Secure User Association in Ultra Dense Heterogeneous Cellular Networks with non-Uniformly Distributed Eavesdroppers

Gongchao Su, Mingjun Dai, Xiaohui Lin, Bin Chen and Hui Wang
College of Information Engineering
Shenzhen University
Shenzhen, China
{gcsu,mjdai,xhlin,bchen,hwang}@szu.edu.cn

***Abstract*—Ultra-dense heterogeneous cellular networks (UDHCNs) offer significant gains to network throughput and constitute a vital part of next generation wireless networks. However, due to the open access mode of small cells, they are vulnerable to wiretap attacks. In this paper we study the information-theoretic secure user association in a two-tier UDHCN where a random number of eavesdroppers coexist with legitimate users and attempt to wiretap the wireless channels. In particular, these eavesdroppers are assumed to proactively seek candidate base stations to maximize information leakage. We then devise a user association scheme that maximize network secrecy throughput. Simulation results show that compared with the traditional user association scheme, our proposed method improves network secrecy performance in terms of secrecy probability and capacity.**

***Index Terms*—heterogeneous networks; user association; physical layer security; eavesdrop**

I. Introduction

Next generation wireless networks demand significantly higher system throughput, lower latency and ubiquitous connectivity for network users. For this reason, Heterogeneous Cellular Networks (HCNs) are being deployed to provide better coverage and bring users closer to radio resources, which are available through the coexistence of low power low cost small cell Base Stations (BSs) with the macro cell BSs. Increasing the densities of small cell BSs is proven to greatly enhance system capacity and user rates [1]. However, the diversity of HCNs also introduces more vulnerabilities to malicious attacks. Particularly, these small cell BSs may be operated by third parties and provide open access to users, they are vulnerable to eavesdropping, jamming, etc. Hence addressing these security concerns becomes urgent in UDHCNs.

User association mechanism, which dictates the serving base station for each HCN user, has a profound impact on network performance. A plethora of user association schemes are proposed to improve network metrics such as load balancing [2], spectral efficiency [3], energy efficiency [4], etc. These schemes are shown to outperform the traditional user association mechanism that assign each user to the base station that provides the strongest signal power. However, these works do not address security issues.

To address security concerns in wireless networks, Physical Layer Security (PLS) is considered as a promising technology that provides perfect secrecy regardless of the computational power of network devices and security protocols [5]. Recent studies on PLS in HCNs focus on metrics such as secrecy outage and capacity. In [6] secrecy outage probability is analyzed in a multi-RAT heterogeneous networks. In [7] the average secrecy rate under Rician fading channels in a two-tier HCNs is analyzed using stochastic geometry. In [8] the optimal secrecy area spectral efficiency is derived in a multi-antenna small cell networks with artificial noise. In [9] the effect of active eavesdroppers who employ jamming and eavesdropping is discussed in a single tier multi-cell network. Their results demonstrate the phenomenon that deploying more small cells improves network secrecy performance. However, these literatures employ traditional user association schemes. A recent study [10] addresses the secure user association problem in UDHCNs and assumes each BS is eavesdropped by its nearest eavesdropper.

Our work distinguishes itself from existing literatures in two folds. First, we assume randomly placed eavesdroppers are smart agents and proactively choose the base stations they eavesdrop so as to maximize their own benefits. Second, with the knowledge of eavesdropers choices, we devise a user association scheme that maximize network secrecy capacity. Our results show the combined effects on network secrecy metrics under different user association schemes and eavesdroppers behavior.

The rest of this paper is organized as follows. Section II describes the system model. Section III describes the eavesdropping model and the user association process. Section IV validate our results through extensive simulations. Section V concludes this paper.

The research was supported by research grants from Guangdong Natural Science Foundation (2017A030310462,2018A0303130131), Natural Science Foundation of China (61575126),the Key Project of Department of Education of Guangdong Province (2015KTSCX121), Natural Science Foundation of Shenzhen University (000025),Foundation of Shenzhen City (JCYJ20170818091801577).

II. System Model

We consider the downlink of a two-tier HCN in a macrocell coverage area where small cell BSs are cochannelly deployed with the macrocell and spatially distributed according to a homogeneous Poisson Point Process (HPPP) ϕ_s with a density λ_s. Similarly, users and eavesdroppers are spatially scattered according to HPPP ϕ_u, ϕ_e with densities λ_u, λ_e,respectively. The sets of BSs, users, eavesdroppers are denoted as $\mathbb{B}$, $\mathbb{U}$, $\mathbb{E}$,respectively. We assume eavesdroppers have the capability to decrypt and decode any data they intercept and they attempt to intercept the secret messages sent to legitimate users. Universal frequency reuse is assumed and all BSs share the same frequency band. We consider a flat fading channel with a path loss factor $\alpha > 2$. The received signal power for user i at distance d_{ij} from BS j is expressed as $P_{ij}h_{ij}d_{ij}^{-\alpha}$,where $h_{ij} \sim exp(1)$ denotes the random channel gain. BS $j \in \mathbb{B}$ is transmitting at its maximum power, denoted as P_j. The signal to noise plus interference ratio (SINR) for user $i \in \mathbb{U}$ associated with BS $j \in \mathbb{B}$ is given by

$$SINR_{ij} = \frac{P_j h_{ij} d_{ij}^{-\alpha}}{\sum\limits_{k \in \mathbb{B}\setminus\{j\}} P_k h_{ik} d_{ik}^{-\alpha} + \sigma^2} \tag{1}$$

where σ^2 is the thermal noise power. Note that users are subject to cross-tier interference from BSs other than their associated BSs. Similarly, when an eavesdropper $e \in \mathbb{E}$ attempts to wiretap the downlink wireless channel from BS j,the received SINR at e is given by

$$SINR_{ej} = \frac{P_j h_{ej} d_{ej}^{-\alpha}}{\sum\limits_{k \in \mathbb{B}\setminus\{j\}} P_k h_{ek} d_{ek}^{-\alpha} + \sigma^2} \tag{2}$$

The transmission rate R_{ij} for data link between user i and BS j, R_{ej} for leakage link between eavesdropper e and BS j are given by

$$R_{ij} = \log_2(1 + SINR_{ij}) \tag{3}$$

$$R_{ej} = \log_2(1 + SINR_{ej}) \tag{4}$$

To provide perfect secrecy against information leakage, PLS requires users to transmit data codewords via the data link channel while those codewords are kept confidential to eavesdroppers in the wiretap channel. Since user association is done periodically, we assume channel conditions remain constant during the association stage. Thus R_{ij} and R_{ej} are the average data link rate and leakage link rate, respectively. It is also possible there are multiple eavesdroppers wiretapping the wireless channels from the same BS. For BS j, denote the maximum leakage link rate of its eavesdroppers as $\widetilde{R_j} = \max_{e \in E} R_{ej}$. then the average secrecy rate for user i associated with BS j is given by [7]

$$R_{ij}^s = [R_{ij} - \widetilde{R_j}]^+ \tag{5}$$

where $[x]^+ = \max(x, 0)$. Note that secrecy cannot be achieved when the secrecy throughput is zero.

Under this approximation, one can evaluate the average secrecy rate for each link between users and candidate BSs. Clearly, in dense HCNs where eavesdroppers can make choices over multiple BSs to wiretap and users can be assigned to different BSs, user association should be investigated jointly with the eavesdropping behavior to get a better view of the secrecy performance.

III. Secure User Association in Dense HCNs

To achieve secure user association, we first make some assumptions on what kind of information can be retrieved prior to the user association phase. Each BS is assumed to be aware of the channel state information (CSI) of both the legitimate users and eavesdroppers. Once an eavesdropper decides to wiretap the wireless channel, we assume the wiretapping behavior can be detected by the corresponding BS, thus each BS knows exactly which eavesdroppers are eavesdropping on its users. In what follows, we first retrieve useful information from eavesdropping behavior and proceed to analyze the user association problem.

A. Eavesdropping behavior

Eavesdroppers are malicious attackers that want to intercept as much information as possible from legitimate users. We assume they are non-colluding, such that they only care about their own objectives. Thus they have their own incentives to maximize their own benefits. In dense HCNs, an eavesdropper faces the problem on which BS he eavesdrops on. Existing literature take a simplified assumption on this problem. For example, it is assumed that there is only one eavesdropper per BS [6]–[8], or each BS only care about its nearest eavesdropper [10]. These assumptions do not reflect the incentive of eavesdroppers. We can envision that eavesdroppers will choose his own best BS, not necessarily the nearest one, and it is possible that some BSs fail to attract any interested eavesdropper.

In contrast, we assume eavesdroppers are smart agents just like users and each eavesdropper make his own choice independently to maximize his own benefits. Let $y = \{y_{ej}, e \in \mathbb{E}, j \in \mathbb{B}\}$ be the binary indicator on which BS the eavesdropper chooses. To maximize information leakage, we formulate the eavesdropping association problem as

$$\begin{aligned} \max \quad & \sum_{e \in \mathbb{E}, j \in \mathbb{B}} y_{ej} R_{ej} \\ s.t. \quad & y_{ej} \in \{0, 1\} \\ & \sum_{j \in \mathbb{B}} y_{ej} = 1 \end{aligned} \tag{6}$$

which is the max sum leakage link rates. Since the rate of individual leakage link is independent from other leakage links, (6) yields a simple solution such that each eavesdropper chooses the BS with the highest SINR. In dense HCNs where macrocells coexist with small cells, this solution indicates that more eavesdroppers attempt to eavesdrop on macrocells due to their strong signal power, and some small cells are free from eavesdropping due to their weak transmission power.

B. Secure User Association

Based on the above information, we proceed to analyze the secure user association problem. When BSs detect the eavesdropping behaviors and have the knowledge on the CSIs of eavesdroppers, the secrecy rate R^s_{ij} of each individual data link can be determined. Similarly, let $x = \{x_{ij}, i \in \mathbb{U}, j \in \mathbb{B}\}$ be the binary indicator on the user association problem, we formulate the secure user association problem as

$$\begin{aligned} \max \quad & \sum_{i\in\mathbb{U}, j\in\mathbb{B}} x_{ij}R^s_{ij} \\ s.t. \quad & x_{ij} \in \{0,1\} \\ & \sum_{j\in\mathbb{B}} x_{ij} = 1 \end{aligned} \tag{7}$$

which is the max sum secrecy rates. The optimal solution to (7) requires each user be assigned to the base station with the highest secrecy rate. Note that the tradition max SINR user association method is identical to the optimal solution to $\max \sum x_{ij}R_{ij}$. Hence the difference between these two solutions are solely dependent on the difference between R^s_{ij} and R_{ij} for each individual data link. However, R^s_{ij} can be vastly different from R_{ij}. For example, if an eavesdropper is located near a particular BS, those users with a larger distance from the BS will experience secrecy outage because their channel qualities are inferior to the eavesdropper. This is particularly the case when there are eavesdroppers placed near a macrocell. In this circumstance this macrocell will be unavailable to many users for secure connections, although it does provide strong signal power and good coverage. Moreover, both the density of small cells and eavesdroppers affect the secrecy rate. Hence the tradition max-SINR user association scheme in existing literature is suboptimal for enhancing network secrecy performance when eavesdroppers proactively and dynamically wiretap the wireless channels.

We now present the secure user association algorithm as Algorithm 1.

Remark: The underlying assumption in Algorithm 1 is that eavesdroppers remain static during the user association stage. Full information on secrecy rate is collected by every BS and subsequently broadcast to users. In a dynamic scenario, whenever eavesdroppers join, leave or change their eavesdropping behavior, user association process is invoked.

IV. Numerical Results

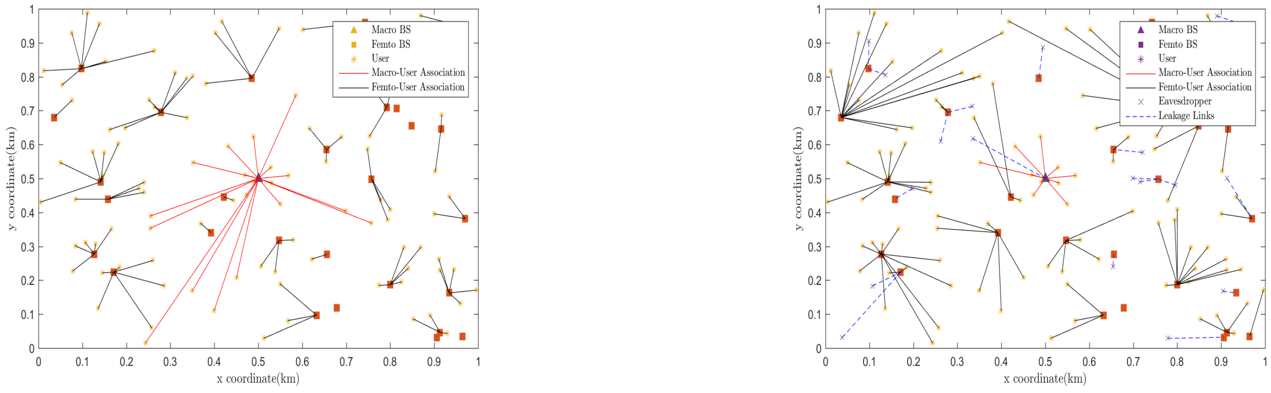
In this section numerical results on network secrecy performance are collected and validated via Monte Carlo simulation under various user association schemes. The Monte Carlo simulation is done over 200 different snapshots of spatially random network topologies. System parameters are configured as follows. The simulated HCN covers a Euclidean plane with a rectangular area of $1km^2$. The transmission power of the marocell and small cells is set to $\{46, 30\}$ dbm respectively. Downlink path loss factor is set to 4. Thermal noise is neglected since dense HCNs are typically interference-limited.

Algorithm 1 Secure User Association Algorithm.

```
Input:
    $SINR_{ij}, SINR_{ej}$;
Output:
    User association, $x_{ij}$;
Initialization:$x, y \leftarrow 0, R_{ij} \leftarrow \log_2(1 + SINR_{ij}), R_{ej} \leftarrow \log_2(1 + SINR_{ej})$;
for each $e \in \mathbb{E}$ do
    $j \leftarrow \arg\max_{j\in\mathbb{B}} R_{ej}$;
    $y_{ej} \leftarrow 1$;
end for
for each $j \in \mathbb{B}$ do
    $\widetilde{R_j} \leftarrow \max_{e\in\mathbb{E}} R_{ej}$;
end for
$R^s_{ij} \leftarrow \max(R_{ij} - \widetilde{R_j}, 0)$;
for each $i \in \mathbb{U}$ do
    $j \leftarrow \arg\max_{j\in\mathbb{B}} R^s_{ij}$;
    $x_{ij} \leftarrow 1$;
end for
return $x = \{x_{ij}\}$;
```

Fig.1 depicts a snapshot of a dense HCN with randomly located eavesdroppers under different user association schemes. In Fig.1(a), the max SINR association assigns users to the BS with the highest SINR, without knowledge of the behaviors of eavesdroppers. A large portion of users remain connected to the macrocell, due to its strong transmission power. However, it can be seen from Fig.1(b) that when eavesdroppers select their best BSs to eavesdrop, some BSs attracts multiple eavesdroppers, while other BSs are immune to eavesdropping. Particularly, the macro cell is prone to being eavesdropped, due to its strong downlink channel quality. The user association decisions, based on the collected information on eavesdropping behavior, attempt to reduce the number of users assigned to eavesdropped BSs. Users who experience inferior channel conditions to the eavesdroppers, i.e. those who are more far away from the candidate BSs than the eavesdroppers, are now assigned to other BSs. This is particularly the case for the macrocell. The existence of eavesdroppers significantly reduces the number of macrocell users.

Fig.2 depicts the secrecy probability in a dense HCN with 100 users and 20 eavesdroppers. The number of small cells varies from 5 to 50. It can be clearly seen from Fig.2 that secrecy probability remains low in max SINR association, since this user association method does not take in account the eavesdropping behavior. Moreover, when the number of small cells is much smaller than the number of users, most users remain connected to the macrocell and unfortunately the macro cell is most likely to be eavesdropped. On the other hand, in the secure user association scheme the number of users connected to the macrocell is significantly reduced, thus secrecy probability is greatly improved for less populated HCNs. As the number of small cells increase, secrecy probability increases. The rationale is that users are now more likely



(a)

(b)

Fig. 1. A snapshot of a dense HCN with one macrocell, 30 small cells ,100 users and 20 eavesdroppers. (a) HCN with the max SINR association. (b) HCN with the max sum secrecy rate association.

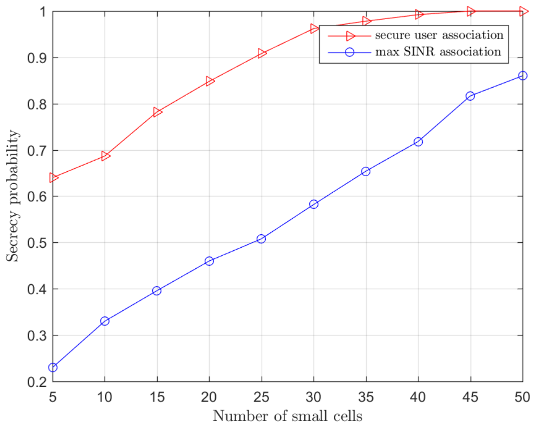


Fig. 2. Secrecy outage probability versus number of small cells.

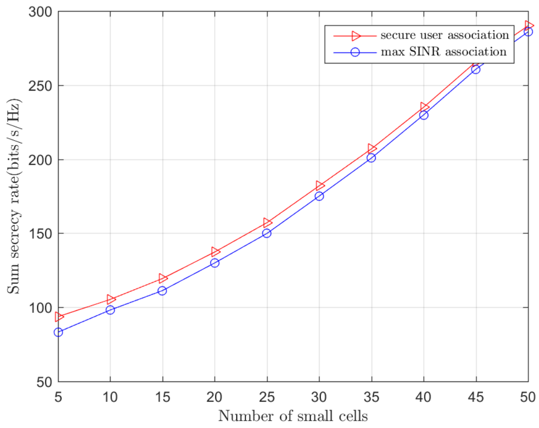


Fig. 3. Sum secrecy rate versus number of small cells.

to find nearby small cells that are free from eavesdropping attacks. Particularly, with a higher density of small cells, perfect secrecy can be achieved for secure user association. However, in max SINR association secrecy probability remains less than 1 because users are not proactively assigned to small cells free from eavesdropping.

Fig.3 shows the sum secrecy rate versus number of small cells in both user association schemes. The secure user association scheme provides a higher network secrecy throughput. However, when the number of small cells increases, the performance gap shrinks. The reason is that a higher density of small cells results in a higher secrecy probability, and even under the max SINR scheme users are more likely to find nearby BSs free from eavesdropping.

V. Conclusion

In this paper we investigate the user association problem with the intention of improve secrecy performance in dense HCNs. We assume non-uniformly distributed eavesdroppers are smart agents and actively eavesdrop on BSs to maximize their own benefits. A secure user association scheme is proposed to maximize networks secrecy throughput. Simulation results show the secrecy performance enhancement in terms of secrecy probability and secrecy throughput compared with traditional user association scheme. In the case that perfect information on eavesdroppers are not available or more complex system metrics are considered, game theory can be used to analyze the interaction between eaves, BSs and users. We leave that as our future works.

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, et al., ”What will 5G be?,” Selected Areas in Communications, IEEE Journal on, vol. 32, pp. 1065-1082, 2014.

[2] J. G. Andrews, S. Singh, Q. Y. Ye, X. Q. Lin, and H. S. Dhillon, ”An Overview of Load Balancing in Hetnets: Old Myths and Open Problems,” Ieee Wireless Communications, vol. 21, pp. 18-25, Apr 2014.

[3] S. Corroy, L. Falconetti, and R. Mathar, ”Dynamic cell association for downlink sum rate maximization in multi-cell heterogeneous networks,” in Communications (ICC), 2012 IEEE International Conference on, 2012, pp. 2457-2461.

[4] A. Mesodiakaki, F. Adelantado, L. Alonso, and C. Verikoukis, ”Energy-efficient context-aware user association for outdoor small cell heterogeneous networks,” in Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 1614-1619.

[5] Y. Liu, H. Chen, and L. Wang, ”Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges,” IEEE Communications Surveys & Tutorials, vol. 19, pp. 347-376, 2017.

[6] H. Wu, X. Tao, N. Li, and J. Xu, ”Secrecy Outage Probability in Multi-RAT Heterogeneous Networks,” IEEE Communications Letters, vol. 20, pp. 53-56, 2016.

[7] M. Kamel, W. Hamouda, and A. Youssef, ”Physical Layer Security in Ultra-Dense Networks,” IEEE Wireless Communications Letters, vol. 6, pp. 690-693, 2017.

[8] W. Wang, K. C. Teh, and K. H. Li, ”Artificial Noise Aided Physical Layer Security in Multi-Antenna Small-Cell Networks,” IEEE Transactions on Information Forensics and Security, vol. 12, pp. 1470-1482, 2017.

[9] W. Wang, K. C. Teh, K. H. Li, and S. Luo, ”On the Impact of Adaptive Eavesdroppers in Multi-Antenna Cellular Networks,” IEEE Transactions on Information Forensics and Security, vol. 13, pp. 269-279, 2018.

[10] S. Wang, Y. Gao, C. Dong, N. Sha, and G. Zang, ”Secure User Association in Two-Tier Heterogeneous Cellular Networks With In-Band Interference,” IEEE Access, vol. 6, pp. 38607-38615, 2018.