Selfish Manipulation of Cooperative Cellular Communications via Channel Fabrication

Shrikant Adhikarla, Min Suk Kang, and Patrick Tague
Carnegie Mellon University, Pittsburgh, PA
{sadhikar, minsukk, tague}@andrew.cmu.edu

ABSTRACT

In today's cellular networks, user equipment (UE) have suffered from low spectral efficiency at cell-edge region due to high interference from adjacent base stations (BSs), which share the same spectral radio resources. In the recently proposed cooperative cellular networks, geographically separated multiple BSs cooperate on transmission in order to improve the UE's signal-to-interference-plus-noise-ratio (SINR) at cell-edge region. The service provider of the system dynamically assigns the cluster of BSs to achieve higher SINR for the UE while optimizing the use of system radio resources. Although it is the service provider that makes the the clustering decision for the UE, the service provider relies on the UE's input to the decision; i.e., the channel states from the adjacent BSs to the UE. In essence, the operation of the cooperative cellular netwokrs heavily relies on the trust in the UEs. In this paper, we propose a new selfish attack against the cooperative cellular networks; an adversary reprograms her UE to report fabricated channel information to cause the service provider to make a decision that benefits the adversary while wasting its system resources. We evaluate the proposed attack in a cooperative cellular network having various performance goals on the simulation-based experiments and show that the adversary can trick the service provider into expending 3.7 times more radio resources for the adversary and, accordingly, the adversary achieves up to 16 dB SINR gain. Finally, we propose a threshold-based countermeasure for the service provider to detect the attack with approximately 90% of accuracy.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*wireless communication*

General Terms

Security, Algorithms, Reliability, Verification

WiSec'13, April 17-19, 2013, Budapest, Hungary.
Copyright 2013 ACM 978-1-4503-1998-0/13/04 ...$15.00.

Keywords

Cooperative cellular networks; channel fabrication; heuristic attack strategies; anomaly detection

1. INTRODUCTION

In traditional cellular networks, each cell uses a different set of radio frequencies from neighboring cells to avoid inter-cell interference [11] [4]. In today's systems, such as LTE, for better usage of scarce radio resources, all the cells in the system share the single frequency band [2] and thus the inter-cell interference management is important to guarantee the quality-of-service (QoS) to the user equipment (UE) in cell-edge regions [6, 8, 9, 12].

Recently proposed *cooperative communication* technique in cellular networks has gained significant interests for it can implement tighter interference coordination among adjacent multiple base stations (BSs) [5, 16][1]. In cooperative cellular networks, a *cluster* of multiple geographically separated BSs *cooperate* on transmission in order to improve spectral efficiency of the UEs. The major advantage of the coordination is to increase the received signal-to-interference-plus-noise-ratio (SINR) by reducing the amount of the interference and increasing the amount of the signals. The more BSs join the cluster for a UE, the higher SINR the UE achieves. However, in the persepctive of system operations, utilizing more coordinated BSs for the specific UE implies that the system uses additional radio resources that could have been used for other UEs. Therefore, the service provider of the cellular network should carefully determine the cluster in order to efficiently use the system resources.

In order for the BS to make clustering decisions for UE, it needs to know the current channel state at the UE. Due to the information asymmetry between UE and BS, the BS has to rely on the channel reported by the UE.[2]. In essence, the operation of the cooperative cellular network heavily relies on the trust in the UE's.

In this paper, we propose a selfish attack on the cooperative cellular networks; the goal of the adversary is to maximize the received SINR at the adversary's UE by increasing the system radio resources allocated to the UE and the re-

[1] In the literature, it is possible to find cooperative communication systems labeled as "Network MIMO", "Multicellular MIMO", "Multicellular cooperation", "CoMP", or "Distributed Antenna System" [23] [13] [1] [10].

[2] This channel information asymmetry holds only in frequency-division duplex (FDD) systems, which is the more popular system configuration for today's cellular networks. Time-division duplex (TDD) systems do not pose this problem.

quired capability to launch the attack is to reprogram (or execute the malicious codes on her UE to reprogram) her UE's network adapters. We propose three heuristic attack strategies for fabricating the channel information and performe simulation-based experiments to evaluate the proposed attack strategies in a cooperative cellular network model. We design two dynamic clustering models for our cooperative cellular network model; guaranteed minimum SINR model and maximum normalized throughput model. Our evaluation shows that the adversary can obtain 3.7 times more radio resources and, accordingly, achieve up to 16 dB SINR gain. To the best of our knowledge, the proposed selfish attack is first discovered attack against the cooperative cellular networks.

In order to mitigate the proposed attack, we present a threshold-based countermeasure for the service provider to detect the attack with approximately 90% of accuracy. The countermeasure requires only a simple modification to the cluster decision model to detect of abnormal channel reports.

2. SYSTEM MODEL: COOPERATIVE CELLULAR NETWORKS

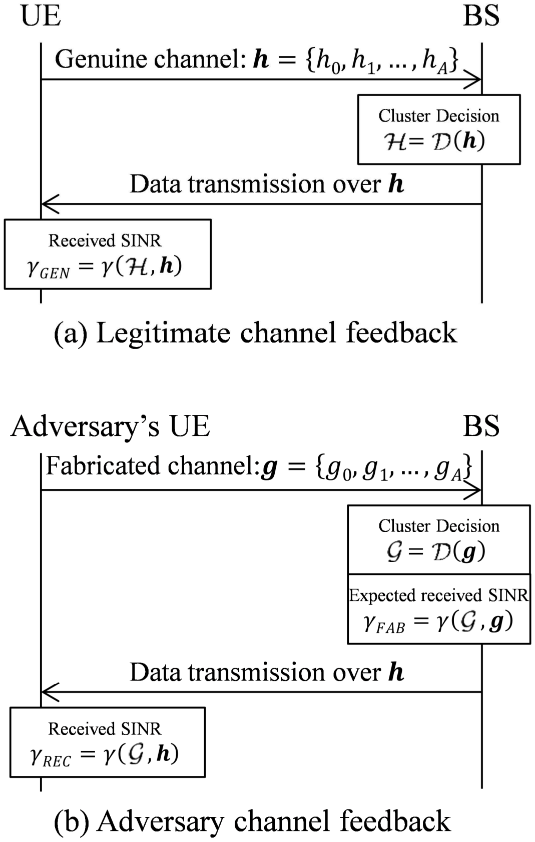
We assume a multi-cell cellular network, where multiple geographically separated BSs manage their own cells and the UEs that belong to them. In this paper, we assume that BSs and UEs are equipped with single antenna. In our system model, a UE is associated with a *primary* base station BS_0 and a set of adjacent base stations, identified by the index set $\mathcal{A} = \{1, \ldots, A\}$. The signal y received by the UE is a combination of the data signals x_i transmitted by these base stations and is given by $y = \sqrt{P_0} h_0 x_0 + \sum_{i\in\mathcal{A}} \sqrt{P_i} h_i x_i + n$, where x_i $(i = 0, \cdots, A)$ is the data signal transmitted from the BS$_i$, h_i $(i = 0, \cdots, A)$ is the channel coefficient from the BS$_i$ to the UE, P_i $(i = 0, \cdots, A)$ is the transmitted power at the BS$_i$, and n is the noise signal at the UE. In non-cooperative conventional multi-cell cellular networks, the signals x_i $(i = 0, \ldots, A)$ are distinct, so those x_i for $i \geq 1$ act as interference from the adjacent cells. In this case, the SINR at the UE is given as $\gamma = \frac{P_0|h_0|^2}{\sum_{i\in\mathcal{A}} P_i|h_i|^2 + N}$, where N is the noise spectral density. In this paper, we assume that all the BS's have the same fixed power transmission level. Thus, the SINR becomes $\gamma = \frac{|h_0|^2}{\sum_{i\in\mathcal{A}}|h_i|^2 + N_0}$, where N_0 is given by N/P_0 .

For cooperative communication we assume that among the set of all adjacent BSs $\mathcal{A}$, the cluster of cooperative BSs $\mathcal{H}$ is selected and the BS's in $\mathcal{H}$ transmit the same x_0 to the UE. The cooperation decision is made at the central entity, which is assumed to be located at the primary BS, by using the channel information vector $\mathbf{h} = \{h_0, h_1, \cdots, h_A\}$. Upon the channel vector $\mathbf{h}$ reported by the UE, the BS decides the cluster $\mathcal{H}$ based on a decision algorithm, denoted here by $\mathcal{D}$ such that $\mathcal{H} = \mathcal{D}(\mathbf{h})$.

Therefore, the SINR at the UE with the BS cooperation is given as

$$\gamma(\mathcal{H}, \mathbf{h}) = \frac{|h_0|^2 + \sum_{c\in\mathcal{H}} |h_c|^2}{\sum_{i\in(\mathcal{A}\setminus\mathcal{H})} |h_i|^2 + N_0}. \tag{1}$$

In this paper, we assume the perfect synchronization among multiple BSs to the UE.


UE
BS
Genuine channel: $\boldsymbol{h} = \{h_0, h_1, \ldots, h_A\}$
Cluster Decision
$\mathcal{H} = \mathcal{D}(\boldsymbol{h})$
Data transmission over $\boldsymbol{h}$
Received SINR
$\gamma_{GEN} = \gamma(\mathcal{H}, \boldsymbol{h})$

(a) Legitimate channel feedback

Adversary's UE
BS
Fabricated channel: $\boldsymbol{g} = \{g_0, g_1, \ldots, g_A\}$
Cluster Decision
$\mathcal{G} = \mathcal{D}(\boldsymbol{g})$
Expected received SINR
$\gamma_{FAB} = \gamma(\mathcal{G}, \boldsymbol{g})$
Data transmission over $\boldsymbol{h}$
Received SINR
$\gamma_{REC} = \gamma(\mathcal{G}, \boldsymbol{h})$

(b) Adversary channel feedback

Figure 1: An adversary can manipulate the BS cooperation model using an SCF attack, fabricating channel information to achieve an increased SINR.

2.1 Clustering Decision Models

The clustering decision process, which determines the set of BSs to cooperate for a UE, is based on the implementation or management of the service providers. As there currently doesn't exists any concrete decision model, as a part of our system model, we design the two following clustering decision models.

Guaranteed Minimum SINR Model: This model $(\mathcal{D}_{th})$ aims to guarantee at least a minimum SINR (γ_{th}) for each UE when deciding the BS cooperation. This model can be used in aiming to guarantee quality of service to each user. If the SINR provided in the absence of cooperation already satisfies the threshold, i.e. $\gamma(\emptyset, \mathbf{h}) \geq \gamma_{th}$, then no cooperation is required. Otherwise, the system chooses the smallest set $\mathcal{H}$ that satisfies the following equation:

$$\mathcal{H} = \underset{\mathcal{H}\neq\emptyset}{\arg\min} |\mathcal{H}| \quad \text{s.t.} \quad \gamma(\mathcal{H}, \mathbf{h}) \geq \gamma_{th}. \tag{2}$$

γ_{th} is a pre-determined threshold value and we note that its choice is critical in determining the number of UE devices that can be supported.

Maximum Normalized Throughput Model: This model $(\mathcal{D}_{max})$ aims to maximize the normalized throughput when deciding the BS cooperation. This model can be used in aiming to guarantee highly efficient resource utilization by the system. In this formulation, the system aims to maximize the Shannon-Hartley capacity [20] per cooperating base station. Independent of the channel bandwidth, this model is specified formally as

$$\begin{aligned} \mathcal{H} = &\quad \arg\max\nolimits_{\mathcal{H}\neq\emptyset} \log_2\left(1+\gamma(\mathcal{H},\mathbf{h})\right)/|\mathcal{H}| && (3)\\ \text{s.t.} &\qquad\qquad \gamma(\mathcal{H},\mathbf{h}) > 0. && (4) \end{aligned}$$

In the above formulation, the system can break ties according to a preference for smaller $|\mathcal{H}|$, or an additional penalty could be imposed to artificially force the cooperating set to be small.

3. SELFISH ATTACK AGAINST COOPERATIVE CELLULAR NETWORKS

We present *Selfish Channel Fabrication*, or SCF, attack. Figure 1 depicts the SCF attack process, described as follows.

The foundation of the SCF attack relies on the fact that the BS determines the cooperation set $\mathcal{H}$ using the decision model $\mathcal{D}$ as a function of the channel information $\mathbf{h}$ provided by the UE. Instead of reporting the truly measured channel quality indicators $\mathbf{h}$, however, a selfish UE can report *fabricated* channel quality indicators $\mathbf{g}$ given by

$$\mathbf{g} = \{g_0,\ g_1, \cdots,\ g_A\}\,. \tag{5}$$

The adversary fabricates the value of $\mathbf{g}$ such that use of cooperation set $\mathcal{G} = \mathcal{D}(\mathbf{g})$ instead of $\mathcal{H} = \mathcal{D}(\mathbf{h})$. Because of the deception of the adversary, the system is forced into provisioning for the SINR, such that,

$$\gamma\left(\mathcal{G},\mathbf{g}\right) = \frac{|g_0|^2 + \sum_{c\in\mathcal{G}} |g_c|^2}{\sum_{i\in(\mathcal{A}\setminus\mathcal{G})} |g_i|^2 + N_0} > \gamma\left(\mathcal{H},\mathbf{h}\right). \tag{6}$$

We note, however that the SINR $\gamma(\mathcal{G},\mathbf{g})$, is only what the BS *believes* it is providing to the UE, while the *true channel* from the BS to the UE behaves according to the actual channel indicators $\mathbf{h}$. Therefore, the *actual* SINR achieved by the selfish UE is $\gamma(\mathcal{G},\mathbf{h})$, so the three SINR values involved in the attack formulation are as follows

- $\gamma\left(\mathcal{H},\mathbf{h}\right)$: SINR that the UE would get when it reports the *genuine* channel indicators $\mathbf{h}$.

- $\gamma\left(\mathcal{G},\mathbf{g}\right)$: SINR that the BS *believes* the UE would get when the *fabricated* channel indicators $\mathbf{g}$ are reported.

- $\gamma\left(\mathcal{G},\mathbf{h}\right)$: SINR that the UE would *actually* get when it reports the *fabricated* channel indicators $\mathbf{g}$.

The goal of the selfish UE is thus to choose $\mathbf{g}$ as a function of $\mathbf{h}$ such that

$$\gamma\left(\mathcal{H},\mathbf{h}\right) < \gamma\left(\mathcal{G},\mathbf{g}\right) < \gamma\left(\mathcal{G},\mathbf{h}\right). \tag{7}$$

The first inequality in (7) implies that the SINR with the fabricated channel indicators should be greater than that with the genuine channel indicators. This must hold because otherwise the selfish UE does not have any motivation in sending the fabricated channel indicators. The second inequality in (7) implies that the SINR that is used for adaptive modulation and coding (AMC) at the BS should be lower than the actual SINR that the UE measures when receiving the packet. This also must hold otherwise the selfish UE cannot decode the packet with low packet error probability[3].

In order to optimize the attack the adversary needs to find the optimum value of $\mathbf{g}$, which satisfies the inequalities in in (7). Furthermore, the attack is only useful if it can be done in a timely manner; specifically, it should be done faster than the cellular system frame time (generally of the order of 5ms). Because of the complex form of the inequality constraints in in (7), the adversary has to rely on the use of heuristic approaches for choosing $\mathbf{g}$, which we address in the next sub-section.

3.1 Heuristic SCF Attack Strategies

In this section, we propose three heuristic strategies for timely computation of $\mathbf{g}$ in the SCF attack. Each strategy provide a different method for mapping the true $\mathbf{h}$ to the fabricated $\mathbf{g}$.

Over-Projecting Interference Channel Indicators (OPICI). The adversary generates $\mathbf{g}$ by increasing the magnitude of interference channel indicators according to $\mathcal{H} = \mathcal{D}(\mathbf{h})$. Thus, when the BS calculates the SINR for the selfish UE using the fabricated and reported $\mathbf{g}$, the BS is tricked into believing that the user needs additional cooperation using the stronger signals that are currently acting as interference. For a given over-projection factor $\alpha > 1$, the OPICI strategy is given by

$$\boxed{\begin{array}{l} \textbf{Given: } \alpha > 1 \text{ ; } \textbf{Choose: } g_i \text{ as} \\ g_i = \begin{cases} h_i & \text{if } i\in\mathcal{H} \\ \alpha h_i & \text{if } i\in\mathcal{A}\setminus\mathcal{H}. \end{cases} \end{array}} \tag{8}$$

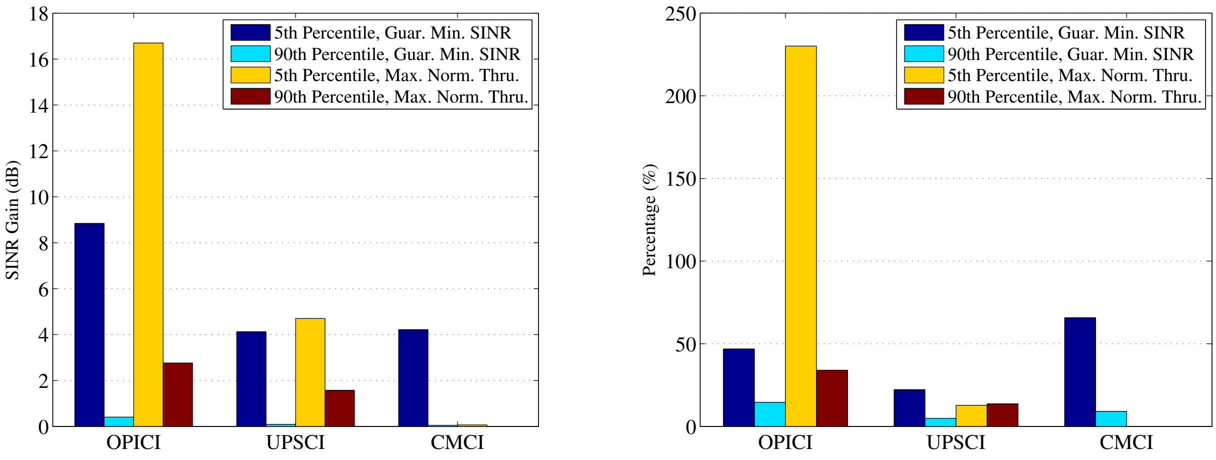
Under-Projecting Signal Channel Indicators (UPSCI). The adversary generates $\mathbf{g}$ by decreasing the magnitude of signal channel indicators according to $\mathcal{H} = \mathcal{D}(\mathbf{h})$. Thus, when the BS calculates the SINR for the selfish UE using $\mathbf{g}$, it will be similarly tricked into believing that an even great extent of cooperation is needed. For a given under-projection factor $\beta > 1$, the UPSCI strategy is given by

$$\boxed{\begin{array}{l} \textbf{Given: } \beta > 1 \text{ ; } \textbf{Choose: } g_i \text{ as} \\ g_i = \begin{cases} \beta h_i & \text{if } i\in\mathcal{H} \\ h_i & \text{if } i\in\mathcal{A}\setminus\mathcal{H}. \end{cases} \end{array}} \tag{9}$$

Controlling Minimum Channel Indicators (CMCI). The adversary generates $\mathbf{g}$ by increasing any signal or interference channel indicator that falls below a threshold C_{min}, a parameter that can be fine-tuned in such a way that the resulting SINR triggers extended cooperation. For a given threshold C_{min}, the CMCI strategy is given by

$$\boxed{\begin{array}{l} \textbf{Given: } C_{min} \text{ ; } \textbf{Choose: } g_i \text{ as} \\ g_i = \begin{cases} h_i & \text{if } |g_i| \geq C_{min} \\ C_{min} & \text{if } |g_i| < C_{min}. \end{cases} \end{array}} \tag{10}$$

[3] In typical cellular systems, the BS uses the expected received SINR to adaptively encode and modulate its packet so that the packet can be decoded and demodulated at a UE with low packet error rate ($< 10\%$). However, when the actual received SINR is smaller than the expected received SINR, the packet error probability becomes high.



(a) SINR Gain for Adversary

(b) Percentage of Additional Resources Used by Adversary

Figure 2: The three proposed strategies are evaluated under the Guaranteed Minimum SINR and Maximum Normalized throughput model in terms of (a) SINR gain and (b) Additional resource allocation.

4. SIMULATION RESULTS

In our simulation study, we implement seven BSs for a multicell cellular network and multiple UEs. The UEs are randomly distributed and form wireless channels to the seven BSs. The wireless channel model is composed of path loss model, large-scale fading model, and small-scale fading model. We employed the detailed simulation parameters from the IEEE evaluation methodology document [22]. Figure 2 shows the effectiveness of the three heuristic attack strategies over the two cooperation models, for 5th and 90th percentile users.

4.1 Results for 5th Percentile Users

When considering the guaranteed minimum SINR model for cell edge users, we can see that OPICI strategy gives adversary a gain of nearly 9 dB using about 50% of additional resources, which is far better as compared to CMCI and OPICI, both of which just have a gain of 4 dB using 65% and 25% of additional resources respectively. Now considering the maximum normalized throughput model for the cell edge users, we can see that the OPICI strategy gives adversary a huge gain of 17 dB as compared to UPSCI and CMCI strategy, which have a gain of about 6 dB and 0 dB respectively. Although, the resource usage is on a higher side for OPICI strategy in this model, which increases the risk of being detected by anomaly detection but still the enormous gain achieved would be worth the risk. Hence, for an adversary at the cell edge, OPICI clearly is a better attack strategy.

4.2 Results for 90th Percentile Users

The 90th percentile users are representative of users who already have a stronger signal from the BS, so there would be a lesser margin for SINR gain for an adversary as a 90th percentile user. Thus, considering the guaranteed minimum SINR model for 90th percentile users, we can see that the OPICI strategy gives the adversary a gain lying between 0.45 to 0.5 dB using about 15% of additional resources, which is far better as compared to UPSCI and CMCI which have a gain of 0.07 and 0.05 dB respectively. Again when we consider the maximum normalized throughput model, we can see that OPICI strategy gives the adversary a gain of 2.6 dB using just 33% additional resources, which is better as compared to UPSCI and CMCI which have a gain of 1.4 and 0 dB respectively. Hence, for an adversary with already high SINR, again OPICI turns out to be a better attack strategy.

4.3 Discussion of Results

We first discuss the comparison across heuristic attack strategies. From the figures given, we see that OPICI outperforms both UPSCI and CMCI in terms of the SINR gain that is achieved, under all cases. This is basically because most of the interference channel indicator values that are over projected by the adversary, while reporting the fabricated channel, become a part of the signal channel indicators after the new cooperation cluster is released. Therefore, OPICI turns out to be better than others.

We next discuss the comparison across cooperation decision models. From the figures given, we see that the guaranteed minimum SINR cooperation model is less vulnerable to the heuristic attacks, as compared to the maximum normalized throughput model. This is because the guaranteed minimum SINR cooperation model maintains a definitive system parameter, making it more difficult to manipulate.

5. SELFISH BEHAVIOR DETECTION

One possible deterrent to selfish behavior is through the use of a trusted platform module (TPM) in each UE to allow the BS to verify the UE's operation [15] by mechanisms like secure boot. Equipping each UE with a TPM allows system developers to build trusted software and guarantee the

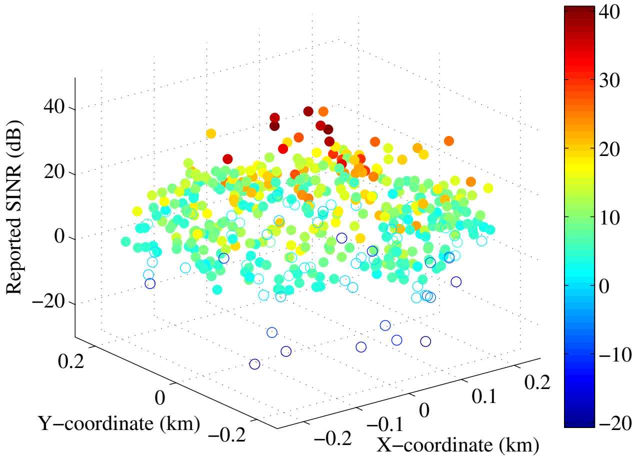


Figure 3: We illustrate the typical distribution of SINR values reported by benign and selfish users in a single cell. Filled dots represent reports from benign users, and hollow dots represent reports from selfish users using our proposed OPICI attack algorithm.

software is operating as intended. However, TPMs are not yet common in mobile phones, so an alternative approach is needed. After doing a detailed analysis of the impact of the proposed selfish misbehavior techniques, we have identified a potential detection strategy that BSs can either incorporate into the decision model $\mathcal{D}$ or use to evict users from the system.

5.1 Detection of Inconsistent SINR Reports

We propose the use of spatial consistency checking and a distance-dependent threshold to provide a course detection capability at each BS. If the network keeps track of a relatively accurate location for each UE, it can check to see whether UEs in similar locations or similar distances from the BSs are experiencing similar channel conditions. Any UE with vastly dissimilar SINR reports can be flagged as potentially misbehaving, and appropriate action can be taken. As the network may need to support a large number of UEs that may move relatively quickly, continual correlation analysis across UEs is likely an overly complex task. Instead, we propose to characterize the average behavior of UEs in the cell and compare each UE's SINR report against this model. Figure 3 illustrates the typical distribution of reported SINR values over the cell region for both benign and selfish behavior. We thus propose the use of a distance-dependent threshold $\tau(d)$ such that an SINR report less than $\tau(d)$ from a UE at a distance d from the BS will be flagged as inconsistent with the model.

We note that several factors should be included in the design of the threshold function $\tau(d)$. If the threshold is too high, UEs that are genuinely experiencing poor channel conditions may be flagged as selfish, yielding false positives, essentially defeating the purpose of cooperative communication. If the threshold is too low, selfish UEs will defeat the detection mechanism, yielding false negatives. In a practical scenario, it seems that systems employing cooperative communication may err on the side of setting the threshold on the low side, accepting a certain amount of selfish behavior in order to provide better service for UEs with unfavorable conditions.

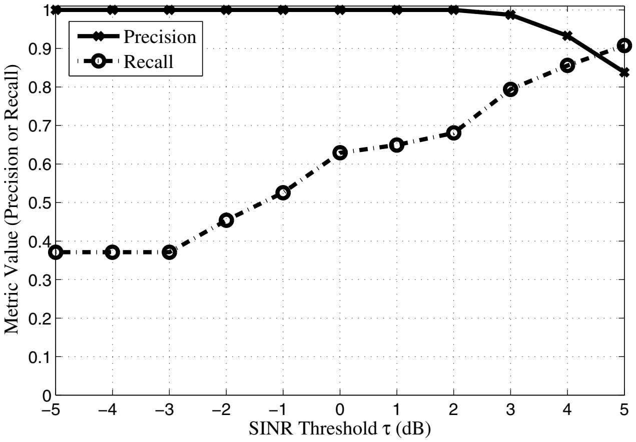


Figure 4: The precision and recall are evaluated as a function of the SINR threshold τ.

5.2 Evaluation of Threshold Detection

In order to evaluate the value of our proposed distance-dependent threshold detection mechanism, we simulate the threshold decision-making in the context of our earlier simulation study using parameters according to the IEEE EMD [22]. We randomly select 20% of the UEs as selfish users, fabricating channel vectors according to the OPICI attack algorithm described in Section 3.1. We consider the case that BSs employ the Maximum Normalized Throughput decision model, as described in Section 2.1. To measure the effectiveness of our detection mechanisms, we compute the resulting precision (fraction of detection results that are correct) and recall (fraction of misbehavior events that are detected) as a function of the constant threshold τ which is shown in Figure 4, noting that a distance-dependent threshold $\tau(d)$ will likely improve performance.

6. RELATED WORK

In recent years, there have been a number of studies on the security of cellular networks, especially focused on 3G networks [7,14,19]. Considering the up-link channel model, Sridharan et al. showed that malicious users can cause interference for normal users, by varying their own power transmission levels [21]. In contrast, the work by Racic et al. focused on down-link bandwidth in 3G networks, in order to exploit the vulnerabilities in scheduling algorithms such as proportional fairness (PF) to gain majority of the time slots in the 3G networks [18]. Bali et al. demonstrated the need for a robust scheduling algorithm by showing that TCP throughput can be reduced by as much as 25 to 30% by a single malicious user [3]. Unlike all the above discussed work which mostly operate on 3G networks, our work focuses on demonstrating selfish behavior by a user equipment in base station cooperation models [17]. Our SCF attack presented in Section 3 is built to attack base station cooperation. The core idea behind the attack is to take advantage of primary

BS's trust over UE. And through the attack, the selfish UE aims to obtain the maximum SINR gain.

7. CONCLUSIONS

In this paper, we identified a fundamental vulnerability of cellular networks using BS cooperations and backed our description with simulation results. As there exists no standardized models for base station to date, hence in our work we first propose two possible cooperation models that base station could potentially use and then further propose attack strategies over those cooperation models. We showed how the selfish UE, fabricated the channel information which degrades the cellular network's performance while benefiting the user's own quality of service. Our proposed heuristic attack strategies demonstrates that the gain for the adversary at cell-edge could go up to 40 times more than the actual received SINR. The results of our research also show that the guaranteed minimum SINR cooperation decision model is less vulnerable to the proposed attacks than the maximizing resource utilization cooperation decision model. Finally, we presented a threshold-based mechanism for BSs to detect SINR fabrication, thereby providing effective mitigation against the fabrication attacks.

8. REFERENCES

[1] 3GPP. TR 36814-900 Further advancements for E-UTRA - Physical Layer Aspects, 2010.

[2] D. Astély, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall. Lte: the evolution of mobile broadband. *Communications Magazine, IEEE*, 47(4):44–51, 2009.

[3] S. Bali, S. Machiraju, H. Zang, and V. Frost. A measurement study of scheduler-based attacks in 3G wireless networks. In *Proceedings of the 8th international conference on Passive and active network measurement*, PAM'07, pages 105–114, Berlin, Heidelberg, 2007. Springer-Verlag.

[4] R. Bernhardt. Macroscopic diversity in frequency reuse radio systems. *Selected Areas in Communications, IEEE Journal on*, 5(5):862–870, 1987.

[5] M. Boldi, C. Botella, F. Boccardi, V. D'Amico, E. Hardouin, M. Olsson, H. Pennanen, P. Rost, V. Savin, T. Svensson, and A. Tolli. Intermediate report on CoMP and relaying in the framework of CoMP, June 2011.

[6] C. Botella, L. Cottatellucci, V. D'Amico, M. Doll, R. Fritzsche, D. Gesbert, J. Giese, N. Gresset, H. Halbauer, E. Hardouin, H. Khanfir, M. L. Pablo, S. Saur, T. Svensson, and W. Zirwas. Definitions and architecture requirements for supporting interference avoidance techniques, August 2010.

[7] A. Bovosa. Attacks and counter measures in 2.5G and 3G cellular IP networks. In Juniper White Paper, 2004.

[8] M. Bublin, E. Hardouin, O. Hrdlicka, I. Kambourov, R. Legouable, M. Olsson, S. Plass, P. Skillermark, and P. Svac. Interference averaging concepts, June 2011.

[9] C. Carneheim, S. O. Jonsson, M. Ljungberg, M. Madfors, and J. Naslund. *FH-GSM Frequency Hopping GSM*, pages 1155–1159. 1994.

[10] W. Choi and J. G. Andrews. The capacity gain from intercell scheduling in multi-antenna systems. *IEEE Transactions on Wireless Communications*, 7(2):714–725, 2008.

[11] D. Cox. Cochannel interference considerations in frequency reuse small-coverage-area radio systems. *Communications, IEEE Transactions on*, 30(1):135–142, 1982.

[12] E. Dahlman, S. Parkvall, J. Skold, and P. Beming. *3G Evolution, Second Edition: HSPA and LTE for Mobile Broadband*. Academic Press, 2 edition, 2008.

[13] D. Gesbert, S. Hanly, H. Huang, S. S. Shitz, O. Simeone, and W. Yu. Multi-cell MIMO cooperative networks: a new look at interference. *IEEE J.Sel. A. Commun.*, 28(9):1380–1408, Dec. 2010.

[14] K. Kotapati, P. Liu, Y. Sun, and T. F. La Porta. A Taxonomy of Cyber Attacks on 3G Networks. Technical Report NAS-TR-0021-2005, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January 2005.

[15] J. M. McCune, Y. Li, N. Qu, Z. Zhou, A. Datta, V. Gligor, and A. Perrig. Trustvisor: Efficient TCB reduction and attestation. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 143–158, Washington, DC, USA, 2010. IEEE Computer Society.

[16] Y.-H. Nam, L. Liu, Y. Wang, J. C. Zhang, J. Cho, and J.-K. Han. Cooperative communication technologies for LTE-advanced. In *ICASSP*, pages 5610–5613. IEEE, 2010.

[17] A. Osseiran, J. Monserrat, and W. Mohr. *Mobile and Wireless Communications for IMT-Advanced and Beyond*. John Wiley & Sons, 2011.

[18] R. Racic, D. Ma, H. Chen, and X. Liu. Exploiting opportunistic scheduling in cellular data networks.

[19] F. Ricciato. Unwanted traffic in 3G networks. *SIGCOMM Comput. Commun. Rev.*, 36(2):53–56, Apr. 2006.

[20] C. E. Shannon. A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(1):3–55, Jan. 2001.

[21] A. Sridharan, R. Subbaraman, and R. Guerin. Uplink scheduling in the ev-do rev. a system: An initial investigation. In Sprint ATL Research Report Nr. RR06-ATL080139, 2006.

[22] R. Srinivasan, J. Zhuang, L. Jalloul, R. Novak, and J. Park. IEEE 802.16m evaluation methodology document (EMD), July 2008.

[23] S. Venkatesan, A. Lozano, and R. Valenzuela. Network mimo: Overcoming intercell interference in indoor wireless systems. In *Signals, Systems and Computers, 2007. ACSSC 2007. Conference Record of the Forty-First Asilomar Conference on*, pages 83–87. IEEE, 2007.