7

Connectivity of Ad hoc 5G Wireless Networks under Denial of Service Attacks

Zituo Jin[1], Santhanakrishnan Anand[2], Koduvayur P. Subbalakshmi[3] and Rajarathnam Chandramouli[3]

[1]Courant Institute of Mathematical Sciences, New York University, USA
[2]Department of Electrical Engineering and Computer Science, New York Institute of Technology, USA
[3]Department of Electrical and Computer Engineering, Stevens Institute of Technology, USA

7.1 Introduction

This chapter studies the network layer effects of denial of service (DoS) in 5G wireless networks. DoS attacks by malicious nodes have mostly been researched in terms of their effect on the physical layer (i.e., loss of wireless connectivity) for the good nodes or in terms of loss of services for the good nodes. However, one vital consequence of DoS on the network layer is that it can cause unreliable, disconnected networks. This chapter presents an analysis to study the connectivity of ad hoc 5G networks under DoS. The ad hoc network is modeled as a random geometric graph and an approximation for the probability that the network is disconnected due to DoS is determined. This research indicates that in the absence of suitable defense mechanisms, DoS can disconnect a network with significantly high probability. Then, alleviation of this effect by cooperation among good users is discussed. For this, spectrum decision protocols are analyzed, in which good users make individual spectrum decisions to detect DoS and then exchange individual sensing results with their one-hop neighbors (i.e., a distributed protocol) or with a centralized controller (a centralized protocol) to increase resilience to DoS. Our distributed protocol can reduce the probability of the network becoming disconnected under DoS by 31% to two orders of magnitude. The centralized protocol can almost

eliminate the effect of DoS on the network layer under certain spatial density of malicious users.

The number of connected Internet devices is expected to reach 50 billion by the year 2020 [1]. The Fifth generation (5G) wireless networks vision is to provide connectivity with low latency, enhanced quality-of-service (QoS), low energy, mobility, large spectral efficiency for all the devices taking into account the growth in the number of devices [2]. This motivated the deployment of unlicensed access to the 4G long term evolution (LTE) networks [3]. In the recent AWS-3 spectrum auction, cellular companies spent $44.9 billion for licenses to 65 MHz of spectrum [4]. Though unlicensed spectrum is less valuable to cellular companies due to stricter transmission rules and the inability to limit other interferers, the potential to use such bands to augment capacity in certain areas is attractive because devices can use these bands at no cost. For example, in 2014, up to 46% of potential cellular data was offloaded to Wi-Fi [5].

Dynamic spectrum access (DSA) [6] based cognitive radio networks [7] are expected to be an integral part of 5G wireless networks. Device-to-device (D2D) communication is also recognized as one of the technology components of the evolving 5G architecture by the European Union project, Mobile and wireless communications Enablers for the Twenty-twenty Information Society (METIS) [8]. Integration of D2D communication into incumbent 3GPP networks was discussed in [9]. Ye et al. [10] compared infrastructure vs ad hoc mode of communication for D2D communications and found ad hoc mode to be better. More detailed analysis for the achievable rates and signal-to-interference-noise-ratio (SINR) distributions were provided in [11]. Since D2D communications take place without infrastructure, it is essential to efficiently design ad hoc 5G wireless networks.

The access of LTE devices to unlicensed spectrum (or D2D communications) is achieved by "listen before talk (LBT)" spectrum etiquette [3] similar to the secondary user spectrum etiquette in dynamic spectrum access (DSA) networks [12]. Al-Dulaimi et al. proposed a modified LBT etiquette to take into account the interference constraints on Wi-Fi users [13]. However, the access to unrestricted unlicensed spectrum or D2D communications can be susceptible to denial of service (DoS) attacks [14], which have not been discussed in detail for 5G wireless networks. Few types of DoS attacks and their mitigation are discussed in [15, 16]. Li et al. discuss denial of service attacks and malicious attacks [15], where in DoS is measured based on loss of QoS and frequencies that experience DoS are black-listed. Such mechanisms can end up being inadequate because it results in false alarms although the

probability of detection is large [17]. In [16], Klassen and Yang perform NS-3 based simulations to show that DoS attack can be mitigated by intrusion detection. However, these studies are not applicable to 5G wireless networks because in unlicensed access, malicious nodes can neither be localized nor identified.

The DoS attack that 5G networks are susceptible to, is similar to primary user emulation attack (PUEA), introduced in [18, 19], unique to cognitive radio enabled dynamic spectrum access (DSA) networks [20]. In this type of attack, a set of malicious secondary users mimic the primary transmitter, leading other secondary users to believe that a primary user is active, when, in fact, it is not. This makes the good (non-malicious) secondary users, following normal spectrum evacuation process, to vacate the spectrum unnecessarily, causing spectrum wastage. PUEA was first discussed by Chen et al. in [18] and [19]. In [18], two mechanisms to detect PUEA were proposed, namely, the distance ratio test and the distance difference test based on the correlation between the length of wireless link and the received signal strength. In [19], a defense mechanism against PUEA was proposed by locating the spurious transmission via an underlying sensor network and comparing it with the known location of the primary transmitter. Anand et al. presented the first analytical model to characterize the probability of successful PUEA based on energy detection in [21]. Jin et al. then proposed two hypothesis test based approaches [22, 23], which enable each individual good secondary user to detect PUEA.

In the literature, PUEA or DoS in general, has mostly been studied from the perspective of its impact on the physical (PHY) layer, but DoS can also affect the performance of DSA networks at higher layers.

As an example, at the link layer, DoS can cause blocking of new calls and dropping of ongoing calls for delay intolerant traffic and cause additional delay for delay tolerant traffic. Jin et al. presented the first analysis of link layer effects of DoS attacks in [24] and [25], where it was shown how PUEA can adversely affect the link layer performance if it is not carefully addressed. DoS also affects connectivity of the network. Xing and Wang discussed connectivity of ad hoc networks subject to DoS attacks [26]. However, they only analyzed nodes that get isolated (i.e., have no links incident on them). As will be shown in the example in Section 7.2, DoS can disconnect a networks without necessarily creating isolated nodes. Therefore, a more detailed analysis of the connectivity of ad hoc networks under DoS is required.

This chapter, addresses two issues regarding the network level impact of DoS, i.e., (i) Can DoS also affect the network connectivity of ad hoc 5G wireless networks? and (ii) Can good users collaborate in a centralized and

distributed manner, to mitigate the adverse effect of DoS on the network layer?

First, the ad hoc network is modeled as a random geometric graph and an Erdös-Rényi graph based approximate analysis is performed to compute the probability that DoS disconnects the network. Then, centralized [27] and distributed [28] cooperation between the good users is studied to mitigate this effect of DoS. Results indicate that for a small network (a network with 100 secondary users or less), a 5% probability of successful DoS attack results in a significantly large (more than 20%) probability of disconnecting a connected ad hoc network. For small number of malicious users, the centralized protocol proposed in [27] can almost surely guarantee a connected network even in the presence of DoS. For large number of malicious users, the centralized protocol can reduce the probability of the network being disconnected as a consequence of DoS, by about 20%. The distributed protocol presented in [28], can reduce the probability of DoS causing a disconnected network, by about 30% to two orders of magnitude.

7.2 Problem Definition

Consider an example ad-hoc network with three available channels, as shown in Figure 7.1. Nodes communicate with each other using one of three spectrum bands. Figure 7.1 shows a snapshot in which node-pairs (A, D), (B, C) and (E, F) communicate on channel 1.

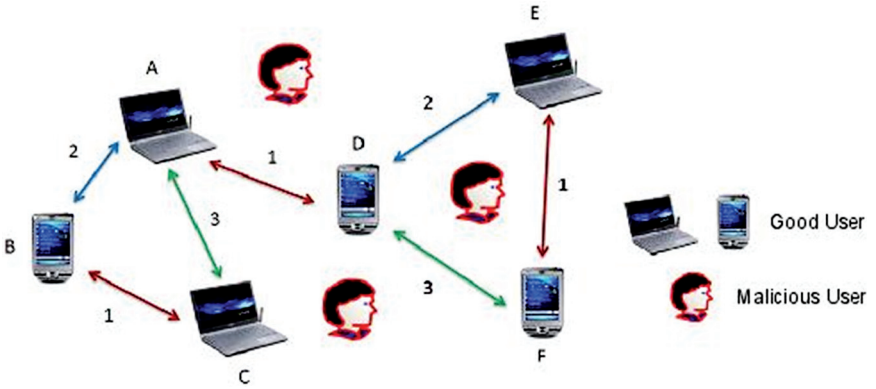


Figure 7.1 A typical ad-hoc network. Nodes A and D are cut-vertices. If DoS is successfully launched on channel 1, node-pairs (A, D), (B, C) and (E, F) will vacate channel 1, thereby resulting in a disconnected network.

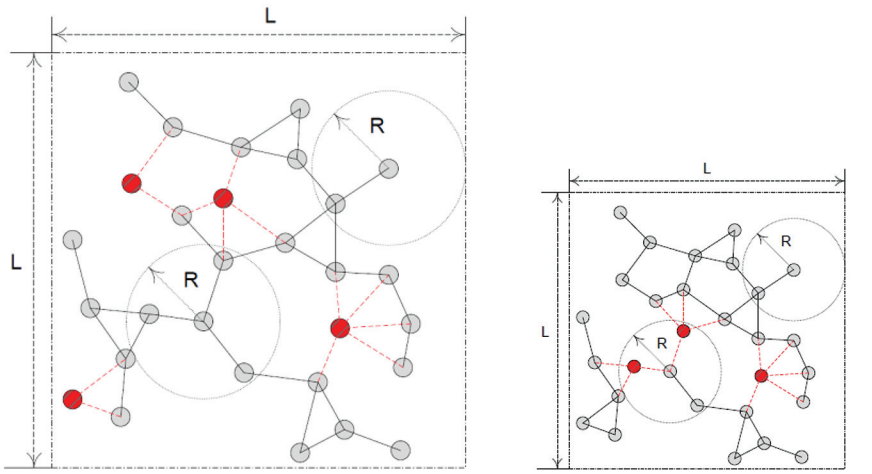
If DoS is successfully launched on channel 1, then these node-pairs need to look for another channel for communication. Since all the three available channels are already in use, these node-pairs cannot find an alternate channel and hence lose the connectivity between them. Since A and D form the cut-vertices of the network, the set of nodes, {A, B, C} will find no means of reaching the set of nodes, {D, E, F}, thus rendering the network disconnected and hence, unreliable. Based on this example, it can be argued that DoS can affect the network layer performance of ad hoc networks adversely, if it is not carefully mitigated.

Since the primary function of the network layer is the routing of data packets to their destinations, a basic requirement for efficient network layer performance is the connectivity of the underlying ad hoc network graph. The good users form the vertices of the underlying network graph and two vertices share an edge if the corresponding secondary users are one hop neighbors, i.e., they are within a specified radio "hearing distance", R, from each other. The network itself is connected if it is possible for packets from any node to reach any other node (possibly over several hops). One metric that can be used to measure the network layer performance is the probability of the network being connected.

If malicious users launch a DoS attack, some of the good users may succumb to the attack and evacuate the spectrum band, while some may be able to detect the attack and stay in the band. As shown in Figure 7.2, the set of remaining nodes could possibly remain connected to each other or could also form a disconnected network where at least two nodes cannot reach each other. The probability that the network becomes disconnected under DoS, is used as a metric to gauge the severity of the attack. The analysis for the case when the network is connected before DoS is launched, is presented. The analysis can easily be extended to the case when the network is disconnected before DoS, by studying each connected component separately.

The objectives in this chapter are as follows.

- Develop an analysis to measure the probability that DoS disconnects a connected ad hoc network.
- Study the probability that DoS renders a connected ad hoc network, disconnected, when deploying the centralized protocol developed in [27] and the distributed protocol developed in [28] are deployed.



(a) Connected network after DoS attack

(b) Disconnected network after DoS attack

Figure 7.2 A connected ad hoc network with users independently and uniformly distributed in an L × L grid. All users have "hearing distance" R, within which they can communicate with each other. Each user could potentially be affected by DoS. The users succumb to the attack are marked red and have to be removed, along with all associated links. The removal of the DoS victims could lead to either a connected or disconnected network.

7.3 Connectivity Analysis

The underlying network graph can be modeled as a random geometric graph [29], where each vertex represents a good user and an edge between two vertices indicates that the two corresponding users are within a distance, *R*, of each other. The DSA network can be viewed as a random geometric graph $G(N, p_{ij})$, where *N* denotes the number of vertices (users), and p_{ij} denotes the probability that there exists an edge between the *i*th and the *j*th vertices, i.e., the probability that vertices *i* and *j* are less than a distance *R* apart. Note that $p_{ij} = p_{ji}, \forall\, i, j$.

The probability, $\mathrm{p_{ij}}$, is computed as follows. Let node i be located at $(\mathrm{x_i}, \mathrm{y_i})$ and node j be located at $(\mathrm{x_j}, \mathrm{y_j})$. The co-ordinates, $\mathrm{x_i}$, $\mathrm{y_i}$, $\mathrm{x_j}$ and $\mathrm{y_j}$ are all independent and uniformly distributed in $(0, \mathrm{L})$. Conditioned on $\mathrm{x_i}$ and $\mathrm{y_i}$, the probability, $\mathrm{p_{ij}}(\mathrm{x_i}, \mathrm{y_i})$ can be written as

$$p_{ij}(x_i, y_i) = \frac{1}{L^2} \int_{y_j=y_{\min}}^{y_{\max}} \int_{x_j=x_{\min}}^{x_{\max}} dx_j dy_j, \tag{7.1}$$

where
$\mathrm{x_{min}} = \max(0, \mathrm{x_i} - \sqrt{\mathrm{R}^2 - (\mathrm{y_i} - \mathrm{y_j})^2})$, $\mathrm{x_{max}} = \min(\mathrm{L}, \mathrm{x_i} + \sqrt{\mathrm{R}^2 - (\mathrm{y_i} - \mathrm{y_j})^2})$, $\mathrm{y_{min}} = \max(0, \mathrm{y_i} - \mathrm{R})$ and $\mathrm{y_{max}} = \min(\mathrm{L}, \mathrm{y_i} + \mathrm{R})$. Averaging over $\mathrm{x_i}$ and $\mathrm{y_i}$, $\mathrm{p_{ij}}$ is obtained as

$$p_{ij} = \frac{1}{L^2} \int_{y_i=0}^{L} \int_{x_i=0}^{L} p_{ij}(x_i, y_i) dx_i dy_i, \tag{7.2}$$

which is independent of i and j since $\mathrm{x_i}$, $\mathrm{y_i}$, $\mathrm{x_j}$ and $\mathrm{y_j}$ are all mutually independent and identically distributed. Therefore, $\mathrm{p_{ij}}$ in Equation (7.2) can be written as $\overline{p}$ and the random geometric graph can be represented as $\mathrm{G}(\mathrm{N}, \overline{p})$. First, the probability that $\mathrm{G}(\mathrm{N}, \overline{p})$ is connected needs to be computed. Since the analysis of random geometric graphs is complex because some links are dependent on others due to *triangle inequality* [29], the graph is analyzed as if it were a Erdös-Rényi graph [30][1].

Let $\mathrm{p_c}(\mathrm{N})$ denote the probability that $\mathrm{G}(\mathrm{N}, \overline{p})$ is connected and $\mathrm{q}(\mathrm{N}) \triangleq 1 - \mathrm{p_c}(\mathrm{N})$ denote the probability that $\mathrm{G}(\mathrm{N}, \overline{p})$ is disconnected. When $\mathrm{G}(\mathrm{N}, \overline{p})$ is disconnected, any arbitrary vertex, i, must belong to a component with k vertices, $1 \leq \mathrm{k} \leq \mathrm{N} - 1$. Let $\mathrm{G}(k, \overline{p})$ denote the sub-graph that contains the arbitrary vertex, i. An arbitrary vertex, i, belongs to a component with exactly, k vertices, with probability, $\mathrm{p^{(i)}(k)}$, when $\mathrm{G}(k, \overline{p})$ is connected and there is no edge from any vertex in $\mathrm{G}(k, \overline{p})$ to any of the remaining $\mathrm{N} - \mathrm{k}$ vertices. Therefore, $\mathrm{p^{(i)}(k)}$ can be written as

$$\mathrm{p^{(i)}(k)} = \mathrm{p_c(k)}(1 - \overline{\mathrm{p}})^{\mathrm{k(N-k)}} \tag{7.3}$$

The probability that $\mathrm{G}(\mathrm{N}, \overline{\mathrm{p}})$ is initially disconnected, $\mathrm{q(N)}$, can then be written as

$$\mathrm{q(N)} = \sum_{\mathrm{k=1}}^{\mathrm{N-1}} \binom{\mathrm{N-1}}{\mathrm{k-1}} \mathrm{p_c(k)}(1 - \overline{\mathrm{p}})^{\mathrm{k(N-k)}}, \tag{7.4}$$

and hence, the probability that $\mathrm{G}(\mathrm{N}, \overline{\mathrm{p}})$ is initially connected, $\mathrm{p_c(N)}$, can then be written as

$$\begin{aligned} p_c(N) &= 1 - q(N) \\ &= 1 - \sum_{k=1}^{N-1} \binom{N-1}{k-1} p_c(k)(1 - \overline{\mathrm{p}})^{k(N-k)}, \end{aligned} \tag{7.5}$$

where $\mathrm{p_c(1)} = 1$ and $\mathrm{p_c(2)} = \overline{\mathrm{p}}$.

[1] Such approximations have been done in the past, e.g., [31].

Now, it is essential to calculate the probability that DoS disconnects an initially connected network. All nodes succumb to DoS with probability, p_{DoS} independent of each other. When a node is affected by DoS, the node and all edges incident on the node have to be removed. This is equivalent to independently and randomly removing vertices in $\mathrm{G}(\mathrm{N}, \overline{\mathrm{p}})$, along with all associated links, with probability p_{DoS}. There moval, thus, can be modeled as a Bernoulli trial with success probability p_{DoS}. Hence, the number of secondary users becoming victims of DoS, n_{DoS}, is binomially distributed, i.e., $n_{\mathrm{DoS}} \sim Binomial\ (N, p_{\mathrm{DoS}})$. After the removal process is completed, the resultant graph is modeled as a new random Erdös-Rényi graph $G(\widehat{N}, \quad \acute{\overline{p}})$, where $\acute{\overline{p}} = \overline{p}$ and $\widehat{N}$ is given by

$$\widehat{N} = N - E[n_{\mathrm{DoS}}] = N(1 - p_{\mathrm{DoS}}). \tag{7.6}$$

The probability that $G(\widehat{\mathrm{N}}, \overline{p})$ is connected, $p_c(\widehat{N})$, can be obtained from Equation (7.5). The probability that DoS disconnects a network that is initially connected, i.e., the conditional probability, $\mathrm{P_r}\{G(\acute{N}, \overline{p})\ \mathrm{disconnected}| G(N, \overline{p})\mathrm{connected}\}$, denoted by $p_{\mathrm{disconnect}}$, can be written as

$$p_{\mathrm{disconnect}} = 1 - \frac{\mathrm{P_r}\{G(\widehat{N}, \overline{p})\mathrm{connected}, G(N, \overline{p})\mathrm{connected}\}}{\mathrm{P_r}\{G\,(N, \overline{p\,})\mathrm{connected}\}} \tag{7.7}$$

Since the event that $G(\hat{N}, \overline{p})$ is connected is a subset of the event that $G(N, \overline{p})$ is connected, $p_{\mathrm{disconnect}}$ can be evaluated as

$$p_{\mathrm{disconnect}} = 1 - \frac{\mathrm{P_r}\{G(\widehat{N}, \overline{p})\mathrm{connected}\}}{\mathrm{P_r}\,\{G(N, \overline{p\,})\mathrm{connected}\}} = 1 - \frac{p_c(\widehat{N})}{p_c(N)} \tag{7.8}$$

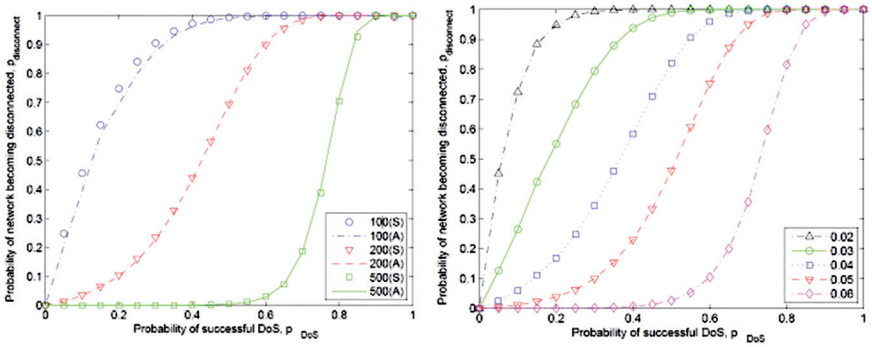
where $p_c(.)$ is given by Equation (7.5).

The discussion thus far for the derivation of $p_{\mathrm{disconnect}}$ in Equation (7.8) does not consider any defense mechanisms against DoS. It is noted from Equation (7.8) that the factor that can be controlled to reduce the value of $p_{\mathrm{disconnect}}$ is the probability that nodes succumb to PUEA, p_{DoS}. One can reduce p_{DoS} by deploying the detection mechanism for each individual secondary user, specified in [27]. The value of p_{DoS} can be further reduced by deploying the centralized protocol presented in [27] or the distributed protocol developed in [28]. The centralized protocol developed in [27] is more efficient in keeping the network connected even in the presence of DoS attacks (as will be seen in Section 7.4), but requires the presence of a centralized controller,

which may or may not be possible in all DSA networks. The distributed protocol is not as efficient as the centralized protocol (as will be observed from the results depicted in Section 7.4), but is less complex to implement.

7.4 Results and Discussions

The locations of all the users including both good and malicious users are considered to be uniformly distributed in a 2000 m $\times$ 2000 m square grid (i.e., $L = 2000$). Each user has a transmission range of $R = 250$ m [7]. Plugging in these values in Equations (7.1) and (7.2), $\overline{p} = 0.0436$. The number of users in the network (i.e., the number of vertices in $G(N, \overline{p})$), N, is set as 100, 200 and 500, respectively. First, the effect of DoS on the connectivity of the network is evaluated. For this, the probability of successful DoS attack, p_{DoS}, is varied from 0 to 1 in increments of 0.05. Figure 7.3(a) depicts the probabilities that DoS disconnects an initially connected ad hoc network (i.e., $p_{\mathrm{disconnect}}$ specified in Equation (7.8)) with different numbers of users. The legends in Figure 7.3(a) are explained as follows. The numbers "100", "200" and "500" represent 100, 200 and 500 secondary users in the network, respectively, while the parenthesized letters "S" and "A" represent simulations results (obtained by C based simulations on UBUNTU Linux platform) and analytical results (using the analysis presented in Section 7.3), respectively.



(a) Varying N (b) Varying $\overline{p}$

Figure 7.3 Comparison of probability that PUEA disconnects an initially connected network with different numbers of secondary users, N and different values of the probability that any two secondary users have a link, $\overline{p}$. In Figure (a), $\overline{p} = 0.0436$. The numbers "100", "200" and "500" in the legends represent 100, 200 and 500 secondary users in the network, respectively, while the parenthesized letters "S" and "A" represent the results from simulations and analysis, respectively. In Figure (b), The numbers "0.02", "0.03", "0.04", "0.05" and "0.06" in the legends represent the probabilities that any two secondary users have a direct link set as "0.02", "0.03", "0.04", "0.05" and "0.06", respectively.

It can be seen from Figure 7.3(a) that as the number of users increases, the network becomes more resilient to disconnectedness under DoS. For example, when $p_{\mathrm{DoS}} = 0.45$, the networks with 100 and 200 secondary users can have a $p_{\mathrm{disconnect}}$ up to about 0.99 and 0.57, respectively, while the network with 500 secondary users achieves almost 0 for $p_{\mathrm{disconnect}}$. That is equivalent to saying that the network with 500 secondary users would almost surely remain connected under DoS as long as the probability of successful DoS attack does not exceed 0.45. This is because, as *N* increases, for the same *R*, i.e., for the same value of $\overline{p}$, the average number of neighbors, $N\overline{p}$, increases for each node. This means that the degree of each node increases and therefore, the probability that the network is connected, increases [29, 30]. It is also observed from Figure 7.3(a) that when the probability of successful DoS attack is high enough, e.g., when $p_{\mathrm{DoS}} = 0.9$, which is the case in networks with no defense mechanisms for DoS, even the network with 500 secondary users becomes disconnected under DoS.

The effect of the probability that any two secondary users have a direct link, $\overline{p}$, on the probability that DoS disconnects a initially connected network, $p_{\mathrm{disconnect}}$, is also studied. The value of $\overline{p}$ can be varied in practice, either by modifying *R* or by increasing the area of the square grid, *L*2. The number of secondary users is fixed at $N = 200$ and the probability of successful PUEA p_{DoS} is varied from 0 to 1 in increments of 0.05. Figure 7.3(b) depicts the probabilities that DoS disconnects an initially connected network with respect to p_{DoS} for varying values of $\overline{p}$. The numbers "0.02", "0.03", "0.04", "0.05" and "0.06" in the legends represent $\overline{p}$ = "0.02", "0.03", "0.04", "0.05" and "0.06", respectively. It is observed from Figure 7.3(b) that as $\overline{p}$ increases from 0.02 to 0.06, $p_{\mathrm{disconnect}}$ decreases, indicating that the network is more likely to remain connected under DoS. For example, when $p_{\mathrm{DoS}} = 0.4$ and $\overline{p} = 0.02$, the network is almost surely disconnected, while for the same value of p_{DoS}, when $\overline{p} = 0.06$, the network is almost surely connected. This is intuitively correct because $\overline{p}$ increases when the grid size, *L*, decreases or when the transmission range, *R*, increases. In both these cases, more nodes tend to be in the transmission range of each other, even after DoS, which, in turn, results in more number of edges in the graph after the removal of nodes that succumb to DoS, thereby increasing the probability that the graph is connected even under DoS attack. However, increase in p_{DoS} results in removal of more nodes and edges, and canstill disconnect the network with a high probability. For example, when $p_{\mathrm{DoS}} > 0.85$, the network is almost surely disconnected for $\overline{p} \leq 0.06$.

Next, the effect of DoS on the network connectivity performance in the presence of defense mechanisms for DoS are studied, considering three defense mechanisms, (i) the individual detection mechanism proposed in [27], (ii) the centralized protocol developed in [27] and (iii) the distributed protocol developed in [28]. A network with 200 secondary users (i.e., $N = 200$ vertices in $G(N, \overline{p})$) is considered and the strength of DoS is increased by increasing the average number of malicious users, $E[Nm]$. For each value of $E[Nm]$, the probability of successful DoS, p_{DoS}, is computed for the individual detection mechanism, the centralized protocol (according to the analysis described in [27]) and for the distributed protocol in [28].

Figure 7.4 shows the probabilities that DoS disconnects an initially connected network, $p_{\mathrm{disconnect}}$, after deploying DoS detection and mitigation

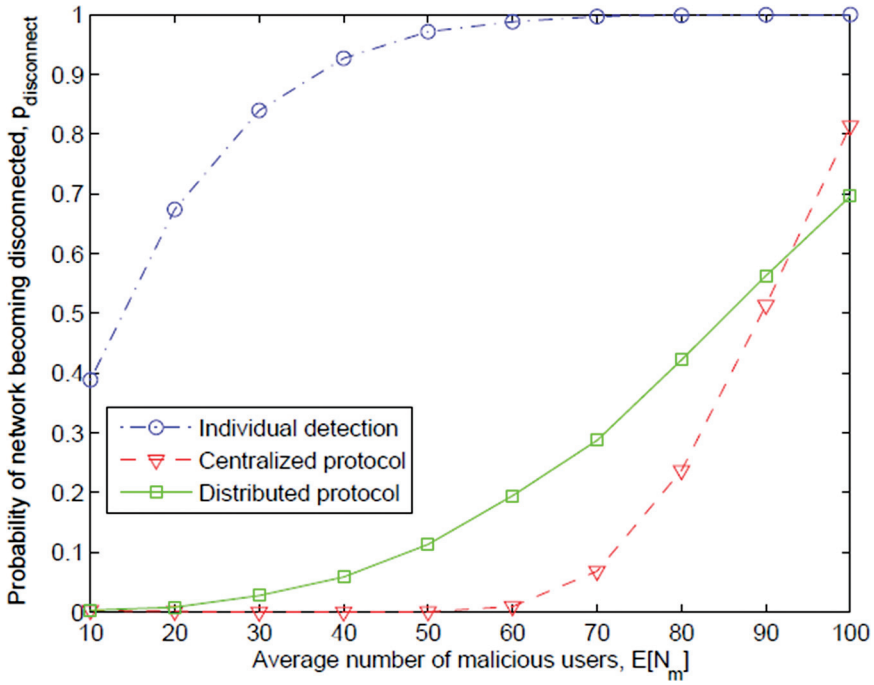


Figure 7.4 Comparison on probability that DoS disconnects an initially connected network after deploying detection and mitigation mechanisms. The probability that any two secondary users have a direct link is 0.0436. The legends "Individual detection" represents the individual detection mechanism described in [27]. "Centralized protocol" and "Distributed protocol" represent the centralized and the distributed protocols proposed in [27] and [28], respectively.

mechanisms[2]. It is observed from Figure 7.4 that different DoS detection and mitigation mechanisms exhibit significantly different impact on keeping the network connected. While the network implementing only the individual detection mechanism shows some resilience to DoS compared to the network with no defense mechanisms against DoS[3], its ability to keep the network connected under DoS is still poor. For example, even with 20 malicious users launching DoS, the probability of network becoming disconnected is about 0.7. This shows that when network level impact is considered, it makes more sense for a collaborative approach to spectrum decision than taking an individual decision. The results shown in Figure 7.4 indicate that the centralized protocol proposed in [27] and the distributed protocol proposed in [28] are effective in maintaining the network connected (and hence, increase reliability) under DoS. For example, when the network has no more than 60 malicious users, the centralized protocol can almost surely maintain the network connected under DoS. When the number of malicious users increases, the centralized protocol can still reduce the probability of the network becoming disconnected due to PUEA by about 20%. The distributed protocol proposed in [28] can improve the probability of the network becoming disconnected due to DoS by about 31% when the number of malicious users is large. For small number of malicious users, the distributed protocol can improve the probability that DoS disconnects the network, by two orders of magnitude.

It is observed that the performance of the distributed protocol is better than that of the centralized protocol for lower loads of malicious users. To understand this behavior in more detail, the probability of successful DoS when deploying the distributed protocol proposed in [28] with that when deploying the centralized protocol proposed in [27] are compared and depicted in Figure 7.5. It is observed that the distributed protocol outperforms the centralized protocol in terms of successfully detecting DoS when the expected number of malicious users $E[Nm] < 45$. For larger number of malicious users, the centralized protocol results in smaller probability of successful DoS and therefore, smaller probability of a disconnected ad hoc network under DoS. The reason for this behavior is explained below.

In a network with N nodes, let the probability that any node succumbs to DoS while implementing the individual detection mechanism alone, be p_{DoS}. While deploying the centralized protocol in [27], a node finally succumbs

[2]The legends "Individual detection" represents the individual detection mechanism described in [27], while "Centralized protocol" and "Distributed protocol" represent the centralized and the distributed protocols proposed in [27] and in [28], respectively.

[3]In such a network, every time DoS is launched, it will succeed with probability one.

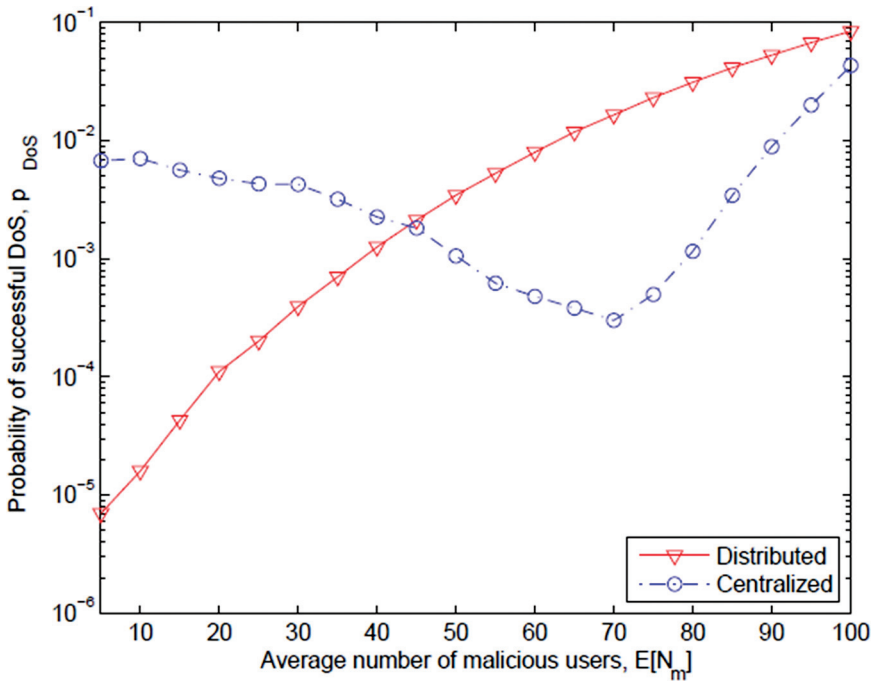


Figure 7.5 Probability of successful DoS by using the centralized protocol in [27] and the distributed protocol presented in [28].

to DoS if the fraction of nodes individually succumbing to DoS (using the individual detection mechanism alone) is greater than a specified threshold, i.e., the probability of successful DoS while deploying the centralized protocol, $p_{\mathrm{DoS}}^{\mathrm{centralized}}$, is approximately written as

$$p_{\mathrm{DoS}}^{\mathrm{centralized}} \approx \mathrm{P_r}\left\{N_{p_{\mathrm{DoS}}} > thershold\right\} \tag{7.9}$$

In a network deploying the distributed protocol presented in [28], a node succumbs to DoS if the node itself and ALL its neighbors succumb to DoS while making the individual decision. Therefore, the probability of successful DoS while deploying the distributed protocol with a node with N_0 neighbors, $p_{\mathrm{DoS}}^{\mathrm{distributed}}$, can be written as

$$p_{\mathrm{DoS}}^{\mathrm{distributed}} = \left(p_{\mathrm{DoS}}\right)^{N_0+1} \tag{7.10}$$

When the number of malicious users is small, each node can detect DoS better while implementing the individual detection mechanism alone, i.e., p_{DoS} is

small. For smaller values of p_{DoS}, the value of $p_{\mathrm{DoS}}^{\mathrm{distributed}}$ in Equtaion (7.10) is negligible and is likely to be smaller than the value of $p_{\mathrm{DoS}}^{\mathrm{centralized}}$ in Equation (7.9). However, when the number of malicious users increase, p_{DoS} increases and the value of $p_{\mathrm{DoS}}^{\mathrm{distributed}}$ in Equation (7.10) maybe significantly larger than that of $p_{\mathrm{DoS}}^{\mathrm{centralized}}$ in Equation (7.9), resulting in better performance for the centralized protocol.

7.5 Conclusions

This chapter analyzed the network layer performance of ad hoc 5G wireless networks under denial of service attacks, in terms connectivity. The ad hoc network was modeled as a random geometric graph and an approximate Erdös-Rényi graph based analysis was performed to determine the probability that DoS disconnects a connected ad hoc network. Numerical results indicated that although connectivity of the network under DoS can be enhanced in a denser network, DoS should always be treated with defense mechanisms for the network to stay connected when nodes are more vulnerable to the attack. The network layer performance when deploying centralized and distributed defense mechanisms against DoS was also discussed. The distributed protocol reduced the probability of the network becoming disconnected by 31% to two orders of magnitude. The centralized protocol was shown to prevent the network from becoming disconnected when the number of malicious users is small. When the number of malicious users increases, the centralized protocol can reduce the probability of DoS disconnecting the network, by about 20%.

References

[1] UMTS, "Mobile traffic forecasts 2010–2020," Report, UMTS Forum, Jan. 2011.

[2] D. R. C. S. E. C. Limited, "5G Vision," White Paper, Feb. 2015. [Online]. Available: http://www.samsung.com/global/business-images/insights/2015/Samsung-5G-Vision-0.pdf

[3] H. Technologies, "U-LTE: Unlicensed spectrum utilization of LTE." [Online]. Available: http://www.huawei.com/ilink/en/download/HW\327803

[4] B. Munson, "Washington glowing over AWS-3 auction results," Wireless Week, Jan. 2015.

[5] "Cisco visual networking index: Global mobile data traffic forecast update 2014 2019," Cisco White Paper. [Online]. Available: http://cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-indexvni/whitepaperc11-520862.html

[6] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands," Proceeding, First Intl. Workshop on Technol. and Policy for Accessing Spectrum (TAPAS) 2006, Aug. 2006.

[7] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," Proceedings, IEEE Conference on Computer Communications (INFOCOM'2008), pp. 1876–1884, Apr. 2008.

[8] G. Fodor, "D2D communications: What part will it play in 5G," Jul. 2014. [Online]. Available: http://www.ericsson.com/research-blog/5g/device-device-communications/

[9] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," IEEE Commun. Mag., vol. 52, no. 4, pp. 40–48, Apr. 2014.

[10] Q. Ye, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "Resource optimization in device-to-device cellular systems using time-frequency hopping." [Online]. Available: http://arxiv.org/abs/1309.4062

[11] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communications in cellular networks." [Online]. Available: http://arxiv.org/abs/1305.4219

[12] "IEEE Standards for information technology – Telecommunications and information exchange between systems – Wireless Regional Area Networks-Specific Requirements – Part 22-Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," Jun. 2006.

[13] Al-Dulaimi, S.l-Rubaye, Q. Ni, and E. Sousa, "5G communications race: Pursuit of more capacity triggers LTE in unlicensed band," IEEE Vehic. Technol. Mag., vol. 10, no. 1, pp. 43–51, Feb. 2015.

[14] M. Hangargi, "Business need for security: Denial of service attacks in wireless networks," Masters Dissertation, Department of Information Assurance, North Eastern University, Apr. 2012.

[15] Y. Li, B. Kaur, and B. Andersen, "Denial of service prevention for 5G," Wireless Personal Commun., vol. 57, no. 3, pp. 365–376, Apr. 2011.

[16] M. Klassen and N. Yang, "Anomaly based intrusion detection in wireless networks using Bayesian classifier," Proc., Intl. Conf. on Advanced Computational Intelligence (ICACI'2012), Sept. 2012.

[17] S. Anand, S. Sengupta, K. Hong, K. P. Subbalakshmi, R. Chandramouli, and H. Cam, "Exploiting channel fragmentation and aggregation/bonding to create security vulnerabilities," IEEE Trans. on Vehic. Technol., vol. 63, no. 8, pp. 3867–3874, Oct. 2014.

[18] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," Proceedings, IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 110–119, Sep. 2006.

[19] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications: Special Issue on Cognitive Radio Theory and Applications, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[20] M. Wyglinski, M. Nekovee, and Y. T. Hou, Cognitive Radio Communications and Networks: Principles and Practice. Elsevier Inc., 2010.

[21] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2008), Oct. 2008.

[22] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," Proceedings, IEEE International Conference on Communications (ICC'2009), Jun. 2009.

[23] ——, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," ACM SIGMOBILE Mobile Computing and Communications Review, Special Issue on Cognitive Radio Technologies and Systems, vol. 13, no. 2, pp. 74–85, April 2009.

[24] ——, "Performance analysis of dynamic spectrum access networks under primary user emulation attacks," Proceedings, IEEE Global Communications Conference (GLOBECOM'2010), Dec. 2010.

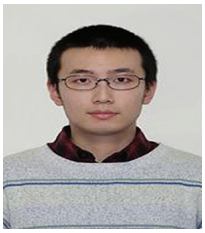
[25] ——, "Impact of primary user emulation attacks on dynamic spectrum access networks," IEEE Trans. on Commun., vol. 60, no. 9, pp. 2635–2643, Sep. 2012.

[26] F. Xing and W. Wang, "Understanding dynamic denial of service attacks in mobile ad hoc networks," Proc., IEEE Military Commun. Conf. (MILCOM'2006), Oct. 2006.

[27] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks," Proceedings, IEEE Global Communications Conference (GLOBECOM'2010), Dec. 2010.

[28] ——, "NEAT: A NEighbor AssisTed spectrum decision protocol for resilience against PUEA," Cognitive Radio Eletromagnetic Spectrum Security (CRESS'2014), Oct. 2014.
[29] M. Penrose, Random Geometric Graphs. Oxford University Press, 2003.
[30] B. Bollobás, Random Graphs, 2nd ed. Cambridge University Press, 2001.
[31] D. Lu, X. Huang, P. Li, and J. Fan, "Connectivity of large-scale cognitive radio ad hoc networks," Proc., IEEE Intl. Conf. on Comp. Commun. (INFOCOM'2012), Mar. 2012.

About the Authors



Zituo Jin (SM'08) is currently pursuing his Master's program in financial management at the Courant Institute of Mathematical Sciences in New York University (NYU). He graduated with a Ph.D. from the Department of Electrical and Computer Engineering at Stevens Institute of Technology, Hoboken, New Jersey. He received the B.E. degree in the Department of Information Engineering from Xi'an Jiaotong University, Xi'an, China, in 2006.

His current research interests include cognitive radio network security and denial-of-service attack in dynamic spectrum access networks. He is a student member of IEEE, IEEE communications society and IEEE computer society.

Santhanakrishnan Anand received his Ph.D. degree from the Indian Institute of Science, Bangalore, India, in 2003. He is currently an Assistant Professor at Department of Electrical and Computer Engineering, New York Institute of Technology.

His current areas of research include spectrum management and security in next generation wireless networks, covert timing channels, social media analytics, dynamics of Wikipedia and information propagation in Internet media.

Dr. Santhanakrishnan Anand received the Seshagiri Kaikini medal for the best Ph.D. dissertation in the electrical sciences division, Indian Institute

of Science for the academic year 2003–2004. He has represented Samsung Electronics in 3GPP SA2 and IEEE 802.20 standardization meetings.

Koduvayur P. Subbalakshmi (Suba) is a Professor at Stevens Institute of Technology. She will serve as a Jefferson Science Fellow at the US Department of State during the academic year 2016–2017.

Her research interests include: Cognitive radio networks, Cognitive Mobile Cloud Computing, Social Media Analytics and Wireless security. She is a Subject Matter Expert for the National Spectrum Consortium.

She is a Founding Associate Editor of the IEEE Transactions on Cognitive Communications and Networking and the Founding Chair of the Security Special Interest Group of the IEEE Technical Committee on Cognitive Networks. She is also a recipient of the NJIHOF Innovator award.

Rajarathnam Chandramouli (Mouli) is the Thomas Hattrick Chair Professor of Information Systems in Electrical and Computer Engineering (ECE) and a Professor in the School of Systems and Enterprises at Stevens Institute of Technology. He is the Founding Director of NSF SAVI: Institute for Cognitive Networking and the Co-Director of the Information Networks and Security (iNFINITY) laboratory. Prior to joining Stevens he was on the ECE faculty at Iowa State University, Ames.

His research covers cognitive radio networking, dynamic spectrum management/access, text analytics and forensics, social media analytics and security, and prototyping/experimental research in these areas.

His research and technology commercialization projects are funded by the National Science Foundation, National Institute of Justice, Department of Defense and the industry.