Received October 23, 2017, accepted November 20, 2017, date of publication November 24, 2017,
date of current version December 22, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2777443

Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in Infrastructureless Peer-Aware Communications

NHU-NGOC DAO[1], YONGHUN KIM[1], SEOHYEON JEONG[1], MINHO PARK[2], (Member, IEEE), AND SUNGRAE CHO[1]

[1]School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, South Korea
[2]Department of ICMC Convergence Technology, Soongsil University, Seoul 06978, South Korea

Corresponding authors: Minho Park (mhp@ssu.ac.kr) and Sungrae Cho (srcho@cau.ac.kr)

This work was supported in part by the Chung-Ang University Graduate Research Scholarship in 2017 and in part by the Ministry of Science, ICT, and Future Planning, South Korea, under the Information Technology Research Center Support Program supervised by the Institute for Information and Communications Technology Promotion under Grant IITP-2017-2012-0-00559.

ABSTRACT The emergence of social networking and proximity services is driving the Internet-of-Things (IoT) paradigms toward a location-aware connecting society. To prepare for such a booming paradigm, IEEE 802.15.8 standardizes peer-aware communication (PAC) within the strict consideration of infrastructureless property and fully distributed coordination features. Since no central entity exists in a PAC network for control and management purposes, every PAC device (PD) plays an equal role in terms of communication. This situation leads to a variety of security challenges, especially in authentication and key agreement for lightweight IoT-enabled PDs. Recently, there are some proposals aimed at the aforementioned problems, such as approaches with personal identification number, physical layer features. However, due to its inconvenience and computational complexity for the lightweight IoT-enabled PDs, authentication and key agreement are still open issues in PAC. From this view, this paper proposes a new approach that utilizes social networking features closely tied to the PAC in order to support authentication and key agreement procedures. A number of trusted PDs are delegated to authenticate the requesting PD on behalf of the requested PD when an association is established between them. Intensive analysis and evaluation show that the proposed protocol provides multiple security levels as well as user convenience with reasonable resource consumption.

INDEX TERMS Multi-security level, infrastructureless peer-aware communication, social networking, lightweight device.

I. INTRODUCTION

In recent decades, mobile social networks and proximity services, wherein geographical proximate devices interact each other through wireless communications, have gained tremendous attentions due to the popularity of smart devices. Since these two services aim at improving interpersonal relationships, location awareness is vitally important to improve user satisfaction [1], [2]. The applications of mobile social networks and proximity services are characterized by their diversity [3]–[6] including infotainment, smart environments, transportation assistance, navigation, monitoring of surroundings, local notifications and alarms, etc., wherein lightweight IoT-enabled devices increasingly introduce its crucial positions.

Table 1 shows prime examples of the IoT-assisted services as reported by IEEE 802.15 TG8 in the technical document of PAC applications [7]. Besides the fact that the broad availability of communication infrastructure (e.g., cellular networks) significantly contributes to the promising success of the aforementioned services [8], [9], fully distributed peer-to-peer (P2P) communication is also indispensable, which facilitates seamless conversation between user terminals in opposing conditions when infrastructure is not needed or is unavailable. For instance, local P2P communications among residential appliances in smart home network help reducing transmission latency and overhead, environmental sensory navigation and guidance based on P2P communications are helpful in natural disasters where public

TABLE 1. Prime examples of IoT-assisted application in PAC network [7].

Category	Application	Data security/ Association security
User-centric services	Elder assistant, smart home	Confidence/Authentication
Advertisement	Personalized advertisements	Integrity/Authentication
Advertisement	Commercial broadcast, pull-type advertisements	Integrity/None
Smart transportation	Traffic events, sensory navigation assistant	Varies/Varies
Smart city	Tour information, local policy auto-instruction	Varies/None
Public safety	Hazard notification, public emergency	Varies/None

communication infrastructure is destroyed, and local information kiosks notify tourists about restricted areas as well as points-of-interest in their proximity.

A. RESEARCH MOTIVATION

Although support for P2P communication has been featured in numerous technologies such as ProSe, WiFi Direct, Bluetooth, and ZigBee [10], a strict consideration of fully infrastructureless and distributed coordination in peer-aware communication (PAC) is still not completely taken into account. Dealing with this situation, IEEE started the 802.15.8 project on March 2012 in order to standardize criteria and technologies for PAC within one identical specification body. IEEE 802.15.8 PAC defines physical (PHY) and medium access control (MAC) mechanisms, providing a scalable and secure peer-aware environment where participating devices directly synchronize, discover, associate, and simultaneously communicate with each other within multi-hop support [11]. Since no central entity is used for control and management purposes, stability and security are big challenges for a dense PAC network (PACNET).

Unfortunately, various effective security algorithms are inapplicable to PAC since they generally require a central entity such as an authentication server. In the IEEE 802.15.8, feasible approaches which have been considered as the best candidates in terms of authentication and key agreement [12], [13] include the personal identification number (PIN) based [14] and physical (PHY) layer features based [15] methods. Historically, the PIN-based approach is known as a typical knowledge based authentication, which is vulnerable against many popular attacks, such as guessing (e.g., social engineering, brute force), stealing (e.g., key logging, human behavior), spoofing (e.g., replay attack, invalid login form), and eavesdropping (e.g., man-in-the-middle, scanning, traffic monitoring). Moreover, since PAC devices (PDs) might simultaneously operate on numerous communications, PIN verification makes it inconvenient for user experience [16]. As for the PHY-based approach, although it has shown more advances in confidence and resistance against these above attacks in comparison to the PIN-based approach, its shortcomings against eavesdropping and jamming attacks have still not been overcome [17].

B. OUR APPROACH

To overcome these aforementioned issues, this paper proposes a new approach that exploits a particular feature of PACNET, i.e., social networking, to support authentication and key agreement procedures for lightweight PDs. It is known that participants of conversations are able to physically identify each other through social relations directly as well as indirectly. When a PD (referred to as an initiator PD, i.e., I-PD) requests an association with other PD (named the responder PD, i.e., R-PD), certain number of mutually common PDs (C-PDs) that have established communications with both PDs are delegated to authenticate the I-PD on behalf of the R-PD. In the scope of this paper, the C-PD is identified by the PD ID (i.e., PD MAC address) and application-specific group ID (i.e., the specific communication session utilized by application) [11]. To be more specific, a PD might be separately identified as different C-PDs corresponding to different application-specific group IDs, even if they share the same PD ID. A combination of a ranking rule and pseudo-random selection is used to suggest C-PDs. Each C-PD negotiates a partial key with the I-PD, then forwards this key to the R-PD. Hash functions in the two PDs use the received partial keys to generate a new secret key between them. Intensive analysis and evaluation show that the proposed social networking based authentication (SNAuth) protocol provides multiple security levels as well as user convenience with reasonable resource consumption. Within assumption that the PDs have full abilities to manage their communications by themselves without any infrastructure entity [11], it is worth noting that key management problem is not considered in the scope of this paper.

C. CONTRIBUTIONS AND PAPER ORGANIZATION

Our contributions in this paper are described as follows:

- We have taken a thorough investigation focuses on specific characteristics of PACNET in order to define the key criteria for a selection of applicable authentication and key agreement algorithms.
- We have proposed the SNAuth protocol which significantly overcomes the existing limitations of typical PIN-based and PHY-based approaches in terms of security and resource consumption, which is proved through intensive analysis and evaluations. Moreover, the protocol also makes a convenient authentication for PAC users due to its auto-procedure without human aid.
- The proposed SNAuth protocol provides multiple security levels according to the number of utilized partial keys, which are suitable for various IoT applications that require different security levels (see Table 1).

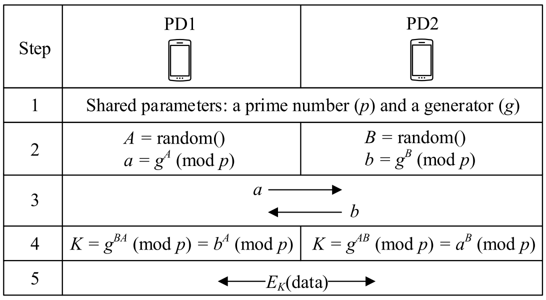
- We have shown the possibility of feasible implementation in a PACNET by a detailed discussion about advantages and shortcomings of the SNAuth protocol.

The remainder of this paper is organized as follows. We survey the existing related work in Section II. Section III introduces an overview of PACNET and its criteria that drive the selection of security algorithms. Based on these recognitions, we propose the SNAuth protocol for authentication and key agreement in Section IV. Section V and Section VI provide security analysis and performance evaluation compared to other techniques, respectively. Finally, the conclusion and future work are discussed in Section VII.

II. RELATED WORK

Given that PAC utilizes wireless channels for data transmission, the common air interface's vulnerability attracts attackers from various domains [18], [19], such as eavesdropping, denial of service (DoS), man-in-the-middle (MITM), jamming, and spoofing. Although numerous existing encryption algorithms effectively provide secure communications, they will not be useful if key agreement cannot be successfully achieved first [20]. The problem significantly worsens since PAC does not accept any central management entity in the network. Therefore, a variety of existing centralized mechanisms become inapplicable, e.g., [21]–[25]; refer to [26] and [27] for detailed surveys. It is widely recognized that there are just three basic approaches that are compatible with the PAC conditions [28]: a straightforward key sharing (via physical interactions between device owners), the well-known Diffie-Hellman key establishment [29], and a secret key extraction from PHY characteristics [17], including their variants that are recent emerging technologies. It is worth noting that asymmetric keying (e.g., public/private keys) is not mentioned due to its impracticality for dynamic peer-aware communications, caused by (i) the need for a key distributor and (ii) the heavy computation.

The straightforward key sharing is a method where a common predetermined secret key is exchanged via human negotiation (e.g., physical meeting, email, phone call). As aforementioned in Section I, the PIN-based approach is a prime example, where the straightforward key sharing reveals various shortcomings and is inconvenient for PAC users.



Step	PD1	PD2
1	Shared parameters: a prime number (p) and a generator (g)	
2	A = random() $a = g^A \pmod p$	B = random() $b = g^B \pmod p$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$K = g^{AB} \pmod p = a^B \pmod p$
5	$\longleftarrow E_K(\text{data}) \longrightarrow$	

FIGURE 1. Diffie-Hellman key exchange.

The well-known classical Diffie-Hellman key exchange [30] is shown in Fig. 1. Initially, PD1 and PD2 agree on two shared parameters: a prime number (p) and a generator (g). In the next steps, PD1 chooses a random integer A to calculate $a = g^A (\bmod\, p)$, then sends the result to PD2. Correspondingly, PD2 does the same works and sends the result $b = g^B (\bmod\, p)$ to PD1, where B is a random integer. The secret key K for PD1-PD2 communication is derived from $K = g^{BA} (\bmod\, p) = b^A (\bmod\, p)$ and $K = g^{AB} (\bmod\, p) = a^B (\bmod\, p)$ in PD1 and PD2, respectively. Although Diffie-Hellman algorithm has been widely utilized during the last decades [29], [31]–[33], it cannot be ignored that the protocol still has two disadvantages: the expensive exponentiation computation, which might overcapacitate the PDs, and its vulnerability against the logjam attacks [34]. Since PAC intends to support low-performance IoT-enabled devices for the purpose of IoT spreading, the algorithm is generally inappropriate for application in PACNET.

The PHY-based key agreement protocol is a method that exploits the randomness and reciprocity of wireless channel fading between two devices. The procedure involves contiguous steps: channel probe, response collection, randomness extraction & quantization, reconciliation, and privacy amplification [17]. The purpose of the first two steps is to gather enough randomness caused by channel fading. The amount of frequency domain responses depends on channel conditions and the negotiated quantization method between the two PDs. In the next steps, the randomness of the small-scale component is extracted from frequency responses by removing the large-scale component, which might be captured by surrounding PDs. The derived randomness is then quantized and the errors are corrected via quantization and reconciliation processes, respectively. Finally, the secret key is drawn using universal hash functions on the resulting randomness bitstream in order to eliminate the bit correlation and eavesdropped information problems [17], [35]–[37]. However, since the PHY-based key agreement protocol still has not matured yet, its shortcomings should be significantly addressed before use in a PACNET [38]. Therefore, the success of secret key generation is not stable and guaranteed against eavesdropping and jamming attacks [17]. Furthermore, the PHY method is considered too sophisticated for acceptable implementation in PDs, which are presumably equipped with low power and performance.

III. PRELIMINARIES

A. IEEE 802.15.8 PAC CHARACTERISTIC ANALYSIS

As introduced in Section I, the IEEE 802.15.8 standard provides P2P communication using relative position awareness for emerging applications such as social networking, advertising, gaming, and emergency services (Fig. 2). Despite the diversity, the applications of IEEE 802.15.8 PAC can be recognized under these common properties [7]:

- *Social networking and proximity awareness:* As explicitly described in [7], although the envisioned PAC application matrix covers a broad range of requirements in terms of data rate, latency, stability, security, etc., they

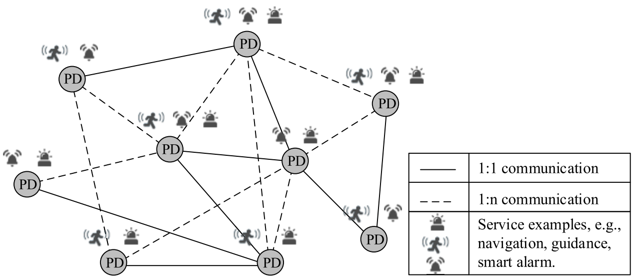


FIGURE 2. PACNET architecture [11].

are generally based on social relations and relative location information among PD holders.

- *Dense deployment:* Since PAC applications are characterized with social properties, the users of a PAC are assumed to collaborate in particular groups or communities where people are densely located and directly communicate with each other.
- *Lightweight IoT-enabled device supports:* Following the IoT paradigms, PAC applications mainly support services for IoT-enabled devices, especially lightweight devices which typically equip low power and low performance.

In order to provide an appropriate technological basis for PAC applications, IEEE 802.15.8 defines a PACNET via its characteristics as follows [11]:

- *Fully distributed coordination:* Where synchronization, discovery, association, and channel access for communication are directly performed among PDs. Equal roles are addressed to every PD in PACNET.
- *Infrastructureless architecture:* Since a PACNET is completely formed from direct communication among participating PDs, i.e., PDs act as the nodes and P2P connections act as the links, there is no infrastructure component existed in the network.
- *Multi-hop support:* For scalability, a PACNET supports multi-hop communication in order to maintain seamless device-to-device (D2D) interface between PDs in a dense and large-scale deployment.
- *Mobility:* It is natural that the mobility feature of a PACNET comes from human activity who hold their PDs.

B. CRITERIA FOR SECURITY PROTOCOL IN PACNET

Due to the aforementioned features, a proposed security protocol is forced to meet particular criteria for PACNET. The key constraints are described as follows:

- *No central management entity:* The fully distributed coordination feature forbids the existence of a central management entity (e.g., for key negotiation or key management purposes).
- *No third-party authentication support:* Where a third-party authentication agency might not be available to verify the authenticity of participating PDs (e.g., in the case of certificate based solutions or asymmetric keys).
- *Lightweight IoT compatibility:* In other word, the security protocol should be a lightweight solution to ensure its applicability in a PACNET where the PDs are lightweight IoT-enabled devices.

IV. SOCIAL NETWORKING BASED AUTHENTICATION PROTOCOL

This section describes the proposed SNAuth protocol, which exploits social networking relations to support authentication and key agreement procedures between two lightweight PDs, i.e., I-PD (initiator) and R-PD (responder).

A. INITIAL NETWORK CONDITIONS

In this paper, we exploit two distinguishable characteristics of PACNET, social networking and dense deployment. In such an environment, each PD participates in multiple multicast groups where it can establish numerous 1:1 and 1:n communication sessions according to the applications' requirements [39]. Since the applications are characterized by their geolocation awareness, a particular PACNET is considered to serve a certain number of applications. For instance, motion detectors can simultaneously support both guidance application and customer statistic application within different multicast groups inside a museum. Moreover, multi-hop routing techniques and dense deployment promise a perfect condition for any two PDs with social relations to a number of C-PDs. In the scope of this paper, we assume that synchronization and discovery processes have already been successfully performed prior to the association establishment, where authentication and key agreement are involved.

TABLE 2. Notations for the SNAuth protocol.

Notation	Description
I-PD	Initiator PAC device.
R-PD	Responder PAC device.
C-PD$_i$	*i-th* common PAC device that has ever established social relations with both I-PD and R-PD. C-PD is identified by PD ID and an application-specific group ID.
ACK	Acknowledgement message.
DoA	Delegation of authentication message.
$K_{I,i}()$	Secure message encrypted by secret key $K_{I,i}$ between I-PD and C-PD$_i$.
$K_{R,i}()$	Secure message encrypted by secret key $K_{R,i}$ between R-PD and C-PD$_i$.
$K_{R,I}()$	Secure message encrypted by secret key $K_{R,I}$ between R-PD and I-PD.
pk_i	Partial key negotiated between I-PD and C-PD$_i$.
$O()$	Open (insecure) message.
$H(\cdot)$	Hash function.
$\bigoplus$	Bitwise XOR operation.

B. THE PROPOSED SNAuth PROTOCOL

The notation used to describe the SNAuth protocol is defined in Table 2. Suppose that an I-PD requests an association with an R-PD, the proposed SNAuth protocol shown in Fig. 3 includes two steps:

Step 1: Authentication delegation. The R-PD delegates authority of I-PD authentication to the C-PDs.

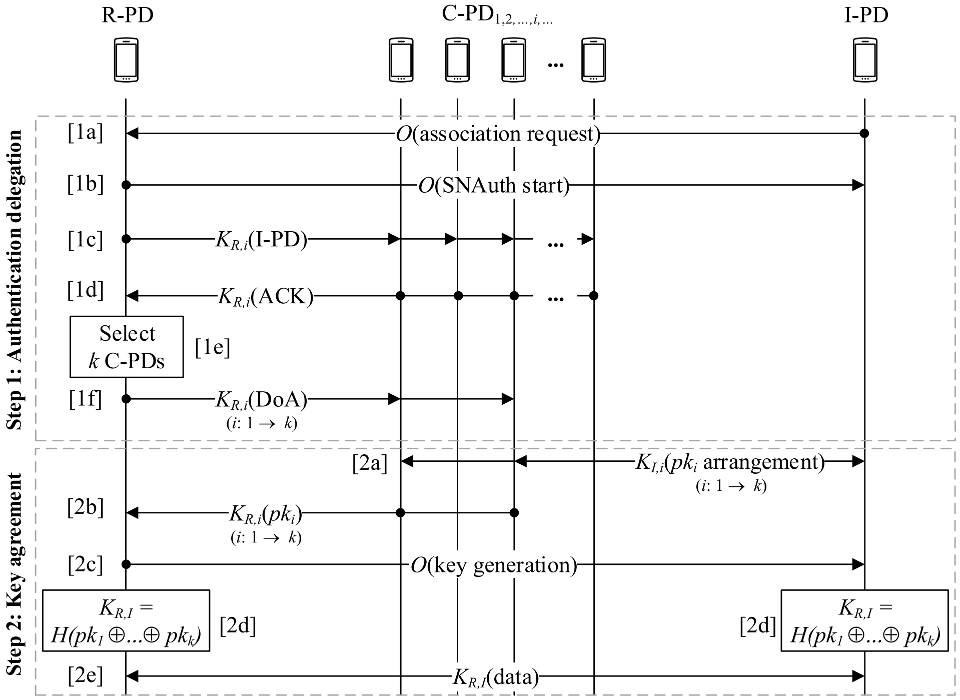


FIGURE 3. SNAuth authentication protocol.

1a. *I-PD* $\xrightarrow{O(association\ request)}$ *R-PD:* In order to establish a communication, the I-PD sends an association request to the R-PD.

1b. *R-PD* $\xrightarrow{O(SNAuth\ start)}$ *I-PD:* Assuming that the R-PD agrees to initiate an authentication process with the I-PD, the R-PD responds with a message of *SNAuth start* to the I-PD.

1c. *R-PD* $\xrightarrow{K_{R,i}(I\text{-}PD)}$ *C-PD$_i$:* Since R-PD has never established any communication with I-PD in advance, it does not have any information on the I-PD for authentication. After receiving the association request from I-PD, R-PD securely unicasts an inquiry message containing the I-PD address to each of its associated PDs in order to ask a delegation of I-PD authentication.

1d. *C-PD$_i$* $\xrightarrow{K_{R,i}(ACK)}$ *R-PD:* Assuming that among the associated PDs of R-PD, there are some C-PDs that have at some point established social relations with I-PD. Whenever each of these C-PDs receives the inquiry message, it should reply to R-PD with an ACK. Otherwise, PDs that have no information on the I-PD just ignore the inquiry message.

1e. *Select k C-PDs:* R-PD derives possible delegatee candidates from the received ACKs. In order to reduce traffic overhead and latency, a certain number of the candidates (i.e., *k* C-PDs) are selected. The chosen ones are suggested by a pseudo-random function of trust based ranking. Recently, there are a variety of ranking algorithms (a.k.a. recommendation systems) appropriate for location-based social networks available in the literature [40]. For the purpose of C-PD selection, we customize a lightweight algorithm based on the original one in [41]. According to the algorithm, the rank r_i of *i-th* C-PD is given by

$$r_i = \sum_{\forall s} D_s T_s, \tag{1}$$

where D_s is the data size in bytes of conversation s and T_s is a strictly decreasing function of time:

$$T_s = \varepsilon^{t_{now} - t_{eos}}, \qquad \leq \varepsilon \leq 1, \tag{2}$$

where t_{now} is the current time and t_{eos} is the ending time of conversation s. The pseudo-random function updates the rank of each C-PD by

$$r_i = r_i \times \text{random}(\min_{\forall j}(r_j), \max_{\forall j}(r_j)). \tag{3}$$

Finally, k C-PDs whose ranks belong to the top-k highest values are chosen as the delegatees for authenticating the I-PD.

1f. *R-PD* $\xrightarrow{K_{R,i}(DoA)}$ *C-PD$_i$:* R-PD unicasts delegation of authentication (DoA) messages to each of the *k* chosen C-PDs to delegate the authority of I-PD authentication. Note that the DoA message is a management message [11], which contains a flag bit indicating DoA assignment.

For instance, consider a PACNET topology as shown in Fig. 4, where an R-PD and I-PD (colored by blue) participate in multicast groups (1, 2, 3) and (4, 5), respectively.

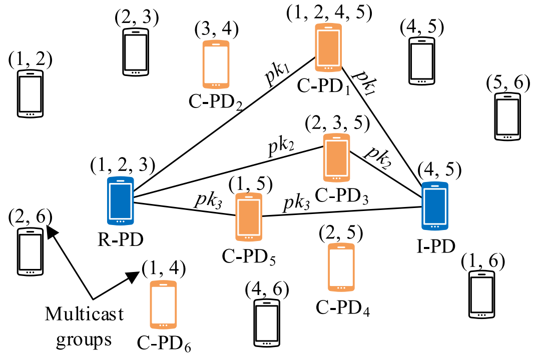


FIGURE 4. An example of SNAuth application in PACNET.

The I-PD requests an association with the R-PD. Since the R-PD has never established any communication with the I-PD in advance, the R-PD sends inquiry message containing the I-PD address to its neighboring devices in multicast groups 1, 2, and 3. C-PD$_{1,2,3,4,5,6}$ (marked by orange) also have relations with the I-PD, then they reply to the R-PD with ACKs. Using Eq. 3, suppose that the R-PD obtains a list of C-PD$_{1,3,5}$ (fulfilled by orange) to be delegated the authority of I-PD authentication.

Step 2: Key agreement. Each delegated C-PD negotiates a partial key with the I-PD and sends the partial key back to the R-PD. The R-PD and I-PD combine all partial keys to generate a common secret key.

2a. $C\text{-}PD_i \xleftrightarrow{K_{I,i}(pk_i\ arrangement)} I\text{-}PD$: A partial key pk_i is randomly generated by using a pseudo-random generator in the *i-th* C-PD. Afterward, the *i-th* C-PD shares this key to the I-PD via its secure peer-to-peer channel.

2b. $C\text{-}PD_i \xrightarrow{K_{R,i}(pk_i)} R\text{-}PD$: Each of the k C-PDs forwards its pk_i to R-PD.

2c. $R\text{-}PD \xrightarrow{O(key\ generation)} I\text{-}PD$: R-PD sends a notification message to I-PD in the insecure channel to start the key generation process.

2d. $K_{R,I} = H(pk_1 \oplus \cdots \oplus pk_k)$: The secret key $K_{R,I}$ is generated using the hash function

$$K_{R,I} = H(pk_1 \oplus \cdots \oplus pk_k). \tag{4}$$

A challenge/response procedure is optionally utilized to ensure secret key synchronization.

2e. $R\text{-}PD \xleftrightarrow{K_{I,R}(data)} I\text{-}PD$: Finally, the communication between I-PD and R-PD is authenticated and secured by secret key $K_{R,I}$.

Continue to consider the example in Fig. 4. After receiving DoA messages from the R-PD, C-PD$_{1,3,5}$ negotiate partial keys $pk_{1,3,5}$ with the I-PD, respectively. Then, these partial keys are forwarded to the R-PD. In case of obtaining all partial keys from the C-PD$_{1,3,5}$, the R-PD notifies the I-PD to start secret key generation. The secret key $K_{R,I}$ is an output of a hash function with the input of all partial keys $pk_{1,3,5}$.

V. SECURITY ANALYSIS

Since PACNET is featured in multi-hop routing technology, the intermediate PDs that participate in the data path between I-PD and R-PD might be exploited to attack the communication. Some popular attack methods in this circumstance are analyzed as below.

A. MAN-IN-THE-MIDDLE ATTACK

1) ADVERSARY MODEL

- *Objective:* To find the secret key.
- *Initial capabilities:* The attackers have chance to eavesdrop some partial keys since they might establish numerous communications with the R-PD, I-PD, and other neighboring PDs in advance. It is worth noting that the attackers must have the role of C-PDs to eavesdrop the corresponding partial keys since the channel between C-PDs and R-PD/I-PD are peer-to-peer secure channel.
- *Attack process:* Against the SNAuth protocol, a MITM attack is a method where the attacker (or a collusion among attackers) utilizes a number of eavesdropping PDs in order to capture partial keys generated by C-PDs. If all partial keys are revealed, the secret key between the I-PD and R-PD can be regenerated.

2) COUNTERMEASURE

As described in Section IV, since the SNAuth protocol is developed based on social relations between I-PD, R-PD, and C-PDs, the proposed trust-based ranking and pseudo-random functions suggest a number of delegated C-PDs within consideration of its historical communications to evaluate the trustfulness. Moreover, dense deployment of PACNETs extremely reduces the possibility that all partial keys can be eavesdropped. Indeed, the possibility of eavesdropping is analyzed as follows.

Without loss of generality, suppose that the number of communication sessions each PD establishes adopts a Poisson distribution with mean λ_1 and λ_2 for *1:1* applications and *1:n* applications, respectively. The interest rate of *1:1* applications and *1:n* applications are assumed to uniformly distributed with mean α and β, respectively. Let N, m, and k denote the total number of PDs in the PACNET, the number of eavesdropping PDs (X-PDs) exploited by attacker(s), and the number of partial keys, respectively. The average number S of concurrent communication sessions that a PD operates is given by

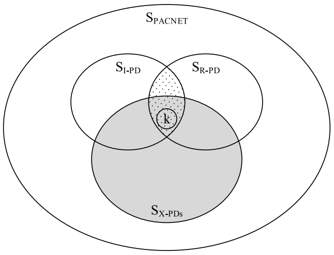
$$S = \sum_{i=0}^{\infty} P(i)i\alpha + \sum_{j=0}^{\infty} P(j)j\beta N, \tag{5}$$

where $P(i)$ and $P(j)$ are the probabilities that i *1:1* applications and j *1:n* applications are used by the PD, respectively. βN shows the number of PDs that participate in an *1:n* application. Since $P(i)$ and $P(j)$ follow Poisson distributions, the average number S of concurrent communication sessions is updated as

$$S = \sum_{i=0}^{\infty} \frac{\lambda_1^i e^{-\lambda_1}}{i!} i\alpha + \sum_{j=0}^{\infty} \frac{\lambda_2^j e^{-\lambda_2}}{j!} j\beta N$$
$$= \lambda_1\alpha + \lambda_2\beta N. \qquad (6)$$

The situation when the attacker(s) can capture all partial keys is the same as when the *total k sessions of C-PDs are eavesdropped on by the X-PDs*. Let S_{PACNET}, S_{I-PD}, $S_{\text{R-PD}}$, and S_{X-PDs} denote the average sessions of PACNET, I-PD, R-PD, and X-PDs, respectively. Hence, the probability that the attacker(s) can capture all partial keys can be expressed as: *The probability that there are at least k sessions simultaneously belonging to S_{I-PD}, $S_{\text{R-PD}}$, and S_{X-PDs}*, denoted by $P(x \geq k)$, where x is the intersection $S_{I-PD} \cap S_{\text{R-PD}} \cap S_{X-PDs}$. Figure 5 describes the Venn diagram that represents the possibility of eavesdropping by attacker(s) against I-PD&R-PD authentication and key agreement processes. Derived from Eq. 6,

$$\begin{cases} S_{PACNET} = \frac{N}{2}S = \frac{N}{2}(\lambda_1\alpha + \lambda_2\beta N), \\ S_{I-PD} = S = \lambda_1\alpha + \lambda_2\beta N, \\ S_{R-PD} = S = \lambda_1\alpha + \lambda_2\beta N, \\ S_{X-PDs} = mS = m(\lambda_1\alpha + \lambda_2\beta N). \end{cases} \qquad (7)$$



S_{PACNET}	Total communication sessions
S_{I-PD}	Commununication sessions of I-PD
S_{R-PD}	Commununication sessions of R-PD
S_{X-PDs}	Commununication sessions of attacker(s) provided by X-PDs
k	Number of partial keys

FIGURE 5. Venn diagram representing the possibility of eavesdropping by attacker(s) against the I-PD&R-PD authentication and key agreement processes.

Therefore, $P(x \geq k)$ is determined by

$$P(x \geq k) = \sum P(S_{I-PD} \cap S_{R-PD} \cap S_{X-PDs} = x | x \geq k). \qquad (8)$$

Using Bayes' theorem, the $P(x \geq k)$ is calculated by

$$P(x \geq k) = \sum_{i=k}^{\min(S_{I-PD}, S_{R-PD})} \Bigg[P(S_{I-PD} \cap S_{R-PD} = I | n(I) = i)$$
$$\times \sum_{j=k}^{\min(I, S_{X-PDs})} P(I \cap S_{X-PDs} = J | n(J) = j) \Bigg]$$
$$= \sum_{i=k}^{\min(I, S_{X-PDs})} \Bigg[\frac{\binom{S_{I-PD}}{i}\binom{S_{PACNET}-S_{I-PD}}{S_{R-PD}-i}}{\binom{S_{PACNET}}{S_{R-PD}}}$$
$$\times \sum_{j=k}^{\min(I, S_{X-PDs})} \frac{\binom{i}{j}\binom{S_{PACNET}-i}{S_{X-PDs}-j}}{\binom{S_{PACNET}}{S_{R-PD}}} \Bigg]. \qquad (9)$$

Replace S_{PACNET}, S_{I-PD}, S_{R-PD}, and S_{X-PDs} from Eq. 7 to Eq. 9,

$$P(x \geq k) = \sum_{i=k}^{S} \left[\frac{\binom{S}{i}\binom{\frac{N}{2}S-S}{S-i}}{\binom{\frac{N}{2}S}{S}} \sum_{j=k}^{i} \frac{\binom{i}{j}\binom{\frac{N}{2}S-i}{mS-j}}{\binom{\frac{N}{2}S}{mS}} \right]$$
$$= \sum_{i=k}^{S} \sum_{j=k}^{i} \frac{\binom{S}{i}\binom{\frac{N}{2}S-S}{S-i}}{\binom{\frac{N}{2}S}{S}} \frac{\binom{i}{j}\binom{\frac{N}{2}S-i}{mS-j}}{\binom{\frac{N}{2}S}{mS}}, \qquad (10)$$

where $S = \lambda_1\alpha + \lambda_2\beta N$.

Figures 6 and 7 show the probability $P(x \geq k)$ depending on PACNET density (#PDs) with the following assumptions: $\lambda_1 = 2$, $\lambda_2 = 3$, $\alpha = 0.4$, and $\beta = 0.15$. Note that the higher value these parameters take on the lower value the probability. Plot starts from #PDs of 50 since densely deployed networking environment is considered. In Fig. 6 and 7, it is observed that the probability that the attacker(s) can capture all partial keys exponentially decreases when #PDs increases in the network. Even if the SNAuth protocol just uses two partial keys, the probability $P(x \geq 2)$ is smaller than 1.0E-04 when the #PDs is over 300 (see Fig. 6). In Fig. 7, the probability is extremely decreased to around 1.0E-08 if 4 partial keys (i.e., $k = 4$) are used. The detailed numerical results are provided in Table 3, revealing that the probability of the attacker(s) capturing all partial keys in order to re-generate the secret key is not considerable when the number of partial keys are sufficient. In other words, the achievable secure level of the secret key should be flexibly decided by individual application due to its own requirements based on the number of partial keys used.

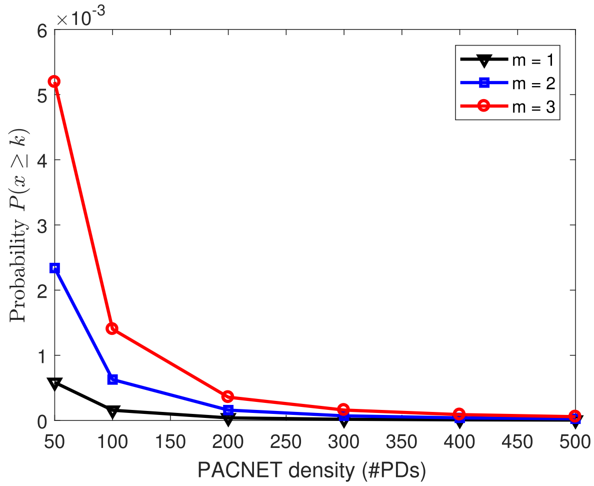


FIGURE 6. The probability $P(x \geq k)$ depends on the PACNET density when $k = 2$ and m varies.

B. MODIFICATION ATTACK

1) ADVERSARY MODEL

- *Objective:* To break the synchronization of secret key generation between I-PD and R-PD.

TABLE 3. The probability that the attacker(s) can capture all partial keys for $m = 5$.

PACNET density (#PDs)	k = 2	k = 3	k = 4
50	1.39E-02	7.03E-04	2.42E-05
100	3.82E-03	1.06E-04	2.11E-06
200	9.82E-04	1.41E-05	1.49E-07
300	4.41E-04	4.28E-06	3.08E-08
400	2.49E-04	1.83E-06	9.98E-09
500	1.60E-04	9.44E-07	4.14E-09

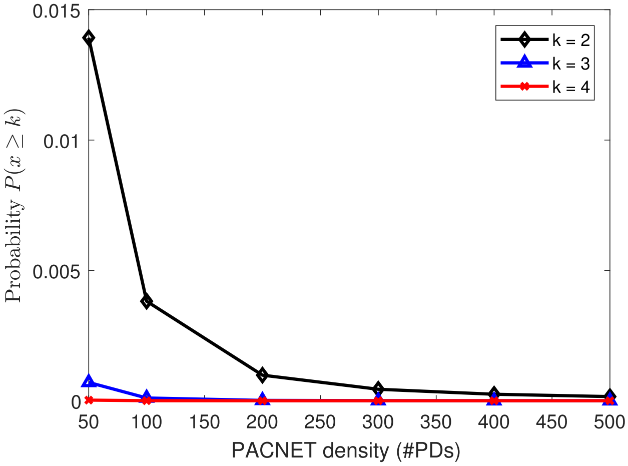


FIGURE 7. The probability $P(x \geq k)$ depends on the PACNET density when $m = 5$ and k varies.

- *Initial capabilities:* The attackers have chance to eavesdrop some partial keys since they might establish numerous communications with the R-PD, I-PD, and other neighboring PDs in advance. It is worth noting that the attackers must have the role of C-PDs to modify the corresponding partial keys since the channel between C-PDs and R-PD/I-PD are peer-to-peer secure channel.
- *Attack process:* Since the SNAuth protocol generates the secret key based on a combination of partial keys which are negotiated between I-PD and the delegated C-PDs, a modification attack aims to exploit some of the C-PDs to modify or counterfeit the partial keys.

2) COUNTERMEASURE

Referring to Eq. 10, the probability that at least one C-PD is hijacked by the attacker is equal to $P(x \geq 1)$. Using the same network environment conditions as in the previous section, $P(x \geq 1)$ is equal to 7.18E-03 and 1.19E-02, corresponding to 500 PDs and 300 PDs in the network, respectively. Even if the attacker can modify some partial keys, the SNAuth protocol is able to detect/protect against ambiguous partial keys by utilizing the challenge/response procedure where each couple of partial keys is used for the challenge. Once the ambiguous partial keys are rejected, the SNAuth protocol can either continue the key generation process or reinitialize the protocol without consideration of the hijacked C-PDs. Although this causes additional verification operations, the SNAuth protocol is secure against modification attacks.

C. REPLAY ATTACK

1) ADVERSARY MODEL

- *Objective:* To capture the partial keys.
- *Initial capabilities:* The attackers might be intermediate PDs between R-PD and C-PDs due to multi-hop PACNET environment.
- *Attack process:* Against the SNAuth protocol, a replay attack is a method where the adversary exploits the intermediate PD that participates in the multi-hop data path between the R-PD, I-PD, and C-PDs in order to eavesdrop the authentication messages, and then they maliciously repeat these messages to incite illegal association.

2) COUNTERMEASURE

The mechanism for the SNAuth protocol is based on delegating the authentication process to numerous trustful PDs, which is performed through secure communications. The only open message contains only a notification to indicate that key generation is ready to be performed (see step 2d of the SNAuth protocol in Section IV-B). Even if the adversary can capture this message, it is meaningless without knowledge of the delegatees information, the number of partial keys, and the partial keys which are vital. In other words, the SNAuth protocol is secure against replay attacks.

D. DENIAL-OF-SERVICE ATTACK

1) ADVERSARY MODEL

- *Objective:* To disrupt the authentication and key agreement processes.
- *Initial capabilities:* The attackers might have knowledge of R-PD and I-PD identifications through eavesdropping in prior.
- *Attack process:* The SNAuth protocol utilizes social networking relations among PDs for authentication and key agreement processes. In order to attack the SNAuth protocol, DoS attackers focus on preventing the R-PD from delegating authentication to the C-PDs by faking and/or duplicating the C-PDs addresses (e.g., hole attacks and Sybil attacks). Note that the physical-layer DoS attack, where the attackers inject jamming signals and interference on the working channels of the victims (i.e., R-PD and I-PD) in order to disable communication capability of the victims, is out of scope of this paper since the proposed protocol is designed for MAC layer and upper layers.

2) COUNTERMEASURE

As aforementioned, the SNAuth protocol delegates the authentication process to the trustful C-PDs, which are pseudo-randomly selected among numerous PDs that have historically private communications with both the R-PD and the I-PD. Moreover, communications between the R-PD and the C-PDs are delivered via secure peer-to-peer links. Therefore, the faked C-PDs can be detected and then prevented by

TABLE 4. Performance comparison.

Characteristic	SNAuth protocol	PIN-based approach	Diffie-Hellman approach	PHY-based approach
Computation cost	$O(n)$	0	$O(c^n)$	$O(n^2)$
Communication cost	$N_C L_D + kL_{pk}$	0	$2L_c$	$N_s L_s + L_r$
Storage cost	$N_C S_r + kS_{pk}$	S_{PIN}	$2S_c$	$N_s S_s$
Time cost	$kT_{pk} + T_{sk}$	Manual	LEO	Undetermined

Note – $O(\cdot)$: computational complexity; LEO: large exponential operation; N_C: the number of C-PDs; L_D: the length of DoA message; L_{pk}: the length of partial key arrangement message; L_c: the length of challenge number exchange message; N_s: the number of samples; L_s: the length of sample message; L_r: the length of exchanged data message for reconciliation process; S_r: the size of C-PD rank; S_{pk}: the size of partial key; S_{PIN}: the size of PIN; S_c: the size of challenge number; S_s: the size of sample; T_{pk}: time spent for partial key arrangement; T_{sk}: time spent for secret key generation.

dropping their messages. In case of C-PDs' message duplication attacks, the R-PD derives informative data from the first-order arrived messages and does not consider the duplication activities in message transfer. Additionally, this activities can be ignored by using the dropping policy for this behavior (out of the proposed protocol's purposes). In other words, the SNAuth protocol is secure against DoS attacks.

VI. PERFORMANCE EVALUATION

A. THEORETICAL ANALYSIS

For performance evaluation purposes, the SNAuth protocol is compared to three typical approaches, including PIN-based, Diffie-Hellman, and PHY-based approaches, in terms of the computation cost, communication cost, storage cost, and time consumption. Detailed information is provided in Table 4.

Regarding the computation cost, the SNAuth protocol performs the C-PDs ranking calculation, partial keys pks arrangement, and secret key $K_{R,I}$ generation within a computational complexity of $\mathcal{O}(n)$. On other side, since the PIN is generally predetermined on PDs, its computation cost is considered as 0. In Diffie-Hellman key exchange, a large exponential operation should be utilized to generate a secure key against logjam attacks [34]. To obtain a high security level, the large exponential operation must pay an expensive computation cost with an $\mathcal{O}(c^n)$ complexity. Within the PHY-based approach, the computation cost issued by small-scale randomness extraction & quantization, reconciliation, and privacy amplification processes has an $\mathcal{O}(n^2)$ computational complexity. Generally, the SNAuth protocol has a smaller computation cost than other competitors, except for the pre-installed PIN-based approach.

Regarding the communication cost, the SNAuth protocol reveals its disadvantage due to the requirements of some message exchanges for authentication delegation and key agreement processes. The number of communication messages proportionally depends on the number of partial keys used. In spite of that, the communication cost of the SNAuth protocol is even lower than PHY-based approaches, which must collect thousands of samples for the randomness extraction [17]. On the other hand, PIN-based approaches do not need to transmit any information for key generation purpose (i.e., a communication cost equal to 0); and the Diffie-Hellman key exchange uses just two messages for challenge number transmission.

TABLE 5. Simulation parameters [39].

Parameter	Value
Notification frame	32.75 bytes
Management frame	48 bytes
Topology size	500 m × 500 m
Transmission range	100 m
Initial transmission probability	0.5
λ_1	2
λ_2	3
α	0.4
β	0.15
m	5 partial keys

In terms of the storage cost, the SNAuth protocol uses memory to save log information for the conversation history for ranking trustfulness among C-PDs and k received partial keys. In the same manner, PHY-based approaches require memory to store thousands of samples for randomness extraction. In contrast, PIN-based approaches need only a few bits to install the PIN; and the Diffie-Hellman key exchange needs only bytes to store the challenge number.

For time consumption comparisons, the SNAuth protocol spends its time on partial key collections and secret key generation processes. With PIN-based approaches, although they introduce advantages in all previous evaluations, the PIN must be manually input and confirmed by the user (note that the PD is able to simultaneously establish multiple communication sessions in a PACNET). On the other hand, the time consumption for Diffie-Hellman key exchange is caused mostly by the large exponential operation, which significantly depends on the PD capability. In PHY-based approaches, since the number of required samples and the success of key generation unpredictably vary based on channel condition and the length of the targeted secret key, the time consumption cannot be determined.

Regardless of other criteria, the performance evaluation shows that the Diffie-Hellman key exchange and the PHY-based approaches are inappropriate for PACNET due to the expensive computation cost and undetermined time consumption, respectively. Between the two remaining ones, the SNAuth protocol and PIN-based approaches, although the PIN-based approach achieves the best performance in terms of computation, communication, and storage cost, the manual PIN provision makes it hard to widely accept among

TABLE 6. Performance costs of the SNAuth protocol.

#PDs	Computation cost [CPU cycles]	Communication cost [bytes]	Storage cost [bits]	Time cost [ms]
50	27,648	4,280.87	6,560	106.08
100	53,248	7,283.45	7,568	148.75
200	105,472	12,482.50	10,112	235.79
300	137,216	19,318.65	11,648	288.69
400	196,608	23,650.83	13,376	387.68
500	218,112	31,837.82	15,440	423.52

PAC users. The SNAuth protocol, in spite of some of the overhead issued from communication and storage, is considered as the best candidate for authentication and key agreement in a PACNET.

B. SIMULATION RESULTS

In this section, we provide performance costs of SNAuth protocol execution. Assuming that the simulation has been conducted with network conditions consisting of: 32.75-byte notification frame, 48-byte management frame, 100-m transmission range, λ_1 of 2, λ_2 of 3, α of 0.4, and β of 0.15 [39]. In this model, 50–500 PDs are randomly distributed in an area of 500 m × 500 m. The SNAuth protocol requires 5 partial keys for authentication and key agreement processes. Detailed parameters are summarized in Table 5. This simulation model is performed by using the OPNET modeler 14.5 [42].

The numerical simulation results, which reveal average value of the performance costs among participated PDs in terms of computation, communication, storage, and time consumption, are shown in Table 6. Generally, all of the performance costs proportionally increase depending on the number of PDs in the network since the number of C-PDs are increased as well. Particularly, the computation and the storage require around 218,112 CPU cycles for execution and 15,440 bits for data saving in each PDs within a 500-PD network model, respectively. These requirements can be capacitated by almost all typical lightweight IoT devices [27]. Moreover, the duration spent for the SNAuth procedures is around 106.08–423.52 ms when the number of PDs is 50–500, respectively, which is acceptable for almost all envisioned PAC applications as specified in [7].

VII. CONCLUSION AND FUTURE WORK

The IEEE 802.15.8 standard explicitly defines technological requirements and criteria appropriate for infrastructureless peer-aware communication featured with fully distributed coordination, which promises significant contributions to the rapid growth of the IoT paradigms. Due to these specific characteristics of PACNET, addressing security issues is considered as a great challenge for popularizing PAC in human life. In this paper, a social networking based authentication (SNAuth) protocol has been proposed for authentication and key agreement processes between lightweight IoT-enabled PDs in a PACNET. Intensive security analysis and performance evaluations show that the SNAuth protocol overcomes other existing candidates for PACNET security algorithms by providing multi-security levels according to particular IoT applications as well as giving usage convenience for PAC users. Since the SNAuth protocol aims at supporting lightweight IoT-enabled PDs by exploiting the social networking feature among PDs, a consideration of SNAuth applications in various devices and environments will be our main goals in future research.

REFERENCES

[1] Y. Wang, A. V. Vasilakos, Q. Jin, and J. Ma, "Survey on mobile social networking in proximity (MSNP): Approaches, challenges and architecture," *Wireless Netw.*, vol. 20, no. 6, pp. 1295–1311, Aug. 2014.

[2] T. H. Luan, R. Lu, X. Shen, and F. Bai, "Social on the road: Enabling secure and efficient social networking on highways," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 44–51, Feb. 2015.

[3] W. Na, N.-N. Dao, and S. Cho, "Reliable multicasting service for densely deployed military sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, p. 341912, 2015.

[4] W. Na, N.-N. Dao, and S. Cho, "Mitigating WiFi interference to improve throughput for in-vehicle infotainment networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 22–28, Feb. 2016.

[5] J. Eom *et al.*, "Using social Internet of Things (SIoT) demand side management on the plant," in *Proc. IEEE Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2016, pp. 685–687.

[6] 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, no. 8, p. e0182527, 2017.

[7] E. Zeira, Q. Li, and S. Jin, *The PAC Application Matrix*, IEEE Standard P802.15 TG8 standardization, Doc#: 15-12-0684-00-0008, 2012.

[8] N.-N. Dao, J. Kim, M. Park, and S. Cho, "Adaptive suspicious prevention for defending DoS attacks in SDN-based convergent networks," *PLoS ONE*, vol. 11, no. 8, p. e0160375, 2016.

[9] N.-N. Dao *et al.*, "Adaptive resource balancing for serviceability maximization in fog radio access networks," *IEEE Access*, vol. 5, pp. 14548–14559, 2017.

[10] D. Feng, L. Lu, Y. Yuan-Wu, G. Li, S. Li, and G. Feng, "Device-to-device communications in cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 49–55, Apr. 2014.

[11] *Official Draft of IEEE 802.15.8 PAC D0.18.0*, IEEE Standard P802.15 TG8 Standardization, Doc#: 15-16-0113-01-0008, 2016.

[12] *IEEE 802.15.8 Document Repository*. Accessed: Jun. 20, 2017. [Online]. Available: https://mentor.ieee.org/802.15/documents?is_group=0008

[13] Y. Kim, N.-N. Dao, J. Lee, and S. Cho, "Trend analyses of authentication in peer aware communication (PAC)," in *Proc. IEEE Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 1053–1055.

[14] W. Na and S. Cho, *MAC Security for IEEE 802.15.8 PAC*, IEEE Standard P802.15 TG8 Standardization, Doc#: 15-15-0254-00-0008, 2015.

[15] B. Kwak and N. Song, *Fixed Equations for PHY Security*, IEEE Standard P802.15 TG8 Standardization, Doc#: 15-16-0696-00-0008, 2016.

[16] C.-S. Tsai, C.-C. Lee, and M.-S. Hwang, "Password authentication schemes: Current status and key issues," *Int. J. Netw. Secur.*, vol. 3, no. 2, pp. 101–115, 2006.

[17] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[18] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.

[19] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–26, Jan. 2017.

[20] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.

[21] C. C. Wu, W. B. Lee, and W.-J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Commun. Lett.*, vol. 12, no. 10, pp. 722–723, Oct. 2008.

[22] I. Butun, Y. Wang, Y.-S. Lee, and R. Sankar, "Intrusion prevention with two–level user authentication in heterogeneous wireless sensor networks," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 107–121, 2012.

[23] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 10, no. 4, pp. 361–371, 2010.

[24] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[25] F. Hu, W. Siddiqui, and K. Sankar, "Scalable security in wireless sensor and actuator networks (WSANs)," in *Security in Sensor Networks*. CRC Press, 2016, ch. 8.

[26] C.-Y. Chen and H.-C. Chao, "A survey of key distribution in wireless sensor networks," *Security Commun. Netw.*, vol. 7, no. 12, pp. 2495–2508, 2014.

[27] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Comput. Surv.*, vol. 48, no. 2, 2015, Art. no. 26.

[28] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for device-to-device communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 336–340.

[29] S. Blake-Wilson and A. Menezes, "Authenticated Diffie–Hellman key agreement protocols," in *Proc. Int. Workshop Sel. Areas Cryptogr.*, Aug. 1998, pp. 339–361.

[30] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[31] M. Steiner, G. Tsudik, and M. Waidner, "Diffie–Hellman key distribution extended to group communication," in *Proc. ACM Conf. Comput. Commun. Secur.*, 1996, pp. 31–37.

[32] W.-B. Hsieh and J.-S. Leu, "Anonymous authentication protocol based on elliptic curve Diffie–Hellman for wireless access networks," *Wireless Commun. Mobile Comput.*, vol. 14, no. 10, pp. 995–1006, Jul. 2014.

[33] P. Subramaniam and A. Parakh, "A quantum Diffie–Hellman protocol," *Int. J. Secur. Netw.*, vol. 11, no. 4, pp. 213–223, Jan. 2016.

[34] D. Adrian *et al.*, "e, L. Valenta, "Imperfect forward secrecy: How Diffie–Hellman fails in practice," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 5–17.

[35] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[36] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[37] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE Conf. Inf. Commun. (INFOCOM)*, Mar. 2010, pp. 1837–1845.

[38] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, Oct. 2012.

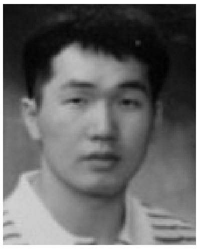
[39] W. Na, Y. Lee, J. Yoon, J. Park, and S. Cho, "Fully distributed multicast routing protocol for IEEE 802.15.8 peer-aware communication," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, p. 531710, 2015.

[40] J. Bao, Y. Zheng, D. Wilkie, and M. Mokbel, "Recommendations in location-based social networks: A survey," *GeoInformatica*, vol. 19, no. 3, pp. 525–565, Jul. 2015.

[41] Y. Wang, L. Li, and G. Liu, "Social context-aware trust inference for trust enhancement in social network based recommendations on service providers," *World Wide Web*, vol. 18, no. 1, pp. 159–184, Jan. 2015.

[42] *OPNET Modeler 14.5*. Accessed: Jul. 23, 2017. [Online]. Available: https://www.opnet.com

NHU-NGOC DAO received the B.S. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology, Vietnam, 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.



YONGHUN KIM received the B.S. degree in digital multimedia from Kyunghee Cyber University, South Korea, in 2014. He is currently pursuing the M.S. degree in computer science with Chung-Ang University, South Korea. His research interests include network security, ubiquitous computing, and Internet of Things.

SEOHYEON JEONG received the B.S. degree in computer science from Chung-Ang University, South Korea, in 2016, where she is currently pursuing the M.S. degree in computer science. Her research interests include network security, ubiquitous computing, and Internet of Things.

MINHO PARK (M'14) received the B.S. and M.S. degrees in electronics engineering from Korea University in 2000 and 2002, respectively, and the Ph.D. degree from the School of Electrical Engineering and Computer Science, Seoul National University, Seoul, South Korea, in 2010. He was with Samsung Electronics from 2002 to 2004. As a Post-Doctoral Researcher, he has been with Carnegie Mellon University (CMU) for two years since 2011. Before the Post-Doctoral Researcher at CMU, he was a Senior Engineer with the 3GPP LTE S/W Development Group, Samsung Electronics. He is currently an Assistant Professor with the School of Electronic Engineering, Soongsil University, Seoul. His current research interests include wireless networks, vehicular communication networks, network security, and cloud computing.

SUNGRAE CHO 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. From 2012 to 2013, he held a visiting professorship at the National Institute of Standards and Technology, Gaithersburg, MD, USA. He is currently a Full Professor with the School of Computer Science and Engineering, Chung-Ang University. Prior to joining Chung-Ang University, he was an Assistant Professor with the Department of Computer Sciences, Georgia Southern University, Statesboro, GA, USA, from 2003 to 2006. His research interests include wireless networking, ubiquitous computing, performance evaluation, and queuing theory.. From 1994 to 1996, he was a Member of Research Staff at the Electronics and Telecommunications Research Institute, Daejeon, South Korea. He was a Senior Member of Technical Staff at the Samsung Advanced Institute of Technology, Giheung, South Korea, in 2003. He has been an Editor of the *Elsevier Ad Hoc Networks* journal since 2012 and has served numerous international conferences as an organizing committee member, such as the IEEE SECON, ICOIN, ICTC, ICUFN, TridentCom, and the IEEE MASS.