain unresolved by the existing approaches.

C. Criteria for Security in PAC network

No central management entity: The fully distributed coordination implies that there is no central management entity for security procedures.

Authentication, authorization, and privacy: As analyzed in Section II-B, the infrastructureless property makes PAC vulnerable against authority and privacy issues due to lack of PD identification.

Multi-security level support: This criterion is directly derived from the diversity of PAC services and PD performances.

III. SNAuth Protocol Overview

Operation of the SNAuth protocol is illustrated in Fig. 2. Detailed descriptions and examples are thoroughly introduced in [11]. In the scope of this paper, we summarize the SNAuth operation in two main stages: (*i*) Authentication delegation and (*ii*) Session key agreement. Let I-PD, R-PD, and C-PD denote the initiator-PD, responder-PD, and

common neighboring PDs of both I-PD and R-PD, respectively. In the authentication delegation stage, an I-PD initially requests connection to a R-PD. The R-PD multicasts an invitation message to a number of its neighboring PDs in order to find a list of common PDs with the I-PD. Acknowledgement messages are voluntarily returned from the neighboring PDs. Based on the received messages, the R-PD selects k C-PDs to delegate the authentication with the I-PD.

In the session key agreement stage, k C-PDs independently arranges k partial keys with the I-PD. These partial keys are, then, delivered to the R-PD. Based on the common set of partial keys, the I-PD and R-PD generate a session key by itself. Afterward, the session key is used to encrypt messages transferred between I-PD and R-PD securely.

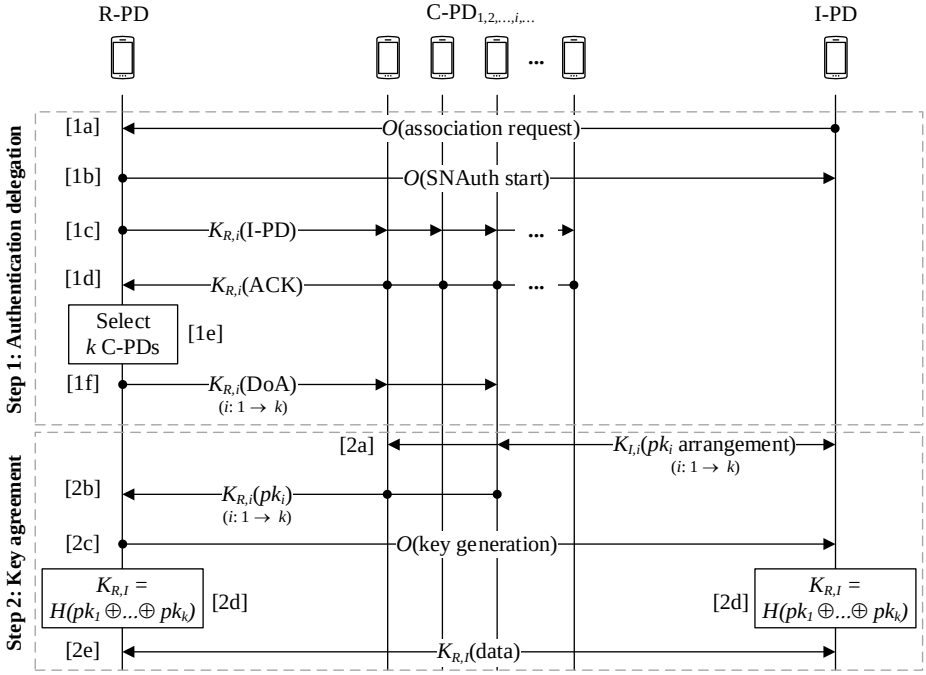

Fig. 2. Operation of the SNAuth protocol between two PDs [11].

IV. Security Analysis

Since the SNAuth protocol uses partial keys issued by intermediate C-PDs to generate the session key, these partial keys might be eavesdropped by attackers in the medium. As described in [11], the probability $P(k)$ that the attackers can capture all of k partial keys is given by

$$P(k)=\sum_{i=k}^{S}\sum_{j=k}^{i}\frac{\binom{S}{i}\binom{\frac{N}{2}S-S}{S-i}}{\binom{\frac{N}{2}S}{S}}\frac{\binom{i}{j}\binom{\frac{N}{2}S-i}{mS-j}}{\binom{\frac{N}{2}S}{mS}} \quad (1)$$

where N, S, and m are the number of PDs, the average number of concurrent communication sessions of a PD, and the number of PDs that the attackers have, respectively. The security level (X) is defined by the probability that the attackers cannot overheard all of k partial keys, i.e., cannot generate the session key successfully. The security level is given by

$$X=1-P(k), \quad (2)$$

It is seen that the security level X is directly proportional to N, S, and k, while the X is inversely proportional to m.

Following the environmental assumption in [11], S is given by $0.8 + 0.45N$. In order to investigate the effects of N, k, and m on the security levels, we develop reference tables indicating the eavesdropping probability depending on various values of k and m while N is set to be in {100, 200, 300, 400, 500}. The total results are provided in Appendix A. Fig. 3 depicts the eavesdropping probability $P(k)$ within a PAC network of 500 PDs (N = 500). It is observed that the eavesdropping probability exponentially decreases when the number of partial keys increases. Meanwhile, an increase of m results in a linear increase of $P(k)$. Accordingly, the security level has inverse behavior to k and m compared to the eavesdropping probability's, respectively. Fig. 4 illustrates the eavesdropping probability within various PAC network densities (i.e., N is adjusted). It is seen that a higher PAC network density results in a lower eavesdropping probability and, therefore, a higher security level.

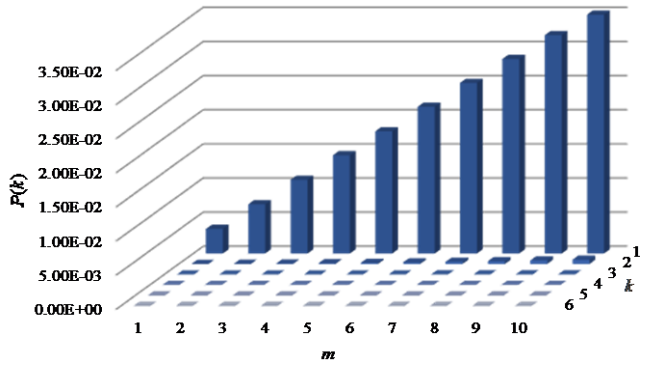

Fig. 3. Eavesdropping probability $P(k)$ within a PAC network of 500 PDs (N = 500).

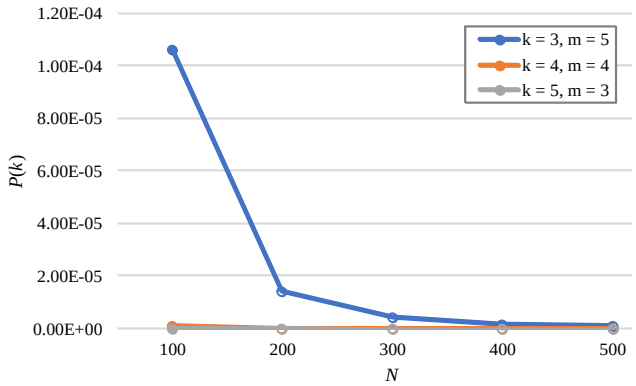

Fig. 4. Eavesdropping probability $P(k)$ within various PAC network densities.

Detailed numerous eavesdropping probability tables (i.e., Tables 2-6) within a variety of environmental configurations in PAC networks in Appendix give convenient reference views for PDs to select their appropriate SNAuth parameters in order to satisfying the security demands.

TABLE II: EAVESDROPPING PROBABILITY WITH N = 100

m	k					
	1	2	3	4	5	6
1	1.82e-02	1.57e-04	8.43e-07	3.18e-09	8.93e-12	1.95e-14
2	3.62e-02	6.28e-04	6.89e-06	5.37e-08	3.17e-10	1.47e-12
3	5.38e-02	1.40e-03	2.32e-05	2.75e-07	2.46e-09	1.75e-11
4	7.11e-02	2.47e-03	5.47e-05	8.67e-07	1.05e-08	9.96e-11
5	8.81e-02	3.82e-03	1.06e-04	2.11e-06	3.19e-08	3.82e-10
6	1.08e-01	5.44e-03	1.81e-04	4.33e-06	7.89e-08	1.14e-09
7	1.21e-01	7.33e-03	2.85e-04	7.95e-06	1.69e-07	2.86e-09
8	1.37e-01	9.47e-03	4.21e-04	1.34e-05	3.27e-07	6.33e-09
9	1.53e-01	1.19e-02	5.92e-04	2.13e-05	5.84e-07	1.27e-08
10	1.69e-01	1.45e-02	8.03e-04	3.21e-05	9.80e-07	2.38e-08

TABLE III: EAVESDROPPING PROBABILITY WITH N = 200

m	k					
	1	2	3	4	5	6
1	9.06e-03	3.98e-05	1.13e-07	2.33e-10	3.70e-13	4.75e-16
2	1.80e-02	1.59e-04	9.14e-07	3.82e-09	1.25e-11	3.28e-14
3	2.69e-02	3.57e-04	3.08e-06	1.94e-08	9.57e-11	3.82e-13
4	3.58e-02	6.32e-04	7.28e-06	6.14e-08	4.04e-10	2.16e-12
5	4.45e-02	9.82e-04	1.41e-05	1.49e-07	1.23e-09	8.26e-12
6	5.32e-02	1.41e-03	2.43e-05	3.08e-07	3.06e-09	2.46e-11
7	6.18e-02	1.90e-03	3.84e-05	5.68e-07	6.58e-09	6.19e-11
8	7.03e-02	2.47e-03	5.70e-05	9.64e-07	1.28e-08	1.37e-10
9	7.87e-02	3.11e-03	8.07e-05	1.54e-06	2.29e-08	2.77e-10
10	8.71e-02	3.82e-03	1.10e-04	2.33e-06	3.85e-08	5.20e-10

TABLE IV: EAVESDROPPING PROBABILITY WITH N = 300

m	k					
	1	2	3	4	5	6
1	6.03e-03	1.78e-05	3.43e-08	4.85e-11	5.36e-14	4.83e-17
2	1.20e-02	7.12e-05	2.76e-07	7.90e-10	1.77e-12	3.25e-15
3	1.80e-02	1.60e-04	9.32e-07	4.01e-09	1.36e-11	3.76e-14
4	2.39e-02	2.83e-04	2.20e-06	1.27e-08	5.72e-11	2.12e-13
5	2.98e-02	4.41e-04	4.29e-06	3.08e-08	1.75e-10	8.10e-13
6	3.56e-02	6.32e-04	7.39e-06	6.37e-08	4.33e-10	2.42e-12
7	4.14e-02	8.57e-04	1.17e-05	1.18e-07	9.34e-10	6.08e-12
8	4.72e-02	1.12e-03	1.74e-05	2.00e-07	1.81e-09	1.35e-11
9	5.30e-02	1.41e-03	2.46e-05	3.19e-07	3.26e-09	2.73e-11
10	5.87e-02	1.73e-03	3.37e-05	4.84e-07	5.50e-09	5.12e-11

TABLE V: EAVESDROPPING PROBABILITY WITH N = 400

m	k					
	1	2	3	4	5	6
1	4.51e-03	1.00e-05	1.46e-08	1.58e-11	1.33e-14	9.25e-18
2	9.01e-03	4.02e-05	1.18e-07	2.55e-10	4.37e-13	6.15e-16
3	1.35e-02	9.02e-05	3.97e-07	1.30e-09	3.34e-12	7.08e-15
4	1.79e-02	1.60e-04	9.40e-07	4.09e-09	1.41e-11	3.99e-14
5	2.34e-02	2.49e-04	1.83e-06	9.98e-09	4.30e-11	1.52e-13
6	2.68e-02	3.58e-04	3.16e-06	2.06e-08	1.07e-10	4.54e-13
7	3.12e-02	4.86e-04	5.00e-06	3.81e-08	2.30e-10	1.14e-12
8	3.56e-02	6.33e-04	7.44e-06	6.49e-08	4.48e-10	2.54e-12
9	3.99e-02	7.98e-04	1.06e-05	1.04e-07	8.04e-10	5.14e-12
10	4.43e-02	9.83e-04	1.44e-05	1.57e-07	1.39e-09	9.65e-12

TABLE VI: EAVESDROPPING PROBABILITY WITH N = 500

m	k					
	1	2	3	4	5	6
1	3.61e-03	6.44e-06	7.55e-09	6.56e-12	4.50e-15	2.53e-18
2	7.21e-03	2.57e-05	6.07e-08	1.06e-10	1.47e-13	1.67e-16
3	1.08e-02	5.78e-05	2.05e-07	5.38e-10	1.12e-12	1.92e-15
4	1.44e-02	1.03e-04	4.84e-07	1.70e-09	4.72e-12	1.08e-14
5	1.79e-02	1.60e-04	9.44e-07	4.14e-09	1.44e-11	4.13e-14
6	2.15e-02	2.30e-04	1.63e-06	8.57e-09	3.58e-11	1.23e-13
7	2.50e-02	3.12e-04	2.58e-06	1.58e-08	7.72e-11	3.10e-13
8	2.85e-02	4.07e-04	3.84e-06	2.70e-08	1.50e-10	6.09e-13
9	3.20e-02	5.14e-04	5.45e-06	4.31e-08	2.70e-10	1.40e-12
10	3.55e-02	6.33e-04	7.46e-06	6.55e-08	4.56e-10	2.62e-12

V. CONCLUSIONS

This paper provides reference tables of eavesdropping probability against the SNAuth protocol within various environmental configurations of the PAC networks. The eavesdropping probability is evaluated by adjusting three key factors including the number of partial keys used, the number of possible eavesdropping devices, and the density of PDs in the networks. Future works should provide suggestion of SNAuth configurations for the PDs according to the requirements of security level dynamically.

REFERENCES

[1] N.-N. Dao, M. Park, J. Kim, and S. Cho, "Adaptive MCS selection and resource planning for energy-efficient communication in LTE-M based IoT sensing platform," *PLoS One*, vol. 12, 2017.

[2] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, *et al.*, "Scenarios for 5G mobile and wireless communications: The vision of the METIS project," *IEEE Communications Magazine*, vol. 52, pp. 26-35, 2014.

[3] N.-N. Dao, M. Park, J. Kim, J. Paek, and S. Cho, "Resource-aware relay selection for inter-cell interference avoidance in 5G heterogeneous network for internet of things systems," *Future Generation Computer Systems*, vol. 93, pp. 877-887, 2018.

[4] *802.15.8-2007—IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Peer Aware Communications (PAC)*, IEEE Standard 802.15.8-2017.

[5] W. Na, Y. Lee, J. Yoon, J. Park, and S. Cho, "Fully distributed multicast routing protocol for IEEE 802.15.8 peer-aware communication," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, 2015.

[6] D. Feng, L. Lu, Y. Yuan-Wu, G. Li, S. Li, and G. Feng, "Device-to-device communications in cellular networks," *IEEE Communications Magazine*, vol. 52, pp. 49-55, 2014.

[7] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, pp. 1250-1258, 2017.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

[9] Y. Kim, N.-N. Dao, J. Lee, and S. Cho, "Trend analyses of authentication in peer aware communication (PAC)," in *Proc. of the 9th International Conference on Ubiquitous and Future Networks (ICUFN)*, 2017, pp. 1053-1055.
[10] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Networks and Applications*, vol. 22, pp. 195-208, 2017.
[11] N.-N. Dao, Y. Kim, S. Jeong, M. Park, and S. Cho, "Achievable multi-security levels for lightweight IoT-enabled devices in infrastructureless peer-aware communications," *IEEE Access*, vol. 5, pp. 26743-26753, 2017.
[12] C. Lee, L. Park, and S. Cho, "Light-weight stackelberg game theoretic demand response scheme for massive smart manufacturing systems," *IEEE Access*, vol. 6, pp. 23316-23324, 2018.
[13] W. Na, J. Park, C. Lee, K. Park, J. Kim, and S. Cho, "Energy-efficient mobile charging for wireless power transfer in internet of things networks," *IEEE Internet of Things Journal*, vol. 5, pp. 79-92, 2018.
[14] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Communications Magazine*, vol. 53, pp. 33-39, 2015.
[15] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Transactions on Networking*, vol. 20, pp. 1440-1451, 2012.
[16] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644-654, 1976.
[17] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proc. of the 3rd ACM Conference on Computer and Communications Security*, 1996, pp. 31-37.
[18] P. Subramaniam and A. Parakh, "A quantum Diffie-Hellman protocol," *International Journal of Security and Networks*, vol. 11, pp. 213-223, 2016.
[19] N.-N. Dao, W. Na, Y. Lee, D.-N. Vu, and S. Cho, "Prefetched asymmetric authentication for infrastructureless D2D communications: Feasibility study and analysis," in *Proc. of IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 2018.

Nhu-Ngoc Dao received the B.S. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology, Viet Nam, in 2009, and the M.S. degree in computer science from Chung-Ang University, South Korea, in 2016, where he is currently pursuing the Ph.D. degree in computer science. His research interests include network security, network softwarization, fog/edge computing, and Internet of Things.

Sungrae Cho is a professor with the School of Computer Science and Engineering, Chung-Ang University (CAU), Seoul. Prior to joining CAU, he was an assistant professor with the Department of Computer Sciences, Georgia Southern University, Statesboro, GA, USA, from 2003 to 2006, and a senior member of technical staff with the Samsung Advanced Institute of Technology (SAIT), Kiheung, South Korea, in 2003. From 1994 to 1996, he was a research staff member with Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. From 2012 to 2013, he held a visiting professorship with the National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA. He received the B.S. and M.S. degrees in electronics engineering from Korea University, Seoul, South Korea, in 1992 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2002.

His current research interests include wireless networking, ubiquitous computing, and ICT convergence. He was an editor of Ad Hoc Networks Journal (Elsevier) from 2012 to 2017. He has served numerous international conferences as an organizing committee chair, such as IEEE SECON, ICOIN, ICTC, ICUFN, TridentCom, and the IEEE MASS, and as a program committee member, such as IEEE ICC, MobiApps, SENSORNETS, and WINSYS.