Secure Communication in Shotgun Cellular Systems

Asma Bagheri, Ghosheh Abed Hodtani
Ferdowsi University of Mashhad, Mashhad, Iran
bagheri.asma84@yahoo.com, ghodtani@gmail.com
Corresponding author: bagheri.asma84@yahoo.com

***Abstract*— In this paper, we analyze the secure connectivity in Shotgun cellular systems (SCS: Wireless communication systems with randomly placed base stations) by Poisson intrinsically secure communication graph (IS-graph), i.e., a random graph which describes the connections that are secure over a network. For a base-station in SCS, a degree of secure connections is determined over two channel models: only path loss model and fading channels.**

***Index Terms*—** Local connectivity, Shotgun cellular systems, in-degree, out-degree.

I. INTRODUCTION

Cellular communication consists of a set of radio base-stations (BSs) distributed over a region that communicate with mobile-stations (MSs). In contrast to hexagonal cellular systems (ideal systems) with regular BS placement, in many wireless systems such as LANs and femtocells [1], due to site acquisition difficulties, BSs are placed randomly over the deployment region. These systems called shotgun cellular systems (SCSs), are described by BS density function.

Rapid deployment over a region is an important need of wireless communication systems. Some applications such as emergency or rescue operations, disaster relief efforts, and military networks, need efficient and secure communications. Recently, there has been considerable interest in the important field ofthe secure connectivity of wireless systems.[2-7]

In a wireless network, the signal propagates over channel and it can be received by legitimate or malicious stations. So, with extended use of these networks, security and privacy communication takes on an important role in wireless networks. Previously, encryption protocols were designed. But for security in networks such as ad hoc network, these protocols got so difficult to implement. Therefore, ability of physical layers in security was investigated.

Physical layer security is a field of research which studies the probability of achieving to secure information communication between the nodes of a network, while the probability of received information for eavesdroppers is zero.[6] Information theoretic security is basedon physical layer

Manuscript Received 27-March-2013 and revised 5-June-2013 *ISSN: 2322-3936*
Accepted on 28- June-2013

security. Basically, the characteristics of wireless channel are troublous to communicate with achieving maximum signal to noise ratio, but indeed these characteristics can provide security and reliability of wireless systems and networks.

The SCS and its performance metrics have been studied under different channel models [1,8-17]. In these papers, the performance of system was defined as carrier to interference plus noise ratio, and under different scenarios, such as non homogenous distribution of BSs [1], lognormal shadowing channels [9],[10], dynamic channel assignment [11], two dimensional systems [12],[13], one, two and three dimensional systems [14], multi-tier network composed of M tiers of homogenous N-dimensional systems [15], the performance at MS was analyzed. Also, a simple analytical tool based on stochastic ordering was developed to compare the distributions of carrier-to-interference ratio (CIR), at the mobile station of two SCS [16],[17]. In these papers, SCS performance was compared with ideal hexagonal systems, and was shown that SCS is a good choice to study for using in the cases that there is not sufficient time for designing location of BSs, such as military or rescue operations.

To the best of our knowledge, in a SCS secure communication has not been analyzed. In wireless networks secure connectivity is an essential issue, particular in military applications, in order to have a secure and successful communication.

Historically, information theoretic security was built on Shannon's notion of perfect secrecy [18]. Then it was introduced in the 1970s by Wyner. In [19], a model for wiretap channels was introduced and it was shown that with transmitting at rate lower than rate of main link, in discrete memory-less channel, the information of eavesdropper from message is equal to zero. Later, in 1977, it was shown that it is possible transmitting with a rate equal to rate of main link, and still information of eavesdropper from message, on many large portions of message could be equal to zero [20].

In [21], a general model for wiretap channels was described, i.e., a model composed of a transmitter and two receivers, in which the transmitter wants to send a common message to both receivers, and a confidential message to one of the receivers (Broadcast Channel with Confidential message: BCC channel), and for this channel, the secrecy capacity region was introduced.

In [22], Wyner results were extended to Gaussian channels, and secrecy capacity region for Gaussian eavesdropper channel was introduced. In [2], information theoretic security over quasi-static fading channels was studied, and it was shown that random fading coefficient can help to secure communication with non zero rates. In [3], the BCC channel affected by fading and AWGN was analyzed, and secrecy capacity region was determined for Gaussian and fading parallel BCC channel. In [4], secrecy capacity region for a transmitter and multi receivers in presence of an eavesdropper was determined.

In [5], the characteristic of randomness of distances between nodes was used for secure transmitting in wireless networks. In [6],[7], the physical layer security was analyzed, and a random wireless channel with a number of legitimates and eavesdroppers with random spatial distributions,

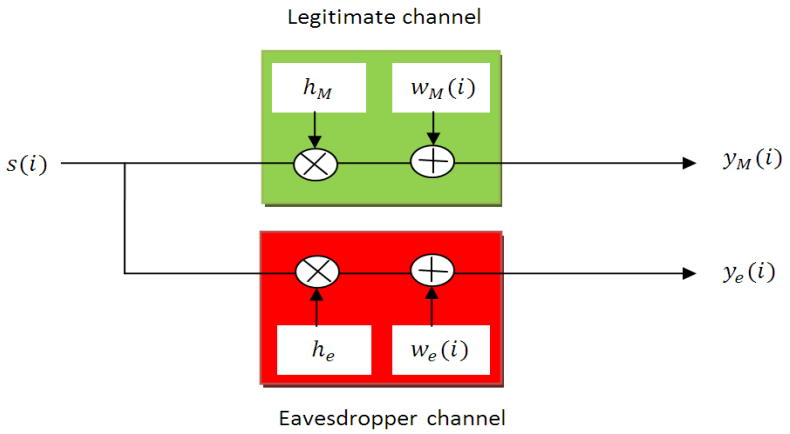

Fig. 1. The legitimate and eavesdropper channels

was assumed and degrees for secure communication of a node with each of its neighbor nodes was analyzed, and secrecy capacity of this communication was introduced by using IS-graph for describing connectivity of nodes. In [23], maximum secure achievable rate for communication between a node and its neighbor nodes, in a random wireless channel with a number of legitimates and eavesdroppers with random spatial distributions, was determined.

Our work-In this paper, we analyze the general definition of secure connectivity for a SCS, from a physical layer perspective and the random location of MSs and BSs, over wireless channel models. Here, we generally analyze the security of a homogenous Shotgun system where the number of BSs and both legitimate and eavesdroppers are Poisson random variables.The degree of security in two scenarios is studied. In the first scenario, we model the channel with only path loss and, in-degree and out-degree for a BS are calculated. In the second scenario, we assume shadowing and fading in additionto path loss, and calculate the secure degrees of a BS.

Paper organization-In Section II, we describe system model used for a SCS, to study its connections. In section III, we explain main results. First, we will calculate the statistic characteristics of out-degree for a BS over path loss channel model. Second,we will calculate the statistic characteristics of in-degree for a BS over assumed model. Third, we will determine out-degree for a BS over shadowing fading channel model. In the fourth part, we will calculate the statistic characteristic of in-degree for a BS over assumed model. In section IV numerical results are presented. In section V, we conclude the paper.

II. SYSTEM MODEL AND DEFINITIONS

This section describes the model of Shotgun cellular system and the parameters which introduce secure connectivity. Here the model of the cellular system used for analyzing the SCS, composed of base stations that are placed randomly over the region and some legitimate and malicious users which are located randomly, too. The BSs are placed due to uniform Poisson distribution with BS density

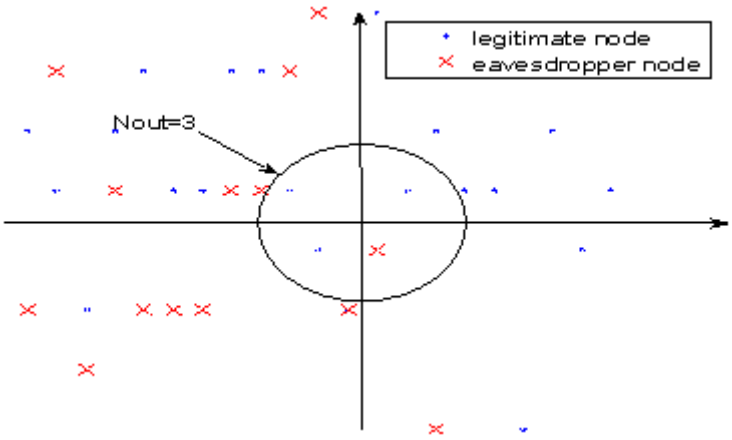

Fig. 2. Example of a Poisson IS-graph for a SCS

function λ_B. Poisson process causes maximum entropy[24],[25] and is a good model for describing the number of random variables. We model the number of legitimate MSs and eavesdropper MSs by Poisson process with density functions $\lambda_M$and λ_e, respectively.In this paper, the focus is on downlink, BS-to-MS.

The received power at the MS in location x_j, from a BS in location x_i, with assumption of equal transmitter power for all BSs, is given by $P_r(x_i, x_j) = P_T . R_{ij}{}^{-\varepsilon} . \prod_{k=1}^{K} z_{ij,k}$, where P_T is transmitter power. The path-loss is a function of the BS to MS separation, i.e., R_{ij}, and it follows an inverse power law with ε, as the path-loss exponent. The fading factors of wireless channel between transmitter (BS) and receiver (MS) are introduced with $z_{ji,k}$s, when K is the number of fading factors.

Now we define secure communication precisely from Information Theory perspective. Assume a BS, a legitimate MS (we say it MS in sequel) and an eavesdropper MS (we say it eavesdropper only), as Fig.1. When the BS wants to send a message to MS, codes the random message *S* with a complex random sequence $S^{\ell} = (s(1), \dots, s(\ell)) \in \mathbb{C}^{\ell}$ with length ℓ, and sends the coded message over the channel. Since the channel is wireless, MS and eavesdropper both can receive the coded message. What MS receives in output of the discrete-time channel at time i would be:

$$y_M(i) = h_M . s(i) + w_M(i) \quad (1)$$

where$h_M$and $w_M(i)$are respectively the gain amplitude of legitimate channel and AWGN with power σ_M^2per sample, and denotes with$w_M(i) \sim N(0, \frac{\sigma_M^2}{2})$.Also eavesdropper observes in output of the discrete-time channel at time i:

$$y_e(i) = h_e . s(i) + w_e(i), \quad (2)$$

where$h_e$and $w_e(i)$are respectively the gain amplitude of eavesdropper channel and AWGN with power σ_e^2per sample, and denotes with $w_e(i) \sim N(0, \frac{\sigma_e^2}{2})$. We assume the message random variable, i.e.,

sandh$_M$, h$_e$, w$_M$ and w$_e$ are mutually independent and transmitted code words have limited transmitter power, i.e., $P_M \geq \frac{1}{\ell}\sum_{i=1}^{\ell} E\{|s(i)|^2\}$.

We analyze here the strong secrecy of a SCS, and define it as[7]:

Definition .1 (Strong Secrecy): The rate$\mathcal{R}^*$ is said to beachievable with strong secrecy if $\forall\epsilon > 0$, for sufficiently largecodeword lengthℓ, there exists an encoder–decoder pair with rate $\mathcal{R}$ satisfying the following conditions:

$$\mathcal{R} \geq \mathcal{R}^* - \epsilon$$
$$H(S|y_e^{\ell}) \geq H(S) - \epsilon$$
$$p\{\hat{S} \neq S\} \leq \epsilon.$$

where H(.) denotes the entropy function. We definethe maximum secrecy rate (MSR) of the legitimatechannel to be the maximum rate that is achievable with strong secrecy[22],[23]. If the legitimate link operates at a rate belowthe MSR, there exists an encoder–decoder pair such that theeavesdropper is unable to obtain additional information about$S$, fromobservationy_e^{ℓ}, in the sense that $H(S|y_e^{\ell})$approaches$H(S)$as the codeword length grows. It was shown in [22],[23] that for a given realization of the channel gains, theMSR of the Gaussian wiretap channel is:

$$\mathcal{R}_s = \left[\log_2(1 + \frac{P_T.|h_M|^2}{\sigma_M^2}) - \log_2(1 + \frac{P_T.|h_e|^2}{\sigma_e^2})\right]^+ \quad (3)$$

where $[x]^+ = \max\{x, 0\}$.

Now, we introduce the Poisson IS-graph which is based on strong secrecy. As depicted in Fig.2, we assume some legitimate and malicious MSs overa SCS. $\Pi_M = \{x_j\}_{j=1}^{\infty} \in \mathbb{R}^2$denotes location of the set of MSs over $\mathbb{R}^2$with density λ_M, and $\Pi_e = \{e_k\}_{k=1}^{\infty} \in \mathbb{R}^2$ denotes location of the set of eavesdroppers over $\mathbb{R}^2$ with density λ_e, and $\Pi_B = \{x_i\}_{i=0}^{\infty} \in \mathbb{R}^2$ denotes location of the set of BSs over $\mathbb{R}^2$with density λ_B, where x_j, e_k, and x_i denote the location of one MS, one eavesdropper, and one BS, respectively, and these are mutually independent, too. Poisson IS-graph for a SCS is defined a directed graph G, as $G = \{\Pi_M, \Pi_B, \mathfrak{D}\}$, where $\mathfrak{D}$ is an edge set:

$$\mathfrak{D} = \{\overline{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho\} \quad (4)$$

Where ϱ is a threshold level for MSR per link, and $\mathcal{R}_s(x_i, x_j)$ is MSR for link $\overline{x_i x_j}$. In [7], for a given realization of the channel gains, MSR of a link was introduced:

$$\mathcal{R}_s(x_i, x_j) = \left[\log_2(1 + \frac{P_r(x_i,x_j)}{\sigma_M^2}) - \log_2(1 + \frac{P_r(x_i,e^*)}{\sigma_e^2})\right]^+ \quad (5)$$

with $e^* = \arg\max_{e_k \in \Pi_e} P_r(x_i, e_k)$, which e^* is the location of an eavesdropper that its received power from i-th BS is stronger than any other eavesdropper. Also here we assumed that eavesdroppers are not able to change or combine information, so they only affect the MSR between any pair ofBS and MS.

In an IS-graph in-degree and out-degree of legitimate users describe the number of users that can communicate safely, and are denoted with $N_{in}$and N_{out}, respectively. We can describe secure connectivity of a BS with in and out degree of legitimate MSs for this BS. These degrees are random variables and we determine their statistical properties in sequel.

Definition .2 (out-degree of legitimate MSs): The number N_{out}, out-degree of legitimate MSs for BS_0, is the number of MSs which their received power of BS_0 is more than received power of every eavesdropper from BS_0.

Definition .3 (in-degree of legitimate MSs): The number N_{in}, in-degree of legitimate MSs for BS_0, is the number of MSs which their received power of BS_0 is more than received power of every eavesdropper from BS_0, and also their received power of BS_0 is more than their received power of every other BS.

We analyze secure communication in a SCS over two types of channel models:

a) we assume just path loss and do not analyze shadowing and fading effects on both legitimate and eavesdropper channels, i.e., $Z_{x_i,x_j} = 1, Z_{x_i,e_k} = 1$.

b) we assume shadowing and fading in addition to path loss and, model the composite fading channel with Z_{x_i,x_j} for legitimate channels and Z_{x_i,e_k} for eavesdropper channels. Here Z_{x_i,x_j} or Z_{x_i,e_k},i.e., the random variables of channel model, are product of two random variables for modeling shadowing and multi path fading, which are denoted by φ_{x_i,x_j} and $\alpha^2_{x_i,x_j}$, for legitimate channels, and φ_{x_i,e_k} and $\alpha^2_{x_i,e_k}$ for eavesdropper channels, respectively. Usually these random phenomena are modeled by statistical distributions. Therefore we model shadowing factor, i.e., $\varphi_{.,.}$, as a zero mean lognormal random variable with variance σ_φ. Also multi-path fading factor, $\alpha^2_{.,.}$, is modeled as a Nakagami-m random variable. It means: $\varphi_{.,.} \sim logN(0, \sigma_\varphi)$ and $\alpha^2_{.,.} \sim gamma\left(m, \frac{1}{m}\right)$With distributions:

$$f(\varphi) = \frac{1}{\varphi\sqrt{2\pi}\sigma_\varphi} \exp\left(-\frac{1}{2}\left(\frac{\ln\varphi}{\sigma_\varphi}\right)^2\right) \quad (6)$$

$$f_\alpha(\alpha) = \frac{2}{\Gamma(m)}\left(\frac{m}{\rho}\right)^m \alpha^{2m-1} \exp\left(\frac{-m}{\rho}\alpha^2\right) \quad (7)$$

Here we also assume the case that noise power of all channels are equal ($\sigma^2_M = \sigma^2_e = \sigma^2$), and the threshold of MSR is zero, ($\varrho = 0$).

III. MAIN RESULTS AND DISCUSSIONS

We analyze the secure connectivity for a BS over a SCS as probability that the BS can securely send a message to legitimateMSs. , i.e.,:

$$\mathrm{P\{secure\ connectivity\ of\ system\}} = \sum_{b=1}^{\infty} \mathrm{P\{secure\ connectivity\ of\ all\ BSs|number\ of\ BSs} = b\} \,.\, \mathrm{P\{number\ of\ BSs} = b\} \quad (8)$$

and when the random variable of number of BSs is denoted by B, and for a constant b we can write:

$$\mathrm{P\{secure\ connectivity\ of\ all\ BSs|B} = b\} = (\mathrm{P\{secure\ connectivity\ of\ a\ BS|B} = b\})^{b} \quad (9)$$

and it is concluded from the fact that connectivity of all BSs are independent.

On the other hand, we can define a degree of security for describing secure connections of a SCS. We define the degree as probability that all BSs can securely connect to at least n MSs:

$$\mathrm{P\{degree\ of\ security} = n\} = \mathrm{P\{all\ BSs\ can\ securely\ connect\ to\ at\ least\ n\ MSs\}} \quad (10)$$

and from (8), (9), we can analyze the secure connectivity for a BS.

$$\mathrm{P\{degree\ of\ security} = n\} = \sum_{b=1}^{\infty} (\mathrm{P\{\ degree\ of\ security\ of\ a\ BS} = n\ |B = b\})^{b} . \mathrm{P\{number\ of\ BSs} = b\} \quad (11)$$

For analyzing security of a BS, without loss of generality, we assume the BS at origin, with location x_0, and denote it with BS_0. Now parameters of Poisson IS-graph are determined. We can describe secure connectivity of a BS with in and out degree of legitimate MSs for this BS. In a cellular system in-degree is important, so here we can say:

$$\mathrm{P\{secure\ connectivity\ of\ a\ BS|B} = b\} \propto \mathrm{P\{N_{in}} = n\}$$

In and out degrees are random variables and we determine their statistical properties in sequel.

From Definition.2 and Definition.3 it can be concluded that for all cases $N_{out} \geq N_{in}$. In this section, at first, we analyze the secure connectivity for a BS with assuming $\varrho = 0$ and only path loss, and in sequel, generalizethe results to other scenario.

a) Out-degree analysis in the first scenario($Z_{x_i,x_j}, Z_{x_i,e_k} = 1$)

In this section we calculate the probability and mean of out-degree for the first scenario, and then the probability of a BS that can safely communicate with no legitimate MS is concluded. In Shotgun cellular system for a BS in the origin, at this scenario, we can write the edge set as:

$$\mathfrak{D} = \{\overline{x_0 x_j} : \mathcal{R}_s(x_0, x_j) > 0\} \quad (12)$$

after some algebra we calculate it as:

$$\mathfrak{D} = \{\overline{x_0 x_j} : |x_0 - x_j| < |x_0 - e^*|\} \quad (13)$$

where $e^* = \arg\min_{e_k \in \Pi_e} |x_0 - e_k|$, so N_{out} is the number of MSs that their distances from $BS_0$is less than any eavesdropper on system.

We can model the N_{out} random variable with Binomial distribution, i.e., $N_{out} \sim B(n, p)$, where p is the probability of MS being legitimate for a user, and q is the probability of being eavesdropper, so we can write: [27]

$$P\{N_{out} = n\} = p^n . q \tag{14}$$

When $p = \frac{\lambda_M}{\lambda_M + \lambda_e}$and $q = \frac{\lambda_e}{\lambda_M + \lambda_e}$. Therefore the probability of $N_{out} = n$ is equal to existing n legitimate MS around the BS_0, and (n+1)-th user near to $BS_0$is eavesdropper. So we can write (14) as:

$$P_{N_{out}}(n) = (\frac{\lambda_M}{\lambda_M + \lambda_e})^n . \frac{\lambda_e}{\lambda_M + \lambda_e}. \tag{15}$$

Formean of N_{out}, in a Shotgun system we calculate:

$$E\{N_{out}\} = \frac{p}{q} = \frac{\lambda_M}{\lambda_e} \quad \text{for } p > q \tag{16}$$

The N_{out} random variable, can also be modeled by random walks to catch first loss. For secure communication analysis in a SCS we need to have the probability of a BS can safely communicate with no legitimate MS. We define it as isolation probability of a BS, and calculate it as:

$$P_{out-iso} = P_{N_{out}}(n = 0) = \frac{\lambda_e}{\lambda_M + \lambda_e} \tag{17}$$

b) In-degree analysis in the first scenario($Z_{x_i,x_j}, Z_{x_i,e_k} = 1$)

In this section we calculate the probability of in-degree for the first scenario, and then the probability that a BS can safely communicate with no legitimate MS from an in-degree perspective is concluded. By using Definition 3 and (3) and some algebra, for j-th MS to be one of N_{in} MSs, we have:

$$\{\overline{x_0 x_j} : |x_0 - x_j| < |x_0 - e^*|\} \tag{18}$$

where $e^* = \arg\min_{e_k \in \Pi_e} |x_0 - e_k|$, so it means that N_{in} is the number of MSs that their distances from $BS_0$is less than any eavesdropper on system. And also must:

$$P_r(x_0, x_j) > P_r(x_i, x_j), \ for\ i \neq 0 \tag{19}$$

andwe define this case when $BS_0$is server of j-th MS, and for the first scenario, it means that:

$$|x_0 - x_j| < |x_i - x_j|, \text{ for } i \neq 0 \tag{20}$$

so it is equal that the distance of j-th MS from BS_0 is less than its distances from other BSs on system.

So the probability of $N_{in} = n$ can be written as:

$$P\{N_{in} = n\} = P\{N_{out} = n\} . P\{BS_0 \text{ is server of these n MSs}\}. \tag{21}$$

Because of independency of MSs :

$$P\{BS_0 \text{ is server of these n MSs}\} = (P\{BS_0 \text{ is server of one MS}\})^n \tag{22}$$

and from (20):

$$P\{BS_0 \text{ is server of } j-\text{th MS}\} = P(R_{0j} < R^*) \quad (23)$$

when $R^* = \arg\min_{x_i \in \Pi_B} |x_i - x_j|$ for $i \neq 0$, and from [1], for distribution of distance of a MS from server BS, i.e., BS_0, we have:

$$f_{R_{0j}}(r) = \lambda_B . e^{-\lambda_B . r} \quad (24)$$

therefore,we can conclude:

$$P(R_{0j} < R^*) = 1 - e^{-\lambda_B . R^*} \quad (25)$$

and from expression (25) it is calculated:

$$P\{N_{in} = n\} = \left(\frac{\lambda_M}{\lambda_M + \lambda_e}\right)^n . \frac{\lambda_e}{\lambda_M + \lambda_e} . (1 - e^{-\lambda_B . R^*})^n \quad (26)$$

From this expression it is concluded that the probability of $N_{in} = n$ is less than probability of $N_{out} = n$.

By using expression (26), the probability that a BS can securely send information to no legitimate MS, on a SCS would be:

$$P_{in-iso} = P_{N_{in}}(n = 0) = \frac{\lambda_e}{\lambda_M + \lambda_e} \quad (27)$$

Comparing this expression with (17), it is concluded that in-isolation probability and out-isolation probability are equal over path loss channel models.

c) Effect of shadowing-fading channel model on out-degree security

In previous sections, we study only path loss effect on security of Shotgun systems. In reality wireless channels are affected by some random phenomena such as shadowing and multi path fading. So in this section we study these random effects on secure connectivity of a SCS.

In this scenario, for edge set of IS-graph by using (4) and (5), and some algebra, we have:

$$\mathfrak{D} = \{\overline{x_0 x_j} : P_r(x_0, x_j) > P_r(x_0, e^*)\}, \quad (28)$$

Now, if define $P_r(x_0, e^*) = \max_{e_k \in \Pi_e} P_r(x_0, e_k) \triangleq P_e^*$, for probability of out-degree we can calculate:

$$P\{N_{out} = n\} = p_z^n . q_z \quad (29)$$

where p_z is probability of being legitimate MS for a user that has edge set limitation. So the probability that a MS, (we denote j-th MS), to be one of out-degree users, can be calculated as:

$$p_z = P\{j-\text{th MS is one of } N_{out} \text{MSs}\} = \frac{\lambda_M}{\lambda_M+\lambda_e}.P(P_r(x_0,x_j) > P_e^*)$$

$$= \frac{\lambda_M}{\lambda_M+\lambda_e}.E_{Z_{x_0,x_j}}\{P(R_{0j} < (\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon})\} = \frac{\lambda_M}{\lambda_M+\lambda_e}(1-E_{Z_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon}}\}) \quad (30)$$

when the latest equation is concluded from (24), and E(.) denotes the expectation by respect to random variable of channel model.

Here Z_{x_0,x_j} ,i.e., the random variable of channel model, is product of two random variables for modeling shadowing and multi path fading, which are denoted by φ_{x_0,x_j} and $\alpha^2_{x_0,x_j}$, respectively, and their distributions were introduced by (6) and (7), it means $Z_{.,.} = \varphi_{.,.}.\alpha^2_{.,.}$.
So the probability of out-degree would be:

$$P\{N_{out}=n\} = P_{N_{out}}(n) = \left\{\frac{\lambda_M}{\lambda_M+\lambda_e}(1-E_{\varphi_{x_0,x_j},\alpha^2_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon}}\})\right\}^n$$
$$.\frac{\lambda_e}{\lambda_M+\lambda_e}.E_{\varphi_{x_0,x_j},\alpha^2_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon}}\} \quad (31)$$

Therefore, the probability that a BS can securely send information to no legitimate MS, on a SCS with shadowing-fading channels, would be:

$$P_{out-iso} = P_{N_{out}}(0) = \frac{\lambda_e}{\lambda_M+\lambda_e}.E_{\varphi_{x_0,x_j},\alpha^2_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon}}\} \quad (32)$$

d) Effect of shadowing- fading channel model on in-degree security

In this section we study the shadowing and multi path fading effects on secure connectivity of a SCS.

In this scenario, using Definition.3, probability of in-degree of Poisson IS-graph, the same as (17), can be written as:

$$P_{N_{in}}(n) = P_{N_{out}}(n).P\{BS_0 \text{ is server of these n MSs}\} \quad (33)$$

by this difference that the probability of $BS_0$to be server for a MS, does not depend only on distance, and here for every BS ($\forall i \neq 0$):

$$P\{BS_0 \text{ is server of } j-\text{th MS}\} = P(P_r(x_0,x_j) > P_r(x_i,x_j)\}) \quad (34)$$

And now if define $P^* \triangleq \max_{x_i \in \Pi_B} P_r(x_i, x_j)$, and with some algebra and using (24) and (31), for probability of in-degree we can calculate:

$$P_{N_{in}}(n) = P_{N_{out}}(n).\left\{1 - E_{\varphi_{x_0,x_j},\alpha^2_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P^*})^{1/\varepsilon}}\}\right\}^n \quad (35)$$

So the in-isolation probability, i.e., the probability that a server BS can securely send information to no legitimate MS, on a SCS with shadowing-fading channels, would be:

$$P_{in-iso} = P_{N_{in}}(0) = \frac{\lambda_e}{\lambda_M+\lambda_e} E_{\varphi_{x_0,x_j},\alpha^2_{x_0,x_j}}\{e^{-\lambda_B.(\frac{P_T Z_{x_0,x_j}}{P_e^*})^{1/\varepsilon}}\} \quad (36)$$

Comparing this expression with (32), it is concluded that in-isolation probability and out-isolation probability are equal over this shadowing-fading channel model, too.

IV. NUMERICAL RESULTS

In this section, the details of simulation are presented. We simulate a SCS with $\lambda_M = 20$, $\lambda_e = 5$ and $\lambda_B = 3$ and also suppose this system as a dense system with $\varepsilon = 4$ and m=4.

Also we assume threshold levels as: $R^* = 1$ and $\frac{P_T}{P_e{}^*} = \frac{P_T}{P^*} = 2$. For the case that fading and shadowing are assumed, we use Mont-Carlo method for calculating the mean.

In Fig.3, the probabilities of in-degree and out-degree securitiesfor a BS in a Shotgun cellular system over only path-loss channel model were depicted. From this figure it is concluded that the probability of $N_{in} = n$, is less than probability of $N_{out} = n$. Also, these probabilities have exponential function characteristics that when n increases the probabilities decrease. It is because of emerging n in the exponent of equations (15) and (26).

In Fig.4, the probabilities of in-degree and out-degree securities for a BS in a Shotgun cellular system assuming shadowing-fading channel model were shown.Also, from this figure it is concluded that the probability of $N_{in} = n$, is less than probability of $N_{out} = n$. But in this case, the difference between the probabilities of in-degree and out-degree securities decreases. Also, these probabilities have exponential function characteristics that when n increases the probabilities decrease. It is because of emerging n in the exponent of equations (31) and (35).

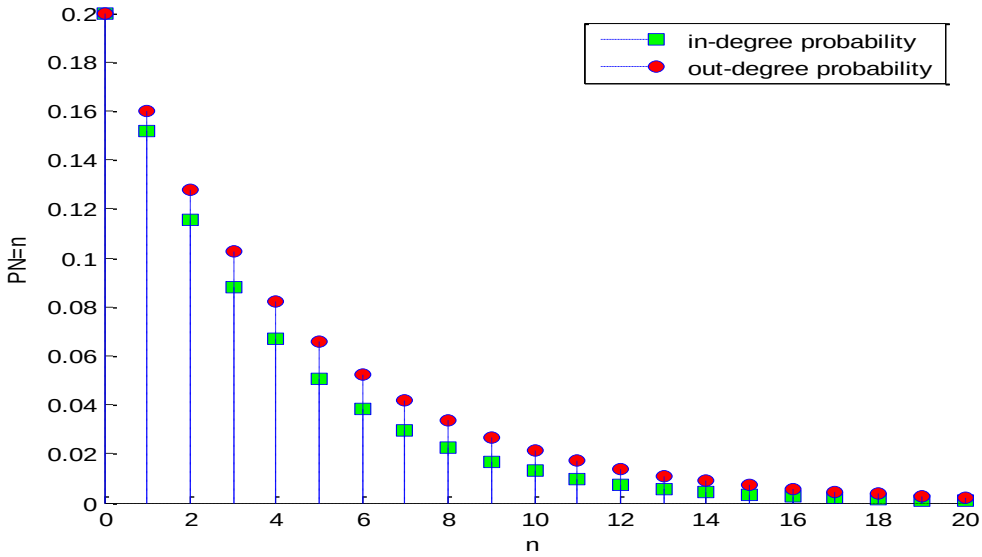

Figure.3: The probabilities of in-degree and out-degree security for a BS in a Shotgun cellular system over only path-loss channel model.

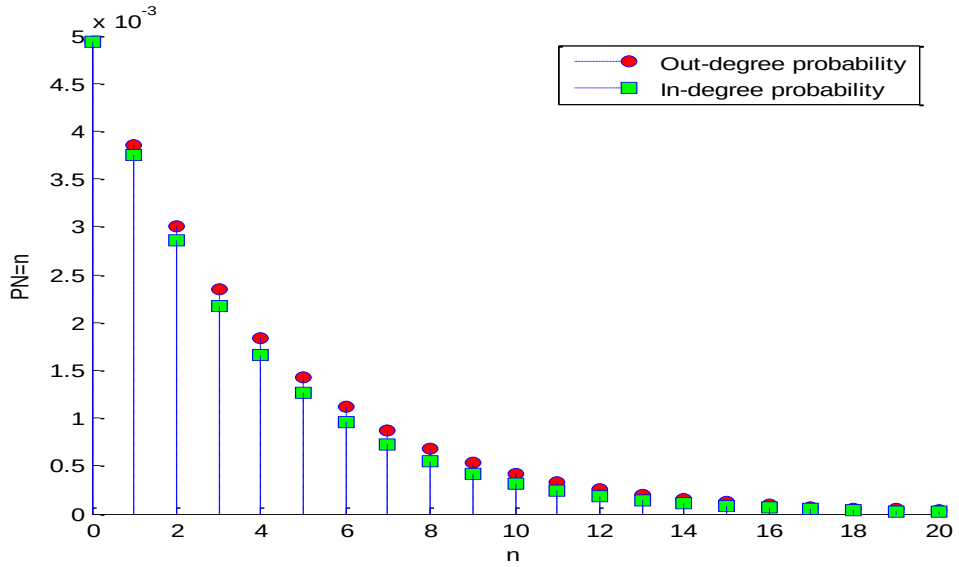

Figure.4: The probabilities of in-degree and out-degree security for a BS in a Shotgun cellular system over shadowing-fading channel model.

V. CONCLUSION

In this paper, the secure connectivity in Shotgun cellular systems by Poisson intrinsically secure communication graph (IS-graph) was analyzed. We used the random IS-graph to describe the connections being secure over a wireless network. At first, we analyzed the secure connectivity for a BS over a SCS as probability that the BS can securely send a message to legitimate MSs, over path loss

channel model. We can calculate a random degree of security by assuming independency of connectivity of the BS with one MS from other MSs.

Then, we calculated the statistic characteristics of out-degree and in-degree for a BS over shadowing fading channel model. Finally we plotted the simulated results.

REFERENCES

[1] P.Madhusudhanan, J.G.Restrepo, Y.E.Liu, T.X. Brown, and K.Baker,"Generalized carrier to interference ratio analysis for the Shotgun cellular system," in IEEE Globecom 2009 Wireless Communications symposium (Honolulu,HI,USA), pp. 1-6, Nov 2009.

[2] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin,"Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[3] Y. Liang, H.V. Poor, and S. Shamai, "Secure communicationover fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] E.Ekrem, andS. Ulukus, "Secrecy capacity region of the Gaussianmulti-receiver wiretap channel" in Proc. IEEE Int. Symp. Inf. Theory (Korea), 2612–2616, 2009.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography—Part I: Secret sharing," IEEE Trans. Inf.Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[6] P.C. Pinto, J.O. Barros, and M.Z. Win, "Physical-layer security in stochastic wireless networks," in Proc. IEEE Int. Conf. Commun. Systems, Guangzhou, China, pp. 974–979, Nov. 2008.

[7] P.C. Pinto, J.O. Barros, and M.Z. Win, "Secure communication in stochastic wireless networks—Part I: connectivity," IEEE Trans. Inf.Forensics Security, vol. 7, no. 1, Feb. 2011.

[8] V.H. Macdonald, "The cellular concept," The Bell SystemTechnical Journal, vol. 58, no. 1, pp. 1541, Jan 1979.

[9] T.X. Brown, "Analysis and coloring of a Shotgun cellular system," in Proceedings of the IEEE Radio and Wireless Conference (RAWCON) 98, IEEE pub, pp. 51–54, 1998.

[10] T.X. Brown, "Analysis of Shotgun cellular systems," Submitted to IEEE JSAC, Jan. 1999.

[11] T.X. Brown, "Dynamic channel assignment in Shotgun cellular systems,"in Proceedings of the IEEE Radio and Wireless Conference (RAWCON) 99, IEEE, pp. 147–150, 1999.

[12] T.X. Brown, "Cellular performance bounds via Shotgun cellular systems," Selected Areas inCommunications, IEEE Journal, vol. 18, pp. 2443-2455, Nov 2000.

[13] T.X. Brown, "Practical cellular performance bounds via Shotgun cellular systems", IEEE JSAC, vol. 18, no. 11, pp. 2443–2455, Nov. 2000.

[14] P.Madhusudhanan, J.G.Restrepo, Y.E.Liu, T.X. Brown, and K.Baker, "Generalized carrier to interference ratio analysis for the Shotgun cellular system in multiple dimensions," CORR, Vol.abs/1002,3943,2010.

[15] P.Madhusudhanan, J.G.Restrepo, Y.E.Liu, T.X. Brown, and K.Baker, "Multi-tier network performance analysis using a Shotgun cellular system," CoRR, Vol. abs/1110.3267,2011.

[16] C. Tepedelenlio, "Applications of stochastic ordering to wireless communications", IEEE Transactions on Wireless Communications, vol. 10, no. 12, December 2011.

[17] P.Madhusudhanan, J.G.Restrepo, Y.E.Liu, T.X. Brown, and K.Baker, "Stochastic ordering based carrier-to-interference ratio analysis for the Shotgun cellular systems," CoRR, vol. abs/1110.3280,2011.

[18] C.E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, no. 7, pp. 379–423, 1948.

[19] A.D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1367, October 1975.

[20] A.B. Carleial, M.E. Hellman, "A note on Wyner's wiretap channel," IEEE Transactions on Information Theory, pp.387-390, May 1977.

[21] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May1978.

[22] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tapchannel," IEEE Trans. Inf. Theory, vol. IT-24, no. 4, pp. 451–456, Jul1978.

[23] P.C. Pinto, J.O. Barros, and M.Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, Feb. 2011.

[24] Peter Haremoes, " Binomial and Poisson distributions as maximum entropy distributions," IEEE Trans. Information Theory,vol.47,no.5,July 2001.

[25] Oliver Johnson, " Log-concavity and the maximum entropy of the poisson distributions," ArXiv: math/0603647v2, 11 Oct 2006.

[26] P.C. Pinto,and M.Z. Win, "A unifying framework for local throughput in wireless networks" arXiv:1007.2814v1 [cs.NI] 16 Jul 2010.

[27] A. Papoulis,and S.Pillai, Probability Random Variables And StochasticProcesses , McGrow-Hill, Fourth edition,2002.