SECRECY ANALYSIS IN LARGE SCALE CELLULAR NETWORK

Neha Septa[1], Dr.Preeti Trivedi[2], Prof. Shekhar Sharma[3]
[1]ME Student, [2]Associate professor, [3]Assistant professor
Shri G. S. Inst. of Tech and science Indore, India
Email: septaneha121@gmail.com[1], preetisgsits@yahoo.co.in[2], shekhar.sgsits@gmail.com[3]

Abstract

Now a days the wide access of smart phones and other mobile devices greatest demand is connectivity with good secrecy in cellular communication. However, the small cells such as picocells and femtocells are newly introduced in Heterogeneous Network, have complicated the network topology and the interference environment, because of that we are facing new challenges in network modelling and design. Communication security has been an important issue to be addressed due to the increasing demand for transmitting private and sensitive data over wireless networks. Physical layer security, as a new way to improve wireless secrecy, is studied for cellular networks in this paper. We investigate the probabilistic characterization of the secrecy rate, and identify the performance impacts of cell association and location information exchange between Base Stations by highlighting the unique cellular features offered by the carrier-operated high-speed backhaul. These results provide necessary network design guidelines for information exchange range and selecting the appropriate cell association method.

Keywords: Stochastic geometry, Small cell network, poisson point process, secrecy.

I. INTRODUCTION

Beyond the improved coverage, as is normally attributed to HetNet, security is another major parameter that needs to be looked upon for the cellular customers. Recently, the research has been on going to provide the customers with information-theoretic security by protecting the physical layer of wireless networks[1-2]. It is markedly different from the orthodox methods of cryptography which are employed in the upper layers of the protocol stacks. Information-theoretic security makes use of the gradient between channels of legitimate users and that of eavesdroppers and for this the intended receivers must have a better channel than the eavesdropper[3].

Of late, a lot of focus has been on achieving security in large-scale networks. The communication between nodes in large-scale networks strongly depends on the location distribution and the interactions between nodes, and not like the point-to-point scenarios. With reference to information-theoretic viewpoint, studies have been carried out recently on secure communication for large scale wireless networks, with an assumption that there is a random distribution of legitimate nodes and eavesdroppers spatially. Secrecy communication graphs that describe secure connectivity over a large-scale network with eavesdroppers. With regards to the transmission capacity of secure communications shows the analysis of the throughput cost in achieving a certain level of security in an interference-limited network[5].

Mostly the research on security communications in large-scale networks are concentrated on ad hoc networks. While for cellular networks, there are a lot of particular characteristics that need to be considered. Therefore, though most of the existing work analyses large-scale networks, this chapter discusses the secrecy performance in large-scale cellular networks, instead of ad hoc networks. We have taken into consideration the unique characteristics of cellular networks that are different from ad hoc networks while doing the analysis: the carrier-operated high-speed backhaul networks connecting the core-network infrastructures and individual Base stations, which provide us potential means of Base station cooperation, such as associating mobile users to the optimal Base Station with secrecy considerations and provide better security in exchange of information[6].

For secure communication in cellular networks, the scenario which has been considered is as follows: private messages are to be sent to a mobile user. Since other mobile users should not have access to these private messages, they are treated as potential eavesdroppers. The serving Base station to make sure that the private messages are successfully delivered only to the intended user and to ensure that perfect secrecy is maintained against all the potential eavesdroppers. Since the cellular service area is divided into cells, each Base station knows the location and identity of each user and accordingly that whether the user is a potential eavesdropper or not in its own cell. The information exchange between Base stations via the backhaul networks gives the information about the identity and location details of mobile users in the other cells[7].

we employed the PPP-based stochastic geometry model for Base Station distribution, i.e., to investigate the secrecy performance in large-scale cellular networks we use modelling Base Stations to be homogeneous PPP in a plane. It needs to be mentioned that a similar work was conducted in to evaluate secrecy performance of large-scale cellular networks but its main area of focus was the scaling behaviour of the eavesdroppers density to allow full coverage over the entire network. There was not much focus on the achievable secrecy rate. Therefore, our study gives analytical results on the statistics of the secrecy rate at a typical mobile user under eavesdroppers location and different cell association models[8].

The system model and the general assumptions for achieving physical layer security in the large-scale network have been presented in this thesis. In which we obtaining simple analytical results for desired secrecy rates with different assumptions for cell association and location information exchange between Base stations. These assumptions[11] have been listed below Scenario-I: the serving Base Station fully occupy potential eavesdroppers location information; the nearest Base Station from the intended user is selected as the serving Base Station. Scenario-II: the serving Base Station fully occupy potential eavesdroppers location information; the Base Station providing best secrecy performance at the intended user is selected as the serving Base Station.

Scenario-III: the serving Base Station partially occupy potential eavesdroppers location information; the nearest Base Station from the intended user is chosen as the serving Base Station.

In section II we describe the system model and Signal Propagation Model ,then we describe the Secrecy Performance Analysis in section III. Section IV presents numerical results and shows the three different scenario based on secrecy performance analysis. section VI presents Conclusion and section VII future work, it gives the overall conclusion of the project and its scope in future. To be more specific, the probabilistic characteristics of the achievable secrecy rates and the average secrecy rates achievable are provided for these three different scenarios/assumptions. The numerical results on the achievable secrecy rate for all the three assumptions are provided respectively.

II. SYSTEM MODEL

We have considered the downlink scenario of a cellular network using an orthogonal multiple access technique and composed of a single class of Base Stations, macro Base Station for instance. The performance achieved by a typical mobile user chosen at random has been our focus. As was done earlier, our analysis will be conducted on the basis of PPP-based Base station model where we assumed that Base stations are distributed in space as two-dimensional homogeneous PP ϕ_{BS} of density λ_{BS}. Another assumption is that the independent collection of mobile users is located according to an independent homogeneous PPP ϕ_{MS} of density λ_{MS} . Lets consider a process $\phi_{MS} \cup \{0\}$, which is obtained from,when a user is added at the origin of the coordinate system. We can assume this user to be a typical user, using Slivnyaks Theorem, as to add a user is similar to conditioning on a user at that location.

A. Signal Propagation Model

The standard power loss propagation model is used with path loss exponent α > 2. Hence, the received power at the receiver from the transmitter is written as

$$P_{rx}(x_i, x_j) = P_{BS} \left\| x_i - x_j \right\|^{-\alpha} \qquad (1)$$

We assume that noise power is additive and constant with value σ^2 for all users, but no specific distribution is assumed. We have assumed in this chapter that there is no in-band interference at downlink receivers. This assumption can be realized by carefully planning the frequency reuse pattern, in which the Base Stations that are interfering to have the serving Base Station occupying some resource blocks exclusively in a relatively large region, and the interference can be incorporated in the constant noise power..

III. SECRECYPERFORMANCE ANALYSIS

Here we gives the main results on the probabilistic characteristics of the achievable secrecy rates R_S and the average secrecy rates achievable E[R] using three major scenarios, where different criteria to choose the serving Base station are used and the serving Base Station can fully or partially occupy the location information of the eavesdroppers, corresponding to the different levels of Base Station cooperation introduced. It needs to be pointed out that the Base station cooperation that has been assumed in this chapter include only the exchange of identity and location details of the mobile users and to assign the appropriate Base station to serve the intended user[11].

A. Scenario-I: Full Location Information; Nearest Base station to Serve

First, we assume that the serving Base station has full access to the information about the location of all the eavesdroppers and we use the cell association model with the constraint that only the nearest Base station serves the mobile user. While the serving Base stations cell can easily obtain the location and identity details of the mobile user, the backhaul network ensures that the information about other users supplied by other Base stations.

Theorem: Under the conditions of mobile users being served by the nearest base station and the availability of full location information for all eavesdroppers, the CCDF of the achievable secrecy rate obtained at the typical user[11] is given by

$$F_{R_S}(R_0) = \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} .2^{2R_0/\alpha}} \quad , \text{ For } R_0 \geq 0 \qquad (2)$$

Corollary: Under the conditions of mobile users being served by the near-est Base Station and the availability of full location information for all eavesdroppers, the average secrecy rate achievable at the typical user[11] is provided by

$$E[R_S] = \frac{\alpha}{2\ln 2} \ln\left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e}\right) \qquad (3)$$

B. Scenario-II: Full Location Information; Optimal base station to Serve

Going forward, we still go with the assumption that the serving Base Station has all the details about the eavesdroppers location, which can be made readily available through the information exchange between the Base Stations. But, in this case we go with the assumption that all Base Stations can serve the typical user.

From the information-theoretic standpoint, this scenario gives us the maximum achievable secrecy rate. This provides the network designer with the information about the ultimate secrecy performance that the cellular network can offer can be viewed as the optimal Base Station cooperation scheme considered in this chapter. Of course, the Base Station with the maximum secrecy rate needs to be selected to get the optimal secrecy performance. We can correlate the secrecy performance with the optimal cell association to quantify the gap between the secrecy performances provided by the optimal Base Station and the nearest Base Station[11].

Theorem: Under the conditions of mobile users being served by the optimal base station and the availability of full location information for all eavesdroppers, an upper bound for the CCDF of the achievable secrecy rate at the typical user[11] is given by

$$F_{R_S}(R_0) \le 1-\exp\left(-\frac{\lambda_{BS}}{\lambda_e 2^{(2R_0/\alpha)}}\right) \qquad (4)$$

Corollary: Under the conditions of mobile users being served by the optimal Base Station and the availability of full location information for all eavesdroppers, an upper bound of the average secrecy rate achievable at the typical user is[11] provided by

$$E[R_S] \le \frac{\alpha}{2\ln 2}[\gamma+\ln(\frac{\lambda_{BS}}{\lambda_e})+E_1(\frac{\lambda_{BS}}{\lambda_e})] \qquad (5)$$

and a lower bond is given as

$$E[R] \ge \frac{\alpha}{2\ln 2}.\ln(\frac{\lambda_{BS}+\lambda_e}{\lambda_e}) \qquad (6)$$

Where $E_1(x)=\int_x^\infty \exp(-t)\frac{1}{t}dt$ and this is exponential integral and γ is the Euler-marcheroni constant.

C. Scenario-III: Limited Location Information; Nearest Base Station to Serve

In this scenario also we make the same cell association model assumption as was carried out in Scenario-I. This means that the nearest Base Station is the one that serves the mobile users, however the serving Base Station only has limited information about the location and identity of the user. Considering the backhaul bandwidth cost in practice and the impeding core-network implementation complexity for Base Station cooperation, in this section we analyse the situation in which the details about the location and identity is only shared with the cells that are in the neighbourhood or even no sharing is allowed whatsoever[11].

Theorem 5.6. Under the conditions of mobile users being served by the nearest Base Station and only intracell eavesdroppers location information available, a lower bound for the CCDF of the achievable secrecy rate obtained at the typical user [11] is given by

$$F_{R_S}(R_0) \ge \frac{1}{1+(\frac{\lambda_e}{\lambda_{BS}}+4).2^{2R_0/\alpha}} \quad , \quad \text{for} \quad R_0 \ge 0$$

(8)

Corollary: The mobile user being served by the nearest Base Station and only intracell eavesdroppers location information available, a lower bound of the average secrecy rate achievable at the typical user[11] is provided by

$$E[R_S] \ge \frac{\alpha}{2\ln 2}\ln\left(\frac{5\lambda_{BS}+\lambda_e}{4\lambda_{BS}+\lambda_e}\right) \qquad (9)$$

IV. NUMERICAL RESULTS

Here we present the numerical result of secrecy rate of all three scenario, with different value of .The value SINR as the received SNR from serving base station at the distance r=1 and $\lambda_{BS}=1$.

A. Numerical result of Scenario-I

Here fig 1 shows the average secrecy rate at the typical user in scenario-I,for different value of path loss exponent α=2,3,4 and we can say that if the value of is increases the average secrecy rate is also increases, because the larger value of path loss exponent indicates worse signal condition both to the typical user and eavesdroppers, whereas the former effect turns out to be effective, on secrecy performance. here all these curve represent the analytical result of expression 3

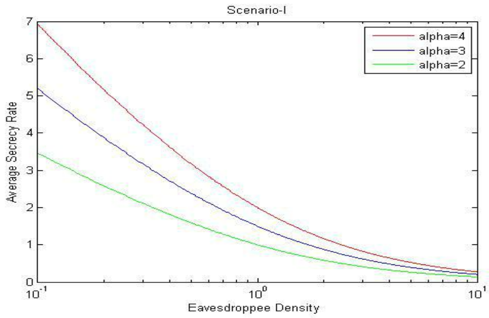

Fig. 1. The average secrecy rate versus the evaesdropper density for Scenario-I

B. Numerical result of Scenario-II

Fig 2 and Fig 3 demonstrate the result of Scenario-II, in which all the identity information and mobile user's location is known and the optimal base station is chosen to maximize the achievable secrecy rate. Here R_0=0 and R_0=5 are the threshold which show the typical user's secure link coverage probability to claim outage. From the fig 2 we can conclude that if the threshold value is less with the less value of α= 2,we get higher coverage probability of secure connection as compare to high value of threshold with the value of α= 4.Fig 3 shows the average secrecy rate versus the evaesdropper density for Scenario-II.

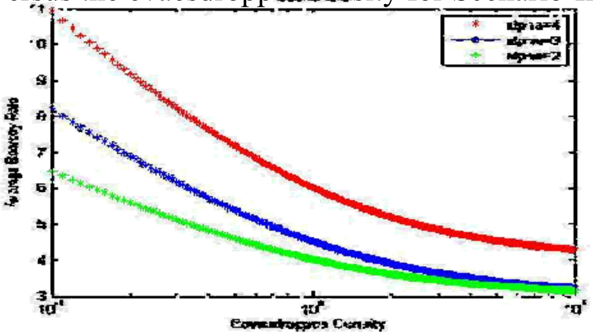

Fig. 2. The coverage probability of Secure connection versus the evaesdropper density for Scenario-I.

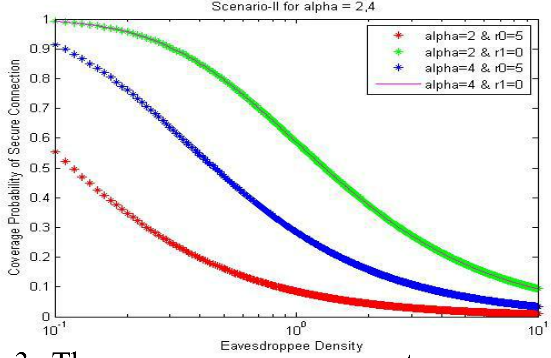

Fig. 3. The average secrecy rate versus the evaesdropper density for Scenario-II.

C. Numerical result of Scenario-III

Fig 5 demonstrate the result of Scenario-III, where no identity information and location exchange

is allowed ,here only intercell user's location is known to serving base station. Due to shrinkage of the region where the location information is available, the secrecy performance is reduce as compare to scenario-II. for example in scenario-I we get the average secrecy rate achievable is nearer to 0.3 for α= 2 and λ_e = 1,and 0.45 for = 3 and λ_e = 1 and the highest value is 0.53 for = 4 and λ_e= 1.From all these results we can conclude that the average secrecy rate is higher for α = 4 and minimum for α= 2.This is because of larger value of α= 4 indicates worse signal condition to both the typical user and the eavesdroppers, and in the lesser value of α = 2 turn out to be effective, on the secrecy performance.

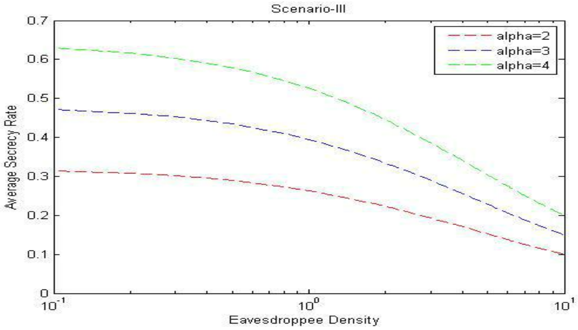

Fig. 4. The average secrecy rate versus the evaesdropper density for Scenario-III

V. CONCLUSION

Now a days, the massive usage of smartphones and other mobile devices, which require good coverage and strong security. Picocells and femto cells, these are small cells, which we can install where, their coverage region is poor.

Security for sensitive data transmissions is another important design issue with the improved cellular coverage communication. To enhance the security performance we used physical layer security in which we discussed the unique cellular features such as cell association and information exchange between Base Stations potentially provided by core-networks and the carrier-operated high-speed backhaul. We have derived the probabilistic distribution of the secrecy rate with three different assumptions on the cell association and location information exchange between Base Stations using different path loss exponent and we archive that at higher value of α= 4 we get higher secrecy rate. Using this scenario as a reference, we achieve near-optimal secrecy performance keeping the nearest Base Station for secure transmission.

VI. FUTURE WORK

There is much work yet to be done in the field of large scale cellular network but many aspects of the stochastic-geometry-based model could be further optimized to match a real word heterogeneous network by investigating practical heterogeneous network deployment data.

REFERENCES

[1] Secrecy transmission capacity of decentralized wireless networks, in Proc. 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton11), Monticello, USA, Sep. 2011, pp. 17261732. [160] A. Sarkar and M. Haenggi, Secrecy coverage, Internet Math-ematics, vol. 9, no. 2-3, pp. 199216, 2013.

[2] M. Haenggi, The secrecy graph and some of its prop-erties, in Proc. IEEE Intl Symp. on Information Theory (ISIT08), Toronto, Canada, Jul. 2008, pp. 539543.

[3] A. D. Wyner, The wire-tap channel, Bell System Tech-nical Journal, vol. 54, no. 8, pp. 13551387, Oct. 1975.

[4] I. Csiszar and J. Korner, Broadcast channels with confi-dential messages, IEEE Trans. Inform. Theory, vol. 24, no. 3, pp. 339348, May 1978.

[5] X. Zhou, R. K. Ganti, and J. G. Andrews, Secure wireless network connec- tivity with multi-antenna transmission, IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 425430, Feb. 2011.

[6] A. Okabe, B. Boots, and K. Sugihara, Spatial Tessella-tions: Concepts and Applications of Voronoi Diagrams. New York, NY: John Wiley Sons Ltd., 1992.

[7] A. L. Hinde and R. E. Miles, Monte Carlo estimates of the distributions of the random polygons of the Voronoi tessellation with respect to a Poisson process, Journal of Statistical Computation and Simulation, vol. 10, no. 3-4, pp. 205223, 1980.

[8] D. Weaire, J. P. Kermode, and J. Wejchert, On the distri-bution of cell areas in a Voronoi network, Philosophical Magazine Part B, vol. 53, no. 5, pp. L101L105, 1986

[9] X. Zhou, R. K. Ganti, and J. G. Andrews, Secure wireless network connec- tivity with multi-antenna transmission, IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 425430, Feb. 2011.

[10] C. Capar, D. Goeckel, B. Liu, and D. Towsley, Se-cret communication in large wireless networks without eavesdropper location information, in Proc. 31st Annual IEEE Intl Conf. on Computer Commun. (IEEE INFO-COM12), Orlando, USA, Mar. 2012, pp. 11521160.

[11] H. Wang, X. Zhou, and M. C. Reed, Physical layer security in cellular networks: A stochastic geometry approach, IEEE Trans. Wireless Commun., submitted for publication.