Security Vulnerability due to Channel Aggregation/Bonding in LTE and HSPA+ Networks

S. Anand, K. Hong, R. Chandramouli
Dept. of ECE
Stevens Institute of Technology
Email: {asanthan, khong, mouli}@stevens.edu

S. Sengupta
Dept. of Math. & Comp. Sc.
City University of New York
Email: ssengupta@jjay.cuny.edu

K. P. Subbalakshmi
Dept. of ECE
Stevens Institute of Technology
Email: ksubbala@stevens.edu

Abstract—We address a unique security vulnerability in long term evolution (LTE) advanced and high speed packet access (HSPA+) wireless networks due to carrier/channel aggregation. This vulnerability is shown to result in various amounts of service disruption based on the radio network parameters and the user locations. Typically, channel aggregation and bonding have been perceived as a means to enhance the bandwidth and throughput for the users. However, this could also result in the loss of orthogonality between the aggregated or bonded spectrum bands. We show that this leads to a security vulnerability that can be exploited by an attacker to cause service disruption. In this case, the attacker need not even operate in the same bands as the user, to be effective. We present an analysis to compare the loss in throughput caused by the vulnerability due to channel aggregation or bonding in advanced LTE and HSPA+ networks. Results indicate that channel aggregation is susceptible to about 70% loss of throughput in LTE networks and about 11-15% in HSPA+ networks compared to systems with no aggregation or bonding. Also, users farther away from the base station suffer larger throughput degradation due to channel aggregation in LTE networks, while it causes larger degradation in throughput for near users in HSPA+ networks. To the best of our knowledge, this is the first attempt to identify and analyze a significant security vulnerability in LTE and HSPA+ networks.

Index Terms – Advanced LTE Networks, HSPA+, Carrier Aggregation, Bonding, Service Disruption.

I. INTRODUCTION

Spectrum in radio access networks (RANs) is scarce and efficient utilization of spectrum has always been a significant challenge in the design of RANs. One means of efficient spectrum utilization is carrier bonding and aggregation. Carrier bonding refers to combining contiguous spectrum bands (e.g., two bands of 20 MHz each) to provide a user, larger (e.g., 40 MHz) bandwidth. Alternatively, non-contiguous spectrum bands can be aggregated (called as carrier aggregation) [1], [2] and allocated to users. Recently, T-Mobile announced that they would bond two contiguous 5MHz channels in HSPA+ [3], that yield 21 Mbps each, to achieve a theoretical throughput of 42 Mbps. Verizon Wireless and AT&T Wireless then proposed channel aggregation [1], [2] (of non-contiguous channels, aggregating the 700 MHz and 3.6 GHz bands) for LTE networks and by using Qualcomm’s Mediaflo spectrum [4], which can theoretically result in double the data rate for LTE users. The RAN working group of the third generation partnership project (3GPP) provide the technical specifications for carrier aggregation and bonding in order to provide higher

should yield larger data rates, we identify a potential vulnerability caused by a unique service disruption attack as a consequence of channel aggregation and bonding. We first present test bed experiments on the 5 GHz WiFi band that illustrates the practicality of the vulnerability motivating the analysis in this paper. This is then followed by a detailed theoretical analysis of the vulnerability in LTE and HSPA+ networks. Typically, the 3GPP LTE and HSPA+ networks use orthogonal frequency division multiple access (OFDMA) based orthogonal carriers for transmission [5], [6]. However, aggregation or bonding of carriers can result in loss of orthogonality and hence, mutual interference or “leakage” from one carrier to the other.

To illustrate this, we conducted test bed experiments based on the SpiderRadio dynamic spectrum access test bed described in [7]. Our prototype for the experiment was based on a software abstraction layer using the off-the-shelf IEEE 802.11 a/b/g wireless cards embedded with Atheros hardware chip sets. We bonded two carriers (corresponding to 5.24 GHz and 5.26 GHz)[8] and measured the power on all the other channels due to bonding.

Fig. 1. SpiderRadio test-bed experiment demonstrating power leakage on other channels due to bonding.
malicious attacker can now transmit on channel or bonding discussed here, is significantly different. Here, a can exploit the correlation between the non-orthogonal carriers vulnerability in networks like 3GPP LTE and HSPA+ that the spectrum bands due to bonding. Similar consequences can also be expected for channel aggregation.

The leakage demonstrated in Fig. 1 can result in a unique vulnerability in networks like 3GPP LTE and HSPA+ that deploy channel aggregation and bonding. A malicious attacker can exploit the correlation between the non-orthogonal carriers (resulting due to carrier aggregation or bonding) and cause service disruption. Service disruption in wireless networks have traditionally been viewed as jamming attacks [9]. However, the service disruption threat due to carrier aggregation or bonding discussed here, is significantly different. Here, a malicious attacker can now transmit on channel to cause service disruption on channel . The attack exploits the loss of orthogonality between channels which is a consequence of carrier aggregation and bonding.

In this paper, we present an analysis of the service disruption caused by a malicious attacker in 3GPP LTE and HSPA+ networks with carrier aggregation or bonding. The loss in throughput due to such vulnerabilities is also investigated. We formulate an optimization problem in which the malicious attacker launches attacks on the carriers so as to use minimum power and cause significant leakage in the system, that can degrade the throughput of the network, significantly. The corresponding loss in throughput caused to different users in a 3GPP advanced LTE and a 3GPP HSPA+ network are computed. Results indicate that channel aggregation can cause about 70% loss of throughput in LTE networks and about 11-15% in HSPA+ networks. The physical interpretation is that aggregating two channels of 20 MHz, 20 Mbps, each, to yield a 40 MHz spectrum band will not provide a throughput of 40 Mbps, but instead can yield about 11-15% less, i.e., about 34 Mbps throughput, which is a significant loss in throughput of about 6 Mbps. In other words, the total bandwidth obtained by aggregation or bonding of carriers is less than the sum of its parts. Also, numerical results show that users farther from the base station suffer higher throughput degradation due to channel aggregation in LTE networks, while channel aggregation causes higher degradation in throughput for near users in HSPA+ networks.

To the best of our knowledge, this is the first attempt to identify and analyze a significant security vulnerability due to carrier aggregation and bonding in LTE and HSPA+ networks. Previously, We identified and security vulnerability and presented its analysis to quantify the service disruption due to channel fragmentation in dynamic spectrum access (DSA) based IEEE 802.22 networks [8]. The analysis presented here is fundamentally different because in [8], we considered DSA based cognitive radio networks in which attackers transmit with as much power as they can to create maximum leakage, while here, the attacker uses minimum power to cause an impact as significant as desired. Our analysis in [8] does not trivially extend to the one presented here. The rest of the paper is organized as follows. The description of the system and the analysis of the service disruption attack is provided in Section II. Numerical results are provided in Section III and conclusions are drawn in Section IV.

II. SERVICE DISRUPTION VULNERABILITY

Consider an LTE or HSPA network with orthogonal carriers. Some of these carriers can be aggregated or bonded to result in bonded/aggregated carriers. Henceforth, throughout the paper, “channel” refers to one of the bonded/aggregated carriers in the system, unless explicitly mentioned otherwise. The bonded channels will not be mutually orthogonal, in general. Therefore, when signals are transmitted in the th channel ( ), it causes energy leakage in the th channel ( ). This kind of energy leakage can be exploited by a malicious attacker in the network to disrupt the communication of the users in the network. A practical example of this was demonstrated in Fig. 1.

It is of interest to determine the service disruption caused by a malicious attacker to the users in the system. In order to perform the analysis, we consider the following system architecture.

- There are channels such that the correlation between channels and is . If the corresponding channels are orthogonal, then .
- On channel , the attacker transmits a signal with signal strength, , that corresponds to a power, .
- The total power that can be transmitted by the attacker on all the channels is .

Let where and and represent the co-variance between channels and , .

Let represent the vector of field strengths on all the channels and let represent the vector of corresponding powers. Signals transmitted on any channel cause a leakage on the other channels since the aggregated or bonded channels are not orthogonal in general. The leakage caused by the attacker on the th channel, , can be written as

\[ l_i = \sum_{j=1}^{N} C_{ij} E_j, \quad \forall i, \]

which can be written as the matrix equation,

\[ \mathbf{l} = \mathbf{C}\mathbf{e}, \]

where . If the channels are all mutually orthogonal, then for . Since the leakage, , the leakage, . Since carrier aggregation or bonding results in non-orthogonal channels, , in general. The power leaked on the th channel can be obtained as . The average power

\[ 1^\text{In practice, it may also be possible that different malicious attackers can collude and create a service disruption. In this case, the analysis is performed by replacing by .} \]
leaked on all the channels in the system, $\mathcal{P}_{\text{leaked}}$, can be written as

$$\mathcal{P}_{\text{leaked}} = \frac{1}{N} \sum_{i=1}^{N} P_i = \frac{1}{N} 1^H 1 = \frac{1}{N} e^H C^H C e,$$

(3)

where $(\cdot)^H$ represents the Hermitian of a vector or a matrix.

Ideally, the attacker allocates its total transmit power, $P_{\text{tot}}$, on all the channels, such that the impact on each of the channels is maximized. In order determine the impact on all the channels, the attacker must have exact knowledge of all the traffic on all the channels in the system, because the impact on a channel also depends on the application run by the user, which, in turn, determines the traffic pattern in the network. This may not be possible in general. More practical scenarios are (i) the attacker tries to maximize the average power due to leakage the attacker wishes to induce on the network. The leakage the attacker wishes to induce is maximized for

$$\sum_{i=1}^{N} P_i = \min_{e} e^H e, \quad \text{subject to the constraints},$$

$$e^H C^H C e = e^H A e \geq \epsilon,$$

(5)

where $A \triangleq C^H C$ and $\epsilon$ is the desired amount of average leakage the attacker wishes to induce on the network. The matrix, $A$, is a Hermitian matrix (i.e., $A^H = A$) and hence, has real eigen values [10]. Let $P$ be the matrix whose columns are the eigen-vectors of $A$. Since $A$ is a Hermitian matrix, $P$ can be chosen to be unitary [10] (i.e., $P^H P = P P^H = I$, the identity matrix, $I$). The vector, $e$ can be written as $[10] e = P d$, where $d = [d_i]_{1 \leq i \leq N}$ is another vector of length, $N$. Let the set of eigen-values of $A$ (called the spectrum of $A$ [10], $\sigma(A)$, be $\sigma(A) = \{\lambda_1, \lambda_2, \cdots, \lambda_N\}$ and without loss of generality, let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. Such an ordering is possible since $\lambda_i$’s are real.

It is then possible to formulate the optimization problem in (4) subject to (5), in terms of $d$. Since $e = P d$ and $P$ is unitary $[10]$

$$e^H e = d^H d.$$

(6)

From (6), the optimization problem in (4) can be written as

$$\min_{d} d^H d = \min_{d} \sum_{i=1}^{N} d_i^2,$$

subject to the constraint (5), which, becomes

$$d^H P^H A P d = d^H D_A d = \sum_{i=1}^{N} \lambda_i d_i^2 \geq \epsilon,$$

(8)

where $D_A = \text{diag}(\lambda_1, \lambda_2, \cdots, \lambda_N)$, is the diagonal matrix of the eigen values of $A$, obtained by unitary transformation of $A$ [10]. The following lemmas and theorem will be used to solve the optimization problem in (7) subject to (8), which, in turn, will be used to solve (4) subject to (5).

**Lemma 2.1:** If $\lambda_k < 0$, $d_k = 0$ at the optimum point.

**Proof:** Let $d = [d_i]_{1 \leq i \leq N}$ be a feasible solution such that $d_k > 0$. Consider another solution $\hat{d} = [\hat{d}_i]_{1 \leq i \leq N}$, where $\hat{d}_k = 0$ and $\hat{d}_j = \hat{d}_j$, $\forall \ j \neq k$. Since $\hat{d}$ is a feasible point,

$$\sum_{i=1}^{N} \lambda_i \hat{d}_i^2 \geq \epsilon,$$

i.e., $\lambda_k \hat{d}_k^2 + \sum_{i \neq k} \lambda_i \hat{d}_i^2 \geq \epsilon,$

i.e., $\sum_{i=1}^{N} \lambda_i \hat{d}_i^2 \geq \epsilon$, since $\lambda_k < 0$.

Therefore, $\hat{d}$ is also a feasible point such that

$$\sum_{i=1}^{N} \hat{d}_i^2 = \sum_{i \neq k} \hat{d}_i^2 < \sum_{i=1}^{N} d_i^2.$$

Lemma 2.1 implies that the attacker must allocate positive $d_i$’s only to the corresponding positive eigen values. The following lemma provides a constraint on the positive $d_i$’s.

**Lemma 2.2:** Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$ and let $\lambda_i < 0$, $i > m$, $m \leq N$. Let $\lambda_i > m, m \leq N$. At the optimum point, $\sum_{m=1}^{m} \lambda_i d_i^2 = \epsilon$, i.e., (8) is met with equality.

**Proof:** From Lemma 2.1, $d_i = 0$, $\forall i > m$. Consider a feasible point $\tilde{d} = [\tilde{d}_i]_{1 \leq i \leq m}$ such that $\sum_{m=1}^{m} \lambda_i \tilde{d}_i^2 = \epsilon$. Let $\Delta \triangleq \tilde{\epsilon} - \epsilon$. It is noted that $\Delta \geq 0$. Consider $\tilde{d} = [\tilde{d}_i]_{1 \leq i \leq m}$, such that $\tilde{d}_m = \sqrt{\tilde{d}_m^2 - \Delta \lambda_m}$ and $\tilde{d}_i = \tilde{d}_i, i = 1, 2, \cdots, m-1, m + 1, \cdots, N$. Therefore,

$$\sum_{m=1}^{m} \lambda_i \tilde{d}_i^2 = \sum_{m=1}^{m} \lambda_i \tilde{d}_i^2 - \Delta = \epsilon,$$

i.e., $\tilde{d}$ is also feasible and

$$\sum_{i=1}^{N} \tilde{d}_i^2 = \sum_{m=1}^{m-1} \tilde{d}_i^2 + \tilde{d}_m^2 - \frac{\Delta}{\lambda_m} < \sum_{i=1}^{N} d_i^2.$$

From Lemmas 2.1 and 2.2, the following theorem which yields the optimal solution, $d^*$, can be obtained.

**Theorem 2.1:** Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$, $m \leq N$ and $\lambda_i < 0$, $i > m$. The objective function in (7) subject to (8) is maximized for $d = [d_i]_{1 \leq i \leq N}$ such that $d_i^* = \sqrt{\frac{\epsilon}{\lambda_i}}$ and $d_m^* = 0$, $i = 2, 3, \cdots, N$.

**Proof:** From Lemmas 2.1, 2.2 and (8),

$$\sum_{i=1}^{N} \lambda_i d_i^2 = \epsilon,$$

i.e., $\sum_{i=1}^{m} \lambda_i d_i^2 = \epsilon$,

i.e., $\lambda_i \sum_{i=1}^{m} d_i^2 \geq \epsilon$,

i.e., $\sum_{i=1}^{m} d_i^2 \geq \frac{\epsilon}{\lambda_i}$,

with equality if and only if $d_i^* = \sqrt{\frac{\epsilon}{\lambda_i}}$ and $d_m^* = 0$, $i = 2, 3, \cdots, N$. 


Since \( \mathbf{e} = \mathbf{P}_d \mathbf{e}^* = \sqrt{\lambda_i} \mathbf{x}_i \), where \( \mathbf{x}_i = [x_{i1}]_{1 \leq i \leq N} \) is the eigen vector corresponding to \( \lambda_i \). Also, since \( \mathbf{d}^H \mathbf{d} = \mathbf{e}^H \mathbf{e} \), the minimum power transmitted by the attacker is \( \frac{\mathbf{d}^H \mathbf{d}}{\lambda_i} \). Since the total power that the attacker can transmit over all the channels is \( P_{\text{tot}} \), it follows that the attack is feasible if and only if \( \epsilon \leq P_{\text{tot}} \lambda_1 \). It is noted that in general, \( x_{i1} \) can be non-zero, \( \forall i \) and hence, the attacker transmits non-zero powers on all the channels to create significant leakage resulting in service disruption.

The reduced signal-to-interference-noise ratio (SINR) at each receiving user in the system can be measured because the power transmitted by the attacker causes additional interference to the user. The reduced SINR results in larger bit error rate (BER), which represents the percentage loss in the power transmitted by the attacker causes additional interference to the user. The SINR and the modulation used. We consider quadrature phase shift keying (QPSK) 16 point quadrature amplitude modulation (16-QAM) and 64 point quadrature amplitude modulation (64-QAM) in our analysis as specified in the LTE [5] and HSPA [6] standards.

III. RESULTS AND DISCUSSION

We consider a 19-macro cell LTE and HSPA system in which users are distributed uniformly in a cell with \( P_{\text{tot}} = 10 \) and \( \epsilon \) is chosen so that \( \epsilon << P_{\text{tot}} \lambda_1 \). Each cell has 10 near users using 64-QAM modulation, 10 far users using QPSK and 10 users using 16-QAM. Channels in the LTE system are aggregated according to the specification in [2] [11], where in, among five channels (centered at 460 MHz, 700 MHz, 803 MHz, 2.6 GHz and 3.75 GHz) [1] the 700 MHz and the 2.6 GHz channels are aggregated. Channels in the HSPA+ system (1 GHz, 1.5 GHz and 2 GHz bands) are aggregated in the HSPA+ system as specified in [3]. Channel gains to the users from the base stations or E-Node B’s and the attacker are generated using the Jake’s model [12].

Figs. 2-4 represents the average loss in throughput in the LTE and HSPA+ networks for the far users deploying QPSK (Fig. 2), users that are neither near nor far, deploying 16-QAM (Fig. 3) and near user deploying 64-QAM (Fig. 4). It is observed from Fig. 2, that the attack discussed in this paper can cause significant loss in throughput for the far users. Particularly, in LTE systems, this loss could be as high as 70%. The impact is much lesser on the high data rate users who are either near the E node B’s (using 64-QAM) or between the E Node B’s and the periphery of the cells (using 16-QAM). This is because, these users being nearer to the E Node Bs are farther from the attacker and perceive lesser impact in terms of percentage loss. However, a loss in throughput of 3-4% (for 64-QAM LTE users) corresponds to a loss in throughput of about 1.7 Mbps when two 20 Mbps channels are aggregated. Therefore the theoretical throughput of 42 Mbps mentioned in [2] does not really yield 42 Mbps but yields only 40 Mbps, which is a significant loss. This loss is more significant for HSPA+ networks as it corresponds to a loss of 4-6 Mbps, thus resulting only in 34 Mbps as against the theoretical rate of 40 Mbps.

Also, Figs. 2 and 3 seem to suggest that the impact on the throughput due to channel aggregation in LTE Advanced networks is more significant (about 70% reduction) than that in HSPA+ networks (about 15%) for the far users and the users that are neither near nor at the periphery of the cells. From Fig. 4, near users in HSPA+ networks suffer larger degradation in throughput (12%) due to channel aggregation than those in advanced LTE networks (3-4%). This is because, the correlation between channels in HSPA+ networks is larger than that in LTE networks. However, the absolute throughput of far users in HSPA+ networks is less than that in LTE networks. Therefore, although the throughput decreases for far users both in LTE as well as in HSPA networks, the percentage in the degradation in LTE networks is more prominent. For near users though, the absolute throughput is large both in LTE as well as in HSPA networks and hence, the degradation in throughput due to the large correlation between channels in HSPA networks is more evident.

![Fig. 2. Average loss in the throughput for far users deploying QPSK in a system with 19 cells. Users are indexed such that whenever \( i < j \), user \( i \) receives less signal strength from the E Node B than user \( j \).](image)

![Fig. 3. Average loss in the throughput for users neither near the E Node B or at the periphery, deploying 16-QAM, in a system with 19 cells. Users are indexed such that whenever \( i < j \), user \( i \) receives less signal strength from the E Node B than user \( j \).](image)
IV. CONCLUSION

We identified a security vulnerability that could lead to service disruption in 3GPP advanced LTE and HSPA+ networks as a consequence of the newly proposed channel aggregation or bonding. We presented an experimental result to motivate the problem and presented an analysis to determine the transmit power of the malicious attacker on all the channels to create significant service disruption while using minimum power. Some key inferences drawn included

- Bonding or aggregating two channels of specified capacities does not yield a channel with the sum of the capacities (the total capacity obtained is less than the sum of its parts).
- Far users or low data rate users perceive larger impact in loss of throughput due to channel aggregation or bonding than near high data rate users.
- The impact on far users is larger in advanced LTE networks than in HSPA+ networks while near users in HSPA+ networks suffer larger impact than those in advanced LTE networks.

REFERENCES