A Reliable Physical Layer Authentication Algorithm for Massive IoT Systems

YUPENG WANG1, JIANFENG JIN1, YUFENG LI1, AND CHANG CHOI2, (Senior Member, IEEE)
1College of Electronic and Information Engineering, Shenyang Aerospace University, Shenyang 110136, China
2Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea
Corresponding author: Chang Choi (changchoi@gachon.ac.kr)

This work was supported in part by the Natural Science Foundation of Liaoning Province China under Grant 2019-ZD-0220, in part by the Aeronautical Science Foundation of China under Grant 201926054002, in part by the National Research Foundation of Korea (NRF) Funded by the Korea Government (Ministry of Science and ICT) under Grant 2017R1E1A1A01077913, and in part by the Global Infrastructure Program through the National Research Foundation of Korea (NRF) Funded by the Ministry of Science and ICT under Grant NRF-2018K1A3A1A20026485.

ABSTRACT As the request for network access and a variety of services, the Internet of Things (IoT) has evolved from special networks with simple functions to global information infrastructure, challenging the current authentication mechanism. Due to the dense population in the massive IoT scenario, the increasing connectivity requirements may aggravate the load of the authentication entity and increase the corresponding processing delay, which may further jeopardize the service and affect the quality of the experience. To solve this problem, especially for the case in which the authentication infrastructure is unavailable, a physical layer authentication method is proposed in this paper, which is based on modified physical authentication flow, a modified PDA algorithm based on soft information, and authentication key randomization based on hash mapping. Through Monte Carlo simulations, it is observed that the proposed physical layer authentication mechanism shows a favorable gain compared with that of the existing methods.

INDEX TERMS IoT, physical layer authentication, hash mapping, soft information.

I. INTRODUCTION In the era of the Internet of Things (IoT), all devices that can benefit from Internet connections will be connected, as depicted in figure 1, which may cause explosive growth of the IoT size. Ericsson predicted that approximately 28 billion devices may be interconnected by 2021, which implies a massive deployment and dense population of IoT networks [1]. Compared with the traditional infrastructure-based network, the openness of the wireless link in IoT makes the communication system vulnerable to attack. The performance of the traditional encryption and authentication mechanism mainly depends on the length of the algorithm key with the assumption that the physical layer transmission is secured. However, with the rapid development of computing technology, security protection by increasing the key length does not appear to be feasible. With the support of cloud computing, malicious nodes are able to decrypt the encrypted authentication information through exhaustive search. Additionally, the trends of the massive deployment of IoT may heavily increase the processing burden of conventional network authentication entities, including trusted key management centers, certificate authority, etc., which may ultimately jeopardize the service provision and affect the quality of experience. Furthermore, the absolutely secured physical layer is impossible to achieve, which faces the risks of authentication information leakage, redirection attack and other attacks. To deal with the above problems, the physical layer authentication mechanism has attracted increasing attention from industry and academia [2]–[5].

Studies [6] and [7] utilize the multipath channel state information difference to adaptively identify users and detect abnormal user behaviors. The spatial property of the wireless channel is considered in the proposed physical layer authentication algorithm of [8]. An authentication framework suitable for the time-varying physical layer is proposed in [9], which builds up an autoregressive stochastic process based on the time-varying carrier frequency offset (CFO) to complete the user identification. Furthermore, study in [10] proposes using the unique wireless channel state information (CSI) in the physical layer of a wireless channel as an authentication basis, comparing the CSI of a legitimate node with the subsequent...
transmission message of the node to determine whether it has the same power spectral density, and the authors use the binary hypothesis test for analysis and explanation. Additionally, a coding-based authentication scheme is proposed in [11], where both sides can benefit from information sharing while illegal users can only carry out authentication attacks by guessing. The authors in [12]–[18] carried out research based on watermarking techniques, which include the utilization of spreading techniques in watermarking, joint security certification mechanism design, watermark generation, etc. To accommodate the application trends of OFDM in wireless communication networks, a physical layer challenge-response authentication mechanism (PHY-CRAM) and a physical layer phase challenge-response authentication scheme (PHY-PCRAS) are proposed, which utilize the amplitude and phase to identify the user, respectively; see [19] and [20]. Much research effort has been made in the aspects of physical layer mechanism design, abnormal user detection, CSI information utilization and multicarrier system adaption, but less work has been done regarding authentication information detection and anti-interception ability enhancement.

To enhance the environment adaptability and anti-interception ability of the physical layer authentication algorithm, the conventional challenge-response authentication flow is modified with a new transformation function based on the one-way hash function characteristics to implement the noninvertibility and antifalsification on the key related information. In addition, a soft information-based iterative detection algorithm is proposed to eliminate the effects of time-varying fading channels and noise in order to enhance the detection accuracy of the authentication key response.

The remainder of this paper is organized as follows: The conventional physical layer authentication mechanism is introduced in section 2. Section 3 describes the proposed physical layer authentication mechanism in detail. The evaluation results from Monte Carlo simulations are shown in section 4. Conclusions are drawn in section 5.

II. INTRODUCTION OF THE PHYSICAL LAYER AUTHENTICATION MECHANISM

Physical layer security authentication is an effective supplement to the application layer and transport layer authentication mechanism. A series of influential research results have been applied in sensor networks, cognitive radio and other fields. Compared with the traditional security authentication mechanism, the physical layer authentication mechanism mainly encrypts data at the “information level” to prevent information from being divulged and tampered with, which utilizes the randomness, reciprocity and time-varying property of the wireless channel to improve the security of wireless networks. In the traditional authentication mechanism, the security of the system is guaranteed by designated network entities, which requires the support of wireless or wireline networks and is not suitable for scenarios where the network is unavailable. Additionally, the massive deployment scene of further IoT may increase the burden of the authentication entity and thus extend the authentication processing delay, which may ultimately cause service failure. Therefore, it is an important task to seek an efficient and lightweight authentication scheme to solve the above problems, and the physical layer authentication mechanism may be a feasible approach, especially in the coverage hole scenario [21]–[24].

In the scenario of massive IoT, nodes may directly communicate with others to alleviate the load of network infrastructure and to enhance the connectivity node. To ensure the security of data transmission in this scenario, the legitimacy of node identity needs to be mutually verified. Without loss of generality, the widely used Wyner physical layer authentication model shown in figure 2 is considered in this paper [25]. In this authentication, nodes A and B represent the authentication transmitter and receiver of legitimate nodes, respectively. The two parties have negotiated the authentication protocol based on shared key authentication. The authentication process is carried out according to the authentication protocol based on a shared key without false information transmission to endanger the system security. K represents the authentication shared key that satisfies {KA, KB | K = KA = KB}, KA, KB ∈ {0, 1}. Eavesdropper E represents the illegal node without the information of the shared key K. The illegal node E aims to intercept the shared key K and pretend to be the legitimate node to pass the authentication process further to neutralize the network or acquire the information illegally. In addition, the authentication process in figure 2 is a two-way authentication process, which can also be viewed as two one-way authentication processes with the same procedures. To simplify the description, only the one-way authentication process is considered in this paper.

The detailed flows are as follows:

Step 1: The authentication request node Alice sends a random sequence D, which is used as the authentication excitation.
Step 2: Received signal $DH_{AB} + W^{(1)}$ of Node B is transformed to $F(X_n, B)_{H_{AB}, n} + W^{(2)}_n$ and sent to Node A. $H_{AB, n}$ is the nth channel frequency response between A and B. $W^{(1)}$ is additive white Gaussian noise, and $X_{n, B}$ is the nth element of the shared key. $F(\cdot)$ is a constellation mapping arithmetic; it maps the binary bit 0 and 1 as a positive number; the defined is as follows:

$$F(x) = \begin{cases} K_3, & x = 0 \\ K_4, & x = 1 \end{cases}$$ (1)

Step 3: After receiving $F(X_n, B)_{H_{AB}, n} + W^{(2)}_n$, the shared key-related information is extracted to compare with the stored key to identify the user, and Node B is certified according to the received signal with the shared key $X_{n, B}$. The time used in the whole authentication process above must be characterized by channel reciprocity $H_{AB} = H_{BA}$.

### III. PROPOSED PHYSICAL LAYER AUTHENTICATION ALGORITHM

To enhance the anti-interception ability of the shared key, the unidirectional characteristics of the hash function in chaos theory are utilized in the proposed physical layer authentication algorithm. Additionally, soft information such as prior and post probabilities are introduced in the key detection method in the form of log likelihood ratio to fully utilize the characteristics of the wireless fading channel. Furthermore, the node authentication process is initialized according to the key properties to further improve the accuracy of node authentication detection. The proposed algorithm depends on the characteristics of the wireless fading channel, the relative distance between the two authentication parties, the hash function mapping, etc., with little additional computational complexity compared with that of the conventional algorithms.

#### A. MODIFIED AUTHENTICATION FLOW

To utilize the benefits of the hash function and the soft information on the signal transmission, the convention physical layer authentication flow in Fig 3 are modified as in Fig 4, where the received random sequence $D$ will be detected for noise mitigation and processed using (2) and (3) instead of directly using it as the divider of the response signal in step 2. Additionally, a soft information-based LLR detection processing is inserted to enhance the accuracy of the shared key identification. Due to the hash function-based transformation method in (2), the anti-interception capability of the authentication flow is improved.

$$F_1(\cdot) = \begin{cases} K_1[hash(D, K_i)]_j = 0, & i = A, B, j = 1 \ldots m \\ -K_1[hash(D, K_i)]_j = 0, & i = A, B, j = 1 \ldots m \end{cases}$$ (2)

$$F_2(\cdot) = \begin{cases} K_2, & D_i = 0 \\ -K_2, & D_i = 1 \end{cases}$$ (3)
where \( K_1 \) is the maximum value of the impact response amplitude of the wireless channel, and \( K_2 \) is the reciprocal of the maximum value of the impact response amplitude of the wireless channel, that is, \( K_1 K_2 = 1 \); hash \((D, K_i)\) represents the one-way hash function based on random sequence \( D \) and shared key \( K \).

In this paper, a one-way hash function based on Henon mapping is adopted [26], [27]. The one-dimensional expression of Henon mapping is:

\[
x_{n+1} = 1 - a x_n^2 + b(x_{n-1} - x_n)
\]

where \( a \) and \( b \) represent empirical values that satisfy \( 1.07 < a < 1.09, \ b = 0.3; \ x_n \) is the input value iterated over a range from \(-1.5 \leq x_n \leq 1.5\). Only when the parameter condition is satisfied is the output value of the system random and possessing a chaotic absorption factor, ensuring that the system has the characteristics of noninvertibility and antifalsification.

**B. MODIFIED PDA ALGORITHM**

To improve the efficiency of node identity identification, the probabilistic data assistant (PDA) algorithm [28]–[31] is modified in the modified authentication flow to enhance the noise tolerance and increase the identification accuracy. The PDA algorithm belongs to the suboptimal LLR-based detection algorithm, which calculates the conditional posterior probabilities under the assumption of a multidimensional Gaussian distribution and iteratively updates the calculated probabilities until it converges to detect the transmitted information. Compared with the maximum likelihood detection algorithm, the PDA algorithm has similar performance with reduced complexity.

Assuming the received signal at the receiver is

\[
Y = HX + W
\]

where \( W = [w(0) \ w(1) \ldots w(N-1)]^T \) represents the additive white Gaussian noise vector with mean zero and variance \( \sigma^2 \); \( X = [x(0) \ x(1) \ldots x(N-1)]^T \) represents the transmission signals; and \( H \) is the channel impulse response matrix with \([H]_{m,n} = h(n, m)\) representing the \( n^{th} \) impulse response at the sampling time \( m \). \( Y = [y(0) \ y(1) \ldots y(N-1)]^T \) is the received signal vector. Then, we can rewrite the \( n^{th} \) received symbol \( y(n) \) as

\[
y(n) = h(n, n)x(n) + \sum_{q=0,q\neq n}^{N-1} h(n, q)x(q) + w(n)
\]

Then, we obtain

\[
h(n)x(n) = Y + \sum_{q=0,q\neq n}^{N-1} h(q)x(q) + W
\]

Without loss of generality, it is assumed that the transmission signal \( x(n) \) follows a Gaussian distribution, which makes \( h(n)x(n) \) remain Gaussian distributed with the assumption of slow fading. Thus, the posterior probability density function of \( h(n)x(n) \) can be expressed as

\[
P(h(n)x(n)|y(n)) = \frac{1}{(2\pi)^{\frac{n}{2}} |R_n|^{\frac{1}{2}}} \exp\left\{-\frac{1}{2}(h(q)x(q) - g_n)^H R_n^{-1}(h(q)x(q) - g_n)\right\}
\]

where \( g_n \) and \( R_n \) represent the mean and covariance of \( h(n)x(n) \), respectively, which can be expressed as

\[
g_n = E(h(n)x(n)|Y) = Y - \sum_{q=0,q\neq n}^{N-1} E(x(n)|Y)h(q)
\]

\[
R_n = \text{cov}(h(n)x(n)|Y) = \sum_{q=0,q\neq n}^{N-1} \text{var}(x(n)|Y)h(q)h(q)^H + R_w
\]

where \( R_w \) is the noise variance, and \( E(x(n)|Y) \) and \( \text{var}(x(n)|Y) \) represent the mean value and variance of the symbol, respectively.

\[
E(x(n)|Y) = \sum_{\alpha_i} \alpha_i P(x(n) = \alpha_i|Y)
\]

\[
\text{var}(x(n)|Y) = (\sum_{\alpha_i} |\alpha_i|^2 P(x(n) = \alpha_i|Y)) - |E(x(n)|Y)|^2
\]

In (12) and (13), by defining the modulation index \( Q \), the transmitted bit information corresponding to the \( i^{th} \) transmitted symbol \( \alpha_i = s_i \{s_{i,1} s_{i,2} \ldots s_{i,N}\}, N = \log_2 Q \).

Finally, the log likelihood ratio can be calculated as in (13) based on (8).

\[
L(x(n)|Y) = \ln \frac{P(x(n) = 1|Y)}{P(x(n) = |1|Y)} = 2h(n)^H R_n^{-1} g_n
\]

Observing (13), the calculation of log likelihood ratio relies on the matrix inverse calculation of \( R_n^{-1} \) with the complexity of \( O(N^3) \). Thus, the matrix inverse lemma is utilized here to reduce the matrix inverse calculation complexity. By using the matrix inverse lemma,

\[
R_n^{-1} = R^{-1} + \frac{\text{var}(x(n)|Y) R_n^{-1} h(n) h(n)^H R^{-1}}{1 - \text{var}(x(n)|Y) h(n)^H R^{-1} h(n)}
\]

Similarly,

\[
g_n = g + E(x(n)|Y)h(n)
\]

\[
R = \sum_{q=0}^{N-1} \text{var}(x(n)|Y)h(q)h(q)^H + R_w
\]

To fully utilize the soft information carried by the received symbol and increase the reliability of the symbol detection, the mean and variance of (11) and (12) are iteratively updated until the posterior logarithmic likelihood ratio of (13) converges.
C. SHARED KEY IDENTIFICATION

After the response was received by the excitation node, the shared key related information $T_B = \text{hash}(D, K_B)$ is extracted from the response $F_1(\text{hash}(D, K_B))H_{BA} + W^{(2)}$ by using the modified PDA algorithm. However, due to the unidirectional nature of the hash function, the shared key $K_B$ cannot be obtained directly from the extracted $\text{hash}(D, K_B)$. Instead, the excitation node A will generate a new mapping sequence $T_A = \text{hash}(D, K_A)$ using the same method as the response node B. By measuring the similarity between $T_A$ and $T_B$, the legitimacy of users is identified. The similarity factor $\eta$ is:

$$\eta = \frac{Q - P}{Q + P}$$  \hspace{1cm} (18)

where $Q$ and $P$ represent the number of identical and different bits, respectively. Then, we can use the hypothesis test in (19) to identify the users.

$$\begin{cases} H_0 : \eta < \Gamma & \text{illegal user} \\ H_1 : \eta \geq \Gamma & \text{legal user} \end{cases}$$  \hspace{1cm} (19)

where $\Gamma$ is a predefined threshold to consider the trade-off between user detection and false detection performance.

IV. PERFORMANCE EVALUATION

A. SIMULATION ENVIRONMENT AND PARAMETER CONFIGURATION

To verify the performance of the proposed physical layer authentication algorithm, a Monte Carlo simulation platform is constructed. The detailed parameter configuration and simulation flowchart are shown in Table 1 and figure 5, respectively.

| Parameters                     | Values                                      |
|--------------------------------|---------------------------------------------|
| Carrier Frequency $f_c$       | 2.4 GHz                                     |
| Absolute Speed of Vehicle Movement $v$ | 50 km/h                                     |
| Shared Keys Length $N$        | 128                                         |
| Channel Model                 | Rayleigh Fading Model Ricean Fading Model   |
| Modulation Method             | BPSK                                        |
| Multipath Number $L$          | 4                                           |
| Relative Power $P$            | $[0, -10, -20, -25]$                       |
| Relative Time                 | $[0, 2, 3, 4]$                              |
| Hash Function                 | Henon Map                                   |

B. EVALUATION RESULTS

Figure 6 shows the distribution diagram of chaotic absorption factors based on the Henon map in (4). It can be seen from the figure that the sequence has uniform distribution and random noise characteristics, which satisfies the basic conditions for the construction of a one-way hash function.
and PHY-CRAM algorithms. From the results, it is observed that the proposed physical layer authentication method outperforms the conventional PHY-CRAM algorithm by at least 15% in terms of legal user detection probability while maintaining a similar false alarm detection probability, especially in the low SNR region where the PHY-CRAM algorithm cannot work.

Figures 8 and 9 present the ROC performance comparison with SNRs of 0 dB and 8 dB under Rayleigh and Ricean fading channels, respectively, which are the two most widely used channel models. From the figure, we find that the proposed authentication algorithm outperforms the conventional algorithm for most threshold selections in the case of 0 dB, irrespective of the channel models, due to the utilization of soft information in detection steps. However, the performance gain provided by the proposed algorithm is reduced when the SNR is increased to 8 dB because the effects of noise are smaller than those in the scenario of 0 dB. The observations of ROC performance are also consistent with the results shown in Fig. 7.

V. CONCLUSION

In this paper, a physical layer authentication algorithm is proposed to deal with security problems in situations where the conventional security infrastructure is not available. Additionally, the proposed physical layer authentication algorithm is able to cooperate with a conventional high-layer mechanism to enhance the system security, which may be extended to IoT applications in service scenarios requiring a high network security level, such as C-V2X in the 5G networks. From the simulation results, we found that the proposed algorithm outperforms the conventional algorithm, especially in the case of a low SNR, due to the introduction of soft information on the shared key-related information detection. In addition to the random sequence transmission in the conventional physical authentication flow, hash mapping is introduced to reduce the interception probability of the shared key-related information transmission by utilizing its unidirectionality, which may prevent key leakage and protect the system from passive or active attack.

REFERENCES

[1] C. Kuhlins, B. Rathonyi, A. Zaidi, and M. Hogan, “Cellular networks for massive IoT,” Ericsson, Stockholm, Sweden, White Paper Uen 284 23-3278, Jan. 2020.
[2] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” IEEE Commun. Surveys Tuts., vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.
[3] K. Zeng, “Physical layer key generation in wireless networks: Challenges and opportunities,” IEEE Commun. Mag., vol. 53, no. 6, pp. 33–39, Jun. 2015.
[4] X. Wang, P. Hao, and L. Hanzo, “Physical-layer authentication for wireless security enhancement: Current challenges and future developments,” IEEE Commun. Mag., vol. 54, no. 6, pp. 152–158, Jun. 2016.

[5] C. D. T. Thai, J. Lee, and T. Q. S. Quek, “Physical-layer secret key generation with colluding untrusted relays,” IEEE Trans. Wireless Commun., vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[6] X. Wu and Z. Yang, “Physical-layer authentication for multi-carrier transmission,” IEEE Commun. Lett., vol. 19, no. 1, pp. 74–77, Jan. 2015.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “A physical-layer technique to enhance authentication for mobile terminals,” in Proc. IEEE Int. Conf. Commun., 2008, pp. 1520–1524.

[8] F. J. Liu, X. Wang, and H. Tang, “Robust physical layer authentication using inherent properties of channel impulse response,” in Proc. Mil. Commun. Conf. (MILCOM), Nov. 2011, pp. 21–21.

[9] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, “Physical layer authentication for mobile systems with time-varying carrier frequency offsets,” IEEE Trans. Commun., vol. 62, no. 5, pp. 1658–1667, May 2014.

[10] J. K. Tugnait, “Wireless user authentication via comparison of power spectral densities,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[11] H. Song, L. Jin, and X. Wang, “A method for security authentication of wireless network physical layer,” J. Xi’an Jiaotong Univ., vol. 52, no. 4, pp. 105–110, 2018.

[12] C. Shrikishan, N. Kaberi, and P. Jeebananda, “Double layered audio zero-watermarking using DWT & DSSS,” in Proc. Int. Conf. Commun. Signal Process. (ICCPSP), Apr. 2017, pp. 419–423.

[13] S. Soderi, L. Mučchi, M. Hamalainen, A. Piva, and J. Iinatti, “Watermark-based secure communications in safety-related scenarios,” in Proc. 10th Int. Symp. Med. Inf. Technol. (ISMITC), Mar. 2016, pp. 1–5.

[14] L. Zhou, D. Wu, B. Zheng, and M. Guizani, “Joint physical-application layer security for wireless multimedia delivery,” IEEE Commun. Mag., vol. 52, no. 3, pp. 66–72, Mar. 2014.

[15] N. Goergen, T. C. Clancy, and T. R. Newman, “Physical layer authentication of wireless network communications through synthetic channel emulation,” in Proc. IEEE Symp. New Frontiers Dyn. Spectr. (DySPAN), Apr. 2010, pp. 1–7.

[16] P. Yu, J. Baras, and B. Sadler, “Physical layer authentication,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[17] J. Kleider, S. Gifford, S. Chapurn, and B. Fette, “Radio frequency watermarking for OFDM wireless networks,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., May 2004, pp. V–397.

[18] F. Pan, “Physical layer authentication based on channel information and machine learning,” in Proc. IEEE Conf. Comput. Netw. Secur. (CNS), Las Vegas, NV, USA, Nov. 2017, pp. 364–365.

[19] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, “PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[20] X. Wu and Z. Yang, “Physical-layer authentication for multi-carrier transmission,” IEEE Commun. Lett., vol. 19, no. 1, pp. 74–77, Jan. 2015.

[21] L. Zhou, D. Wu, B. Zheng, and M. Guizani, “Joint physical-application layer security for wireless multimedia delivery,” IEEE Commun. Mag., vol. 52, no. 3, pp. 66–72, Mar. 2014.

[22] X. Qiu, J. Ting, S. Wu, and M. Hayes, “Physical layer authentication enhancement using a Gaussian mixture model,” IEEE Access, vol. 6, pp. 53583–53592, 2018.

[23] L. Yang, J. S. Baras, and B. M. Sadler, “Physical-layer authentication,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[24] B. Lebold, “Physical layer watermarking of binary phase-shift keyed signals using standard gnuradio blocks,” M.S. thesis, School Elect. Comput. Eng., Oklahoma State Univ., Stillwater, OK, USA, 2011.

[25] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[26] L. Zhou, D. Wu, B. Zheng, and M. Guizani, “Joint physical-application layer security for wireless multimedia delivery,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[27] Y. Wang et al. (Senior Member, IEEE) received the B.S. degree in communication engineering from Northeastern University, China, in 2004, and the master’s and Ph.D. degrees in information and telecommunications engineering from Inha University, South Korea, in 2006 and 2010, respectively. He is currently an Associate Professor with the College of Electronic and IT Engineering, Shenyang Aerospace University, China. His research interests include mobile networks, the IoT, smart antennas, radio resource management, and network security.

[28] Y. F. Li received the B.E. degree in communication engineering from Beijing Jiaotong University, China, in 1991, the master’s degree in communication systems from Jilin University, China, in 2002, and the Ph.D. degree in optical engineering from the Changchun Institute of Optics, Fine Mechanics and Physics, China, in 2006. He is currently a Professor with the College of Electronic and IT Engineering, Shenyang Aerospace University, China. His research interests include image processing and transmission technologies, wireless and mobile communication technologies, and avionics information technology.

[29] C. Shrikishan, N. Kaberi, and P. Jeebananda, “Double layered audio zero-watermarking using DWT & DSSS,” in Proc. Int. Conf. Commun. Signal Process. (ICCPSP), Apr. 2017, pp. 419–423.

[30] J. Luo, K. R. Pattipati, and P. K. Willett, “Near-optimal multiuser detection in synchronous CDMA using probabilistic data association,” IEEE Commun. Lett., vol. 5, no. 9, pp. 361–363, Sep. 2001.

[31] D. Pham, J. Luo, K. Pattipati, and P. Willett, “A PDA-Kalman approach to multiuser detection in asynchronous CDMA,” IEEE Commun. Lett., vol. 6, no. 11, pp. 475–477, Nov. 2002.