IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 22, 2018, accepted April 24, 2018, date of publication May 3, 2018, date of current version June 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2832839

Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges

YUAN GAO[1,2,3], (Member, IEEE), SU HU[3], (Member, IEEE), WANBIN TANG[3], (Member, IEEE), YI LI[4], (Member, IEEE), YUNCHUAN SUN[5], (Senior Member, IEEE), DAN HUANG[3], SHAOCHI CHENG[1], AND XIANGYANG LI[1]

[1]Academy of Military Science of PLA, Beijing 100091, China
[2]State Key Laboratory on Microwave and Digital Communications, National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China
[3]University of Electronic Science and Technology of China, Sichuan 610054, China
[4]The High School Affiliated to Renmin University of China, Beijing 100081, China
[5]Business School, Beijing Normal University, Beijing 100875, China

Corresponding authors: Yuan Gao (yuangao08@tsinghua.edu.cn) and Su Hu (husu@uestc.edu.cn)

This work was supported in part by National Natural Science Foundation of China under Grant 61701503. The work of S. Hu was supported by the MOST Program of International S&T Cooperation under Grant 2016YFE0123200, in part by the National Natural Science Foundation of China under Grant 61471100, Grant 61101090, and Grant 61571082, in part by the Science and Technology on Electronic Information Control Laboratory under Grant 6142105040103 and in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2015J012 and Grant ZYGX2014Z005.

ABSTRACT The increasing demand in 5G wireless systems has brought significant improvement in transmission speed with lower latency, especially in ultra-dense networks. The demand of privacy and security are becoming more critical in such large scale wireless networks. Different from traditional encryption methods, in this paper, we discussed the physical layer security features in large scale social networks. The opportunities in large scale social networks are summarized in physical, link and upper layer using the cross layer optimization, traditional physical layer security will meet new problems pending to be tackled. Also, we summarized the challenges due to some ideal considerations: the detection of wire-tap users, the utilization of high dynamic range and the information exchanging in cross layer design.

INDEX TERMS Physical layer, security, large scale, social network, 5G.

I. INTRODUCTION

With the development of wireless personal mobile communication systems, the increasing amount of mobile terminals with higher computational ability has brought additional load to current network structure. In social networks, users are connected together according to the similarity of their social activities, where not only physical connections are studied, but also logical connections must be considered, e.g. friends will be connected together even the physical distance is large. However, the social network will brought out severe security problems due to the leakage of information and eavesdrop from the network devices.

Encryption is one effective solution to protect security and privacy in social networks [1]. The encryption methods are always working in application layer, the security level is relying on the strength of the encryption method, e.g. the AES-256 [2]. However, the security operation in application layer is insufficient to provide satisfied security options, especially in mobile networks [3]. The wireless signal is spreading in the free space and not only the authorized user could receive the information but also the adjacent illegal user could obtain wireless power [4]–[6] and retrieve secured information from the power leakage in wireless signals. In this way, the physical layer security is raised to avoid the wireless leakage and strengthen the security level of the information [7]. There are plenties of scholars studying physical layer security in 5G related wireless systems. A new measurement in physical layer security is discussed in [8], which is different from traditional security rate, the new measurement named secrecy pressure could provide more details of security. The influence of social awareness is considered in [9], and in [10] and [11], the link level clustering and OFDM optimization are discussed but the scale is still small. In [12] and [13], the physical layer security in full-duplex networks is studied, which is the key technique in 5G network. The above discussions are mainly focused on small scale networks, the increasing number of users will bring significant difference in modeling and solution. So Kamel *et al.* [14]discussed the problem in UDN scenario, similar as large scale social networks, the modeling and artificial noise are raised and optimized. Then in [14]–[17], the physical and link layer procedures are presented to enhance the security level using channel awareness, adaptive modulation and coding (AMC). Thus, the influence of channel model is also discussed in [18], where typical Rician/Nakagami-m Fading Channels are considered and in [19], the Millimeter Wave network is studied due to the need to enhance transmission speed.

According to the above references, it can be inferred that, the physical layer security is an effective way to enhance security rate despite of upper layer encryption. However, the scale of the network in current studies are quite small, which is not suitable for large scale social networks. In this work, we mainly focus on the security issues of physical layer in large scale social networks. And, both physical and logical connections will affect the performance of network security. The rest of the paper is organized as follows.

In part II, we discuss the characteristics of the physical layer security in large scale social networks, in III, we summarize the opportunities of physical layer security in social networks and on the contrary, we discussed the challenges in part IV. Finally, conclusion is given with summary and outlook.

II. CHARACTERISTICS OF PHYSICAL LAYER SECURITY IN SOCIAL NETWORKS

In the existing safety network architecture and operations, most of the security measures are based on the key and the encryption algorithm. This encryption system is working above the physical layer (in MAC layer, network layer, application layer, etc.) In wireless communication systems, the eavesdropper can easily receive the signal transmitted through the physical layer, that is, the cipher text of the upper layer security. When the eavesdropper intercepts a large amount of cipher text, it is possible to find easy ways to get the key parameters that determines the security of the system. Eavesdroppers cannot receive or correctly decoded the received information when physical layer security is considered, then the security level will be greatly improved. At present, multi-antenna multi-carrier technology is widely used in wireless communication systems, and multi-antenna multi-carrier is introduced into network standards such as wireless LAN, wireless metropolitan area network and 5G. Both of these technologies bring more space and frequency freedom to secure physical layer transmission. It is necessary to study the security of physical layer transmission, which will improve the security performance of existing wireless communication systems to a certain extent.

The physical layer security is known as Alice-Bob-Eve model as illustrated in figure 1, which means, Alice and Bob are communication with each other but Eve is the wiretap user and could receive power from wireless spreading in an illegal way, through the wiretap channel. The wire-tap user could use the information to destroy, attack and interfere the target user.

Traditional information theory indicates that, Eve may get the zero mutual information through coding with the expression $I\left(W;Z^n\right) = 0$, at the same time, Bob could receive decoded signal expressed as $\hat{w} = I\left(X;Y\right) - I\left(X;Z\right)$ in single carrier systems (notations are given in figure 1). It is also known as security rate, the security rate greater than zero can be obtained only when the channel gain of the main channel is higher than the channel gain of the intercepted channel. In other words, if you want to ensure secure transmission, you must ensure that there is no eavesdropper within the range closer to the legitimate recipient than the sender. The security rate in MIMO scenario is expressed in equation (1) [20]:

$$C_s = \max_{Q:Q\geq 0, Tr(Q)\leq P} \left[\log\left|I + HQH^H\right| - \log\left|I + GQG^H\right|\right] \tag{1}$$

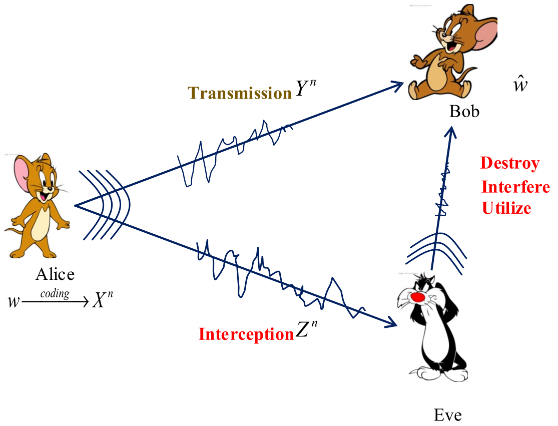


FIGURE 1. Traditional Alice-Bob-Eve Model. The wire-tap user may use the illegal information to destroy, attack or interfere with target user.

In figure 2, we describe the scenario in large scale social networks. Traditional physical layer security problem only focuses on physical connections, that means, only adjacent users may intercept signal from wireless spreading. But in

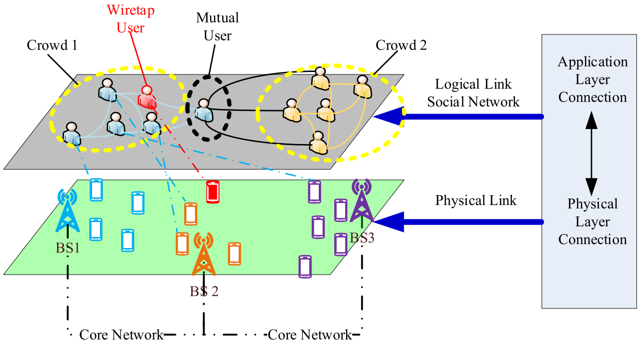


FIGURE 2. Physical Layer Security in Large Scale Social Networks.

large scale social networks, both physical link and logical link is considered. In physical link, mobile users are located within the range of base stations (BSs), wire-tap user(s) is hidden inside the normal user(s) and receive wireless power to decode useful information. Despite of the encryption in application layer, only if the received power makes it possible to decode the information through possible mathematical methods. It is clear that if the distance between target user and wire-tap user is long, the interception will not succeed. In logical link in large scale social networks, users are connected through their social attributes, such as classmates, family members, etc. There is a one-to-one correspondence between logical and physical link, the users in logical link level are mapped to physical link one by one, and the mapping is unique. For different users in social networks, they can be sorted into different crowd and this sorting is not unique. The connection in logical link is also called a graph [21]. As known, the complexity of the graph would increase more quickly while the scale of the network increases. This lead to the problem and chance to study the physical layer security in such environment.

III. OPPORTUNITIES OF PHYSICAL LAYER SECURITY IN LARGE SCALE SOCIAL NETWORKS

The increasing scale of network has brought complexity in management, resource allocation, etc., but also provide opportunities to discuss new scenarios and problems. The opportunities are sorted by the OSI architecture.

A. PHYSICAL LAYER

Physical layer security mainly makes the use of special channel coding and random characteristics of wireless channels to secure the communication. It differs from modern cryptography that the degree of security does not depend on the calculated strength of Eve, but relies on the channel environment with random features. However, in terms of confidentiality, physical layer security has the essential similarities with the traditional cryptology of computing cryptography. Physical layer security in the coding, modulation and channel randomness is a necessary condition for secure communications, as in the modern cryptography encryption algorithm. The coding and modulation mean that Alice assures a safe and reliable communication between Alice and Bob through unique channel coding according to Alice-Bob and Alice-Eve channels. From the security point of view, the coding and modulation environment can be regarded as the encryption process in modern cryptography, and the cipher text generated after the information encryption is recorded as X_n. Cipher text can be regarded as the decryption part of modern cryptography through wireless channels and demodulation and decoding. The channel information $\{h, g\}$ can be regarded as the public key, and the noise σ_b of Bob can be regarded as Bob's private key, Eve is unable to get such information. Therefore, cipher text can be decoded and decrypted by Bob correctly through Bob's wireless channel, and Eve cannot obtain any information through Eve's wireless channel and demodulation decoding. Thus, although the physical layer security and traditional cryptography based on modern cryptography are completely different, but they can also find common ground in the implementation framework. Physical layer security can be seen as modulation and coding technologies such as sending end encryption algorithm, take full advantage of the Alice-Bob and Alice-Eve wireless channel differences, the wireless channel as an ''encryption key'', so that Alice and Bob form a secure and reliable communication.

Opportunities in physical layer optimization are still open. Previous studies in physical layer are mainly in small scale scenario, so in large scale social networks, operations that may avoid the receiving of wireless power is still uncertain, especially in dynamic scenario. In figure 3, we propose the possible opportunities in beamforming, power control and joint clustering.

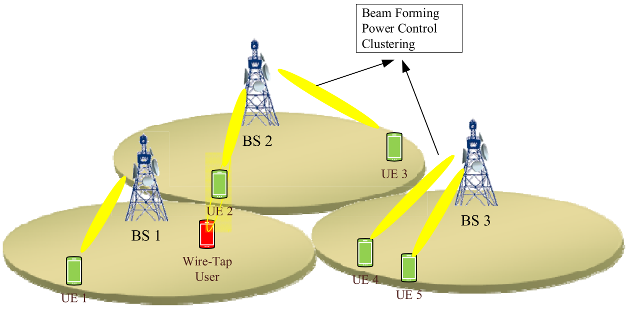


FIGURE 3. Opportunities in large scale social networks.

Power control means when detecting the existence of wire-tap user and the position of the illegal listener, the base station side or the user side must control the transmission power to prevent the wire-tap user receiving any information, just like the scenario in figure 3, especially when the illegal user and the target user are locating in line. In this way, the precise dynamic power control is in great need and related study is rarely blank according to recent publications.

Beamforming is also a useful method to avoid the leakage of transmission power. Assuming the global information of wire-tap users, a rapid beamforming and switching using mechanical or electrical [22] method. Usually, this operation is jointly operated with power control, to increase the transmission speed and reduce the leakage of transmission power. However, the scholars only discovered the bound of the joint optimization, but lack of practical implementation, e.g. the practical algorithm and heuristic algorithm.

Clustering is the method to stick similar users together and form a group, which is suitable for large scale social networks. Considering the interception of illegal users, the system must recognize the target users and form them a group, within which the illegal users will be excluded from such clusters. The opportunities in current studies are how to make the cluster dynamic and optimal, for the channel condition and the data traffic are dynamic.

B. LINK LAYER

In link layer, the modulation and coding are mainly focused. Traditional optimization in modulation and coding is to increase the transmission speed according to different channel conditions, which is also known as adaptive modulation and coding (AMC). In the scenario of physical layer security, the AMC need to be optimized in a new manner. The target of AMC in physical layer security is to jointly design and increase the speed of target users but reduce the speed of illegal users, e.g., we can use higher order modulation and coding when the channel condition is poor between transmitter and the illegal user, through which the bit error rate will be significantly increased.

When the modulation is PSK, the input signal could not be modeled as Gaussian but discrete, as is shown in figure 4. The x-axis means the SNR in dB and the y-axis means the security capacity, the curves reflect the trends of Gaussian, 16QAM and QPSK [23]. When the modulation is not ideal, the combination of modulation and coding in adaptive way will form new optimization problem in such scenario.

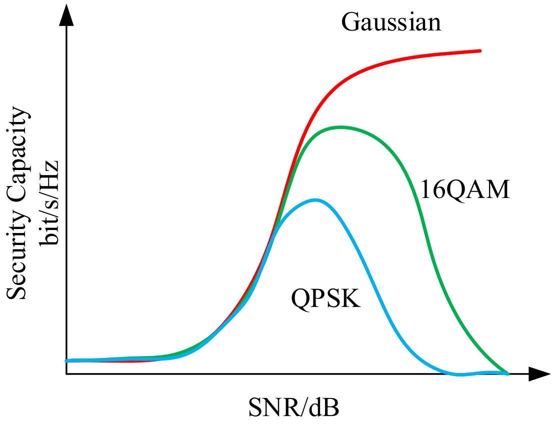


FIGURE 4. Discrete input in physical layer security.

C. CROSS LAYER

Single layer optimization is simple for its ideal assumptions and considerations. The joint optimization is to make the cross layer design using artificial noise, power control, AMC, etc. to make the security rate increase in large scale social networks.

Based on artificial noise, the system resources need to be optimally configured to maximize the system's safe transmission efficiency. Considering the subcarrier power allocation in OFDM system and the optimization of artificial noise, the rate of OFDM system is improved. Therefore, the cross-layer resource optimization is not limited to the Gaussian signal in theoretical research, but also to discrete constellation inputs commonly used in real systems (such as QAM and PSK modulation). Due to the different distribution of channel input, the relationship between the security rate and the transmission power is different.

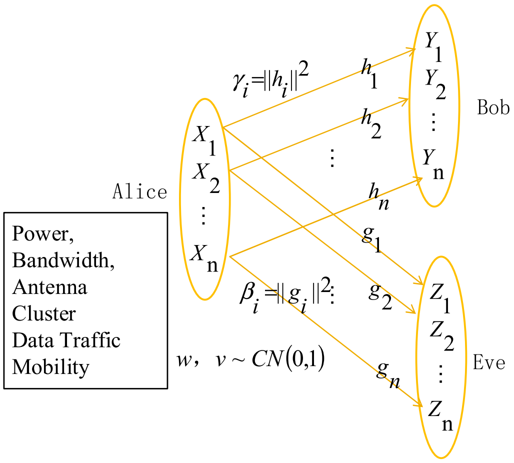


FIGURE 5. Multicarrier system using cross layer design.

In 5G related wireless networks, multicarrier transmission is considered, the proposed security rate is proved to be the sum of each subcarriers: $C_S = \sum_{i=1}^{n} [I(X_i; Y_i) - I(X_i; Z_i)]$ as is shown in figure 5. In the cross layer design, the variables pending to be optimized are located in different layers. Considering the characteristics of social networks, the optimization must contain the influence in application layer, such as the traffic model, connection graph, etc. The joint optimization of such factors could be expressed using the following equation:

$$\begin{aligned} &\min_{w,\sum} \ tr\left(ww^H + \sum\right) \\ &s.t. \ \log\left(1 + \frac{w^H hh^H w}{h^H \Sigma h + \sigma_n}\right) \geq \gamma_h \\ &\max_{m\in\{1,2,\ldots,M\}} \log\left(1 + \frac{w^H g_m g_m^H w}{g_m^H \Sigma g_m + \sigma_n}\right) \leq \eta\gamma_h \end{aligned} \tag{2}$$

The above optimization is not convex and the solution is still an open target.

IV. CHALLENGES OF PHYSICAL LAYER SECURITY IN LARGE SCALE SOCIAL NETWORKS

In large scale social networks, physical layer security has its new opportunities in layers and the combination optimization, considering the scale and connectivity of the network, however, there are still some assumptions and parameters we must consider as ideal, which will limit the use of the physical layer security.

Physical layer security is independent to upper layer security operations. Therefore, in the wireless communication system, the security of the physical layer transmission can be supplemented while the existing upper layer security measures remain the same. This may provide extra protection to target systems. On the other hand, the use of physical layer security to transmit cryptographic keys is also a way of enhancing the system security. In current communication system, the password encryption is adopted in many layers, the PGP encryption mechanism is adopted in the application layer, and the data is transmitted through the TLS mechanism in the transport layer, the IPsec mechanism in the network layer and the WPA security link in the link layer Encryption of layers. The application of physical layer security for these data adds a layer of security, making the system further enhance the safety performance.

A. DETECTION AND MODELING OF WIRE-TAP USERS

In the above discussion, we have a strong assumption that all the wire-tap users are detected and the information is global. In fact, we cannot discover the wire-tap users if they do not attack or perform harmful injection to the normal data, it is because the spreading and the reflection of wireless signals could not be controlled, even if the beamforming operation is performed.

So if the wire-tap users are working in passive mode, the transmitter will need to add artificial noise to the orthogonal space of the target users, which means all the space that do not belongs to the target users is assumed to have eavesdropper. If the wire-tap users are working in active mode, that means the users will measure the channel condition in active mode and send interference signal or fake messages to the normal communication, the transmitter could detect the illegal behavior of wire-tap users and restrict the activity of such users.

In large scale social networks, such problems become critical and harder. In figure 6, we illustrate the changes between small scale and large scale network. The logical connection may confuse the identification of wire-tap users, and when the number of wire-tap users grow bigger, the physical operations such as power control and beamforming may not work well for the beam could not be separately in such small angles. So how to identify and model such users are still quite uncertain in current researches.

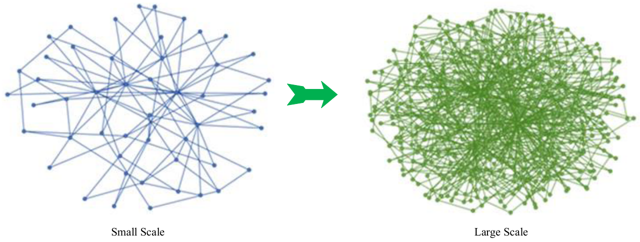


FIGURE 6. Scale of social networks and challenges for physical layer security.

B. HIGH DYNAMIC RANGE OF THE SCENARIO

In social networks, modeling of traffic data is very important, the connection from multiple objects will significantly increase the complexity of the network, and the optimization will be hard. In application layer, typical clients such as WeChat could provide text/audio message, p2p video or group chat. To describe the connectivity and the demand of transmission, we must model the traffic considering the high dynamic range of such traffic data.

The traditional model cannot accurately describe the network traffic. For example, through the modeling of existing models such as http and ftp data, it is bound to ignore the delay tolerance and bandwidth of the service. Therefore, by analyzing the large-scale social network again, the characteristics of existing networks and using multiple parameters to re-describe the network services is the basis for implementing physical layer security using service aggregation and scheduling.

In table 1, we listed the possible influence factors that need to be considered. For example, in the high-speed video transmission service (video conference), due to the delay tolerance of the voice and image itself, it is decided that the granularity is about 2M videos transmitted every 500 milliseconds (taking 480p as an example). Therefore, t_g and l_g are 500ms and 2M; and for access request service, the single transmission tolerance of about 20ms, the amount of data is usually less than 1k, so the corresponding, respectively, t_g and l_g are 20ms and 1k. Here, 1k / 20ms is not equivalent to 50k /s, because time granularity is defined, that means, the delay tolerance of service transmission. This is also the main difference with the traditional average rate and interrupt probability as the research object. The arrival rate, which reflects the number of arriving events per unit time, is a frequency parameter. The primary physical scenario is the delay that allow the switch or router node to schedule and process traffic. It shows the correlation between the business, according to the above shortcomings of the direct separation, it should be realized that some business data and control data have something similar, and different control or business data may also vary greatly, it should be based on the transmission Need to move closer, should not simply be distinguished from the data type. Therefore, the more relevant data are more likely to be mapped to the same layer for service, thereby maximizing the use of system resources.

TABLE 1. Traffic model for high dynamic range [24].

Symbol	Name	Description
t_g	delay tolerance	Allowable delay for traffic data, characterizing time granularity
l_g	minimum amount of data	Minimum amount of data within the observation interval t_g
N_g	total amount of traffic data	Total packets, amounts
λ	arrival rate	Characterize the number of arrivals for these events
w_g	waiting parameter	The allowable waiting time before an event is mainly caused by the operation of the users
ρ	correlation	Define the correlation between different businesses, the strength of the correlation affect the mapping principle

C. INFORMATION EXCHANGE IN CROSS LAYER OPTIMIZATION

The assumption of global information among layers is also considered in current studies. However, information exchanging through different layers is also a complex problem need to be discussed.

In figure 7, we describe the cross layer information delivery and the security operations. In physical layer, data will be transmitted through the wireless link, the information required is: channel condition, connection map (upper layer), traffic model (upper layer), and the optimization is to allocate the antenna, power/bandwidth and clustering to enhance system security. In link layer, the modulation and coding is considered, information for modulation and coding is channel condition, real time traffic monitoring (upper layer), and the potential physical layer encryption operations are AMC and artificial noise. In network layer, the target is to choose the right link to transmit the data with low latency and interferences. Information required to perform optimization is connection map (upper layer) and traffic model (upper layer), so the potential operations for this layer is dynamic routing and link selection. It is clear that no more information is required from lower layers, such as channel information, wire-tap channels, etc. So this optimization is sometimes independent. And the layers higher than network layer is considered as upper layer, so the influence is mainly about the application. For example, WeChat software will encrypt the information using AES 256, by considering the traffic model, etc. But this operation will need the information of channel information to perform hybrid transmission and risk detection. The result of risk detection will be transferred to lower layer to ensure the existence and the position of the wire-tap users.

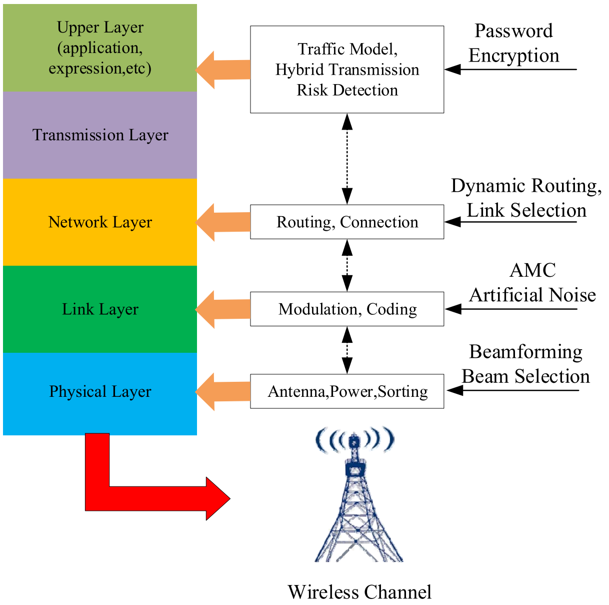


FIGURE 7. Cross Layer Information Exchanging in Large Scale Social Networks.

It is obvious that the information from different layers must be shared to ensure the accuracy of the physical layer security, but there is not suitable mechanism to exchange information, because different layers will only proceed with its own frame, the header of the frame only contains the information that need to be processed.

V. CONCLUSION

In this paper, we discussed the physical layer security in large scale social networks. Considering the traffic model and demand of applications, physical layer security could enhance system security level through system layer, link layer and cross layer optimization. However, there are still ideal assumptions that limit the utilization of physical layer security. As a review article, in this paper, we propose some new opportunities for physical security in 5G based large social networks which we should mention in future works.

ACKNOWLEDGMENT

The author would like to thank all the reviewers and editors with this work, for their kind suggestions and help to make this work better.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[3] M. Atallah, G. Kaddoum, and L. Kong, “A survey on cooperative jamming applied to physical layer security,” in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Montreal, QC, Canada, Oct. 2015, pp. 1–5.

[4] M. H. Yılmaz and H. Arslan, “A survey: Spoofing attacks in physical layer security,” in *Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops)*, Clearwater Beach, FL, USA, Oct. 2015, pp. 812–817.

[5] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, “A survey on multiple-antenna techniques for physical layer security,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.

[6] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, “Beamforming in wireless energy harvesting communications systems: A survey,” *IEEE Commun. Surv. Tuts.*, to be published, doi: 10.1109/COMST.2018.2797886.

[7] L. Sun and Q. Du, “Physical layer security with its applications in 5G networks: A review,” *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[8] L. Mucchi, L. Ronga, K. Huang, Y. Chen, and R. Wang, “A new physical-layer security measure—Secrecy pressure,” in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–6.

[9] Y. Xu, H. M. Wang, Q. Yang, K.-W. Huang, and T. X. Zheng, “Cooperative transmission for physical layer security by exploring social awareness,” in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Singapore, Dec. 2017, pp. 1–6.

[10] M. Iwata, K. Yamamoto, T. Nishio, and M. Morikura, “Dependent interferer arrangement for physical layer security: Secrecy outage probability in clustered wireless networks,” in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–6.

[11] H. M. Furqan, J. M. Hamamreh, and H. Arslan, “Enhancing physical layer security of OFDM systems using channel shortening,” in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[12] A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. K. Wong, “Physical layer security in full-duplex cellular networks,” in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Feb. 2017, pp. 1–5.

[13] N. H. Mahmood, I. S. Ansari, P. Popovski, P. Mogensen, and K. A. Qaraqe, "Physical-layer security with full-duplex transceivers and multiuser receiver at eve," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4392–4405, Oct. 2017.

[14] M. Kamel, W. Hamouda, and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 690–693, Oct. 2017.

[15] S. V. Pechetti, A. Jindal, and R. Bose, "Channel-based mapping diversity for enhancing the physical layer security in the Internet of Things," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–6.

[16] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 9931–9942, Nov. 2017.

[17] M. H. Taieb and J.-Y. Chouinard, "Physical layer security using BCH and LDPC codes with adaptive granular HARQ," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Las Vegas, NV, USA, Oct. 2017, pp. 564–569.

[18] S. Iwata, T. Ohtsuki, and P. Y. Kam, "Performance analysis of physical layer security over Rician/Nakagami-m fading channels," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–6.

[19] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 1139–1152, Mar. 2018.

[20] E. M. Ghourab, A. Mansour, M. Azab, M. Rizk, and A. Mokhtar, "Towards physical layer security in Internet of Things based on reconfigurable multiband diversification," in *Proc. 8th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Vancouver, BC, Canada, Oct. 2017, pp. 446–450.

[21] T. Q. Duong, "Keynote talk #1: Trusted communications with physical layer security for 5G and beyond," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Quy Nhon, Vietnam, Oct. 2017, p. xxxiv.

[22] N. M. O. Silva and C. V. Cordero, "Towards physical layer security systems design using game theory approaches," in *Proc. CHILEAN Conf. Elect., Electron. Eng., Inf. Commun. Technol. (CHILECON)*, Pucon, Chile, Oct. 2017, pp. 1–6.

[23] J. Chen, L. Yang, and M. S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2017.2789223.

[24] Y. Gao, H. Ao, Z. Feng, W. Zhou, S. Hu, and X. Li, "Modeling and practise of satellite communication systems using physical layer security: A survey," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE) IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Guangzhou, China, Jul. 2017, pp. 829–832.

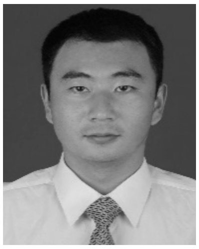
YUAN GAO (S'11–GS'14–M'16) received the B.S. degree in information engineering from PLA Information Engineering University in 2008, the master's degree in communication engineering from Tsinghua University in 2011, and the Ph.D. degree in communication engineering in 2014. He is currently an Assistant Researcher with the Academy of Military Science of PLA, a Distinguished Associate Professor at UESTC, and a Distinguished Assistant Professor with Tsinghua University. He has published over 60 academic papers in peer-reviewed international journals and conferences. His research interests include wireless communication system, satellite communication system, network control theory and big data. He is a member of the ACM. He also serves as a Guest Reviewer and a TPC Member of several journals and international conferences, including the IEEE JSAC, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATION, the IEEE TRANSACTIONS ON COMMUNICATION, the IEEE SYSTEM JOURNAL, the IEEE COMMUNICATION LETTER, ICC, and WCNC. He is an Associate Editor for several international journals, including the IEEE ACCESS, the *EURASIP JWCN*, and *Sensors*. He is also a guest editor of several special issues.

SU HU received the M.S. and Ph.D. degrees from the National Key Laboratory on Communications, University of Electronic Science and Technology of China (UESTC) in 2007 and 2010, respectively. From 2011 to 2012, he was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He is currently a Full Professor at UESTC. His research interests include sequence design with good correlation properties and physical layer design for wireless communication systems, such as filter bank multicarrier systems and cognitive radio networks.

WANBIN TANG received the B.S. and M.S. degrees from the University of Electronic Science and Technology of China (UESTC) in 1993 and 1998, respectively. He is currently a Professor at UESTC. His research interests include MIMO and adaptive signal processing technology in wireless communication.

YI LI (M'15) received the B.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2009, and the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, in 2014. She is currently with The High School Affiliated to Renmin University of China, Beijing.

YUNCHUAN SUN received the Ph.D. degree from the Institute of Computing Technology, CAS, in 2009. He is a Professor with the Business School, Beijing Normal University. His research interests include big data, IoT, semantic technologies, and information security. He is the Secretary of the IEEE Communications Society IoT Technical Subcommittee and the acting Chair of the ETTC TF on Smart World at the IEEE CIS. He is an Associate Editor of the *Personal and Ubiquitous Computing* and has been one of the founders of IIKI series events since 2012.



DAN HUANG received the B.S. and M.S. degrees in computer science and softer engineering from the University of Electronic Science and Technology of China in 2007 and 2011, respectively, where he is currently pursuing the Ph.D. degree in computer science.

SHAOCHI CHENG received the bachelor's degree from Tsinghua University in 2008 and the master's degree from the China Defense Science and Technology Information Center in 2011. He is currently a Research Assistant with the Academy of Military Science of the Chinese People's Liberation Army. His research interests include satellite communication system and data analysis of satellite data.

XIANGYANG LI received the B.S. degrees from Beijing Normal University and the M.S. degree from the National Defence University of People's Liberation Army. He is currently an Associate Researcher with the Academy of Military Science of PLA.