様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 １５ 日現在

機関番号：１４６０３
研究種目：若手研究
研究期間：2019～2021
課題番号：１９Ｋ１４９８３

研究課題名（和文）5G時代におけるIoT無線通信の物理層セキュリテイに関する研究

研究課題名（英文）Physical layer security of IoT wireless communications in the 5G era

研究代表者
張　元玉（ZHANG, YUANYU）

奈良先端科学技術大学院大学・先端科学技術研究科・助教

研究者番号：９０８０４０１３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：無線チャネルに固有の物理層の特性を活用することにより、モバイルアドホックネットワークやミリ波通信システムなど、5G時代の代表的なIoT無線通信を保護するための物理層セキュリティ方式を提案した。また、提案された方式のセキュリティ性能を分析するための理論的フレームワークを開発し、ネットワークの最適なセキュリティ性能を明らかにした．提案した方式は、従来の暗号化セキュリティア方式により高いセキュリティレベルを確保できる．

研究成果の学術的意義や社会的意義
Our research reveals the possibility of securing IoT wireless communications at the physical layer and is anticipated to inspire more excellent studies in this area. The dissemination of our results to society will contribute to the proliferation of the emerging physical layer security technology.

研究成果の概要（英文）：By exploiting the inherent physical layer characteristics of wireless communication channels, we proposed several physical layer security schemes to secure the IoT wireless communications in the 5G era, including mobile ad hoc networks and millimeter-wave communication systems. We also developed theoretical frameworks to analyze the security performances of the proposed schemes. Our proposed security schemes enhance the security level achieved by the traditional cryptographic security approaches and serve as promising candidates for securing IoT wireless communications in the 5G era.

研究分野：ネットワークセキュリティー

キーワード：物理層セキュリティー

１．研究開始当初の背景

Internet of Things (IoT), as the name suggests, extends the network coverage of the Internet to smart things (e.g., sensors and actuators), giving rise to various emerging applications like smart city, smart healthcare and smart transportation. IoT has been recognized as the fundamental platform of the Society 5.0. A challenging requirement for the IoT wireless system in this society is to provide ubiquitous, high-speed and low-latency network connections to billions of devices concurrently. It is believed that the fusion of IoT and 5G will be the key enabler to meet this requirement by 1) integrating IoT D2D and cellular communications for ubiquitous wireless connectivity, and 2) shifting wireless links from the narrow microwave band (below 6GHz) to the extremely wide mmWave band (30GHz-300GHz) for significantly improved data rate and reduced latency. Therefore, we envision that 5G IoT wireless systems will consist of massive mmWave cellular and mmWave D2D (including D2D relaying) links to adapt to various scenarios with full, partial or even no cellular coverage.

However, the ubiquitous wireless connectivity brought by the fusion of IoT and 5G poses great challenges to the security of IoT systems. This is because the open wireless medium makes data easy to intercept by eavesdroppers, whereas IoT devices usually have no enough computing resources to implement complex cryptographic schemes. Thus, without a lightweight yet powerful security solution, the realization of Society 5.0 would be greatly hindered and the safety of the nation and its citizens would be significantly threatened. This motivates the introduction of the highly promising PLS technology into the IoT and 5G, as is evident from several ongoing JSPS projects]. The basic principle behind typical PLS techniques, such as artificial noise (AN) injection and cooperative jamming (CJ), is to exploit inherent channel randomness (e.g., noise, interference, fading) instead of cryptographic schemes to ensure no data is leaked to eavesdroppers To pave the way for the successful application of PLS techniques in 5G IoT wireless systems, this research aims to answer a natural and crucial question: “How can we provide PLS for 5G IoT wireless systems?”.

２．研究の目的

The goal of the research is to design effective PLS security schemes for IoT wireless communications in the 5G era, with a particular focus on millimeter-wave (mmWave) communications. In addition, the security performance analysis and optimization issues will also be addressed to reveal the optimal security configuration.

３．研究の方法

(1) PLS scheme design: We exploit classical techniques of signal processing and cooperative communications and also the intrinsic physical layer characteristics of mmWave signals to design PLS schemes for mmWave IoT communications.

(2) PLS performance analysis and optimization: We apply the tools from stochastic geometry and probability theory, especially Poisson Point Processes, to analyze the network-wide security performances. We apply convex analysis and/or optimization algorithms based on nonlinear optimization/dynamic programming to identify the optimal network security performance.

４．研究成果

(1) **We proposed a sight-based cooperative jamming (SCJ) scheme for mmWave ad hoc networks**

We consider an mmWave ad hoc network where the locations of transmission pairs, potential jammers and eavesdroppers are modeled by PPPs. By carefully exploiting the significant signal difference between NLoS and LoS mmWave links, we propose a novel Sight-based Cooperative Jamming (SCJ) scheme to improve the PLS performance of the transmission pairs. With the aim to achieve channel advantages for the legitimate receivers, in the SCJ scheme, each potential jammer that has no LoS link to its nearest receiver but may have LoS links to the eavesdroppers is selected as a jammer with a certain probability to generate artificial noise. To the best of our knowledge, this is the first work that exploits the intrinsic physical layer features of mmWave channels in the design of PLS schemes for mmWave networks. It is expected that this work will shed light on a new approach for the design of secure mmWave communication systems.

We adopt the secrecy transmission capacity (STC) [25], i.e., the average sum rate of transmissions in perfect secrecy per unit area, as the metric to investigate the PLS performance of the network under the new jamming scheme. Existing works mainly assume that jammers follow homogeneous PPPs, while the jammers in this work follow Poisson Hole Processes (PHPs) and the resultant regions where jammers reside have irregular shapes, posing a significant challenge to the interference modeling for legitimate receivers and eavesdroppers. To tackle this challenge, we apply region approximation to develop novel and efficient theoretical approaches to approximate the inhomogeneous spatial distribution of the jammers such that the challenging issue of interference distribution modeling can be tackled. With the help of the approximations, we then develop a theoretical framework based on stochastic geometry to derive the connection probability and secrecy probability of transmission pairs

(2)**We characterized the eavesdropping region of hybrid wireless communication systems.**

Hybrid communication systems, where mmWave links coexist with microwave links, have been regarded as a fundamental component in 5G systems, while, like any other wireless system, communications in these systems are vulnerable to eavesdropping attacks. In hybrid wireless systems, eavesdroppers can improve their eavesdropping effect by opportunistically selecting the

wave (i.e., mmWave or microwave) to eavesdrop on, partitioning the network into a mmWave eavesdropping region and a microwave eavesdropping region. We therefore investigate the eavesdropping region characterization problem in hybrid wireless systems from the perspective of physical layer security. We first derive the secrecy outage probabilities (SOPs) of the network when eavesdroppers choose to eavesdrop on the mmWave and microwave, respectively. Using the ratio between the SOP of mmWave links and that of microwave links as the eavesdropping wave selection criterion, we determine the mmWave and microwave eavesdropping regions. Finally, we provide extensive numerical results to illustrate the eavesdropping regions under various settings of network parameters.

(3) **We identified novel attack patterns for mmWave ad hoc networks**

MmWave communication is difficult to wiretap due to the short transmission range and highly directional transmitting antennas, meaning that wiretapping is not the best attacking strategy for eavesdroppers in mmWave networks. However, eavesdroppers can maximize their payoffs by opportunistically switching between the wiretapping attack and other attacks, leading to a more interesting and hazardous attack. We, for the first time, investigate such selective eavesdropper attacking strategies, i.e., the selection between the wiretapping attack and another representative attack (jamming), in mmWave ad hoc networks. We first propose two attacking strategies, i.e., Random Attacking (RA), where eavesdroppers independently and randomly select their attack patterns with a common probability, and Selective Attacking based on Distances (SA-D), where each eavesdropper independently conducts the selection based on its smallest distances to transmitters and receivers, respectively. Using tools from stochastic geometry, we then perform theoretical modelling on the secrecy transmission capacity (STC) of the network under both strategies. Finally, we provide extensive numerical results to illustrate the impacts of attacking parameters on the network STC performance under the proposed strategies.

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Zhang Yuanyu、Shen Yulong、Jiang Xiaohong、Kasahara Shoji	４．巻 1
２．論文標題 Secure Millimeter-Wave Ad Hoc Communications Using Physical Layer Security	５．発行年 2021年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2021.3054507	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Li Xiaochen、Zhang Yuanyu、Shen Yulong、Jiang Xiaohong	４．巻 14
２．論文標題 Secrecy transmission capacity in mobile ad hoc networks with security‐aware Aloha protocol	５．発行年 2020年
３．雑誌名 IET Communications	６．最初と最後の頁 4135～4141
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/iet-com.2020.0570	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Liao Xuening、Zhang Yuanyu、Wu Zhenqiang、Jiang Xiaohong	４．巻 98
２．論文標題 Buffer-aided relay selection for secure two-hop wireless networks with decode-and-forward relays and a diversity-combining eavesdropper	５．発行年 2020年
３．雑誌名 Ad Hoc Networks	６．最初と最後の頁 102039～102039
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.adhoc.2019.102039	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Qianyue Qu, Yuanyu Zhang, Shoji Kasahara
２．発表標題 On Eavesdropping Region Characterization in Hybrid Wireless Communications
３．学会等名 2020 International Conference on Networking and Network Applications (NaNA)（国際学会）
４．発表年 2020年

１．発表者名 Xuening Liao, Yuanyu Zhang, Bo Liu and Zhenqiang Wu
２．発表標題 Secure Communication in Two-Hop Buffer-Aided Networks with Limited Packet Lifetime
３．学会等名 2019 International Conference on Networking and Network Applications (NaNA2019)（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関