Distributed Opportunistic Scheduling In Cellular Data Networks-To Prevent The Malicious Attack

N.Kandavel[1] and Mrs.M.Lavanya [2]

[1] Student,M.E – Computer Science & Engineering, Arulmigu Meenakshi Amman College of Engineering, Kanchipuram-604 410,TamilNadu,India. Email: nkanda_vel@yahoo.com.
[2] Supervisor, Asst Prof.Dept of Computer Science & Engineering, Arulmigu Meenakshi Amman College of Engineering, Kanchipuram-604 410, TamilNadu, India.

***Abstract*—Third Generation (3G) cellular networks take advantage of time-varying and location-dependent channel conditions of mobile users to provide broadband services. Under fairness and QoS constraints, they use opportunistic scheduling to efficiently utilize the available spectrum. Opportunistic scheduling algorithms rely on the collaboration among all mobile users to achieve their design objectives. However, we demonstrate that rogue cellular devices can exploit vulnerabilities in popular opportunistic scheduling algorithms, such as Proportional Fair (PF) and Temporal Fair (TF), to usurp the majority of time slots in 3G networks. Our simulations show that under realistic conditions, only five rogue device per 50-user cell can capture up to 95 percent of the time slots, and can cause 2-second end-to-end inter packet transmission delay on VoIP applications for every user in the same cell, rendering VoIP applications useless. To defend against this attack, we propose strengthening the PF and TF schedulers and a robust handoff scheme**

Keywords -

1 INTRODUCTION

3Gcellular networks, such as High Speed Downlink Packet Access (HSDPA) [1] and Evolution-Data Optimized (EV-DO) [2], provide broadband-like downlink speed to enable applications, such as Voice-over-IP (VoIP).The specification for 3G cellular data services recommend implementing an opportunistic scheduler. An opportunistic scheduler uses multiuser diversity—the fading and shadowing of cellular users within a single cell—to optimize bandwidth efficiency. Both HSDPA and EV-DO use an opportunistic scheduler in the downlink to profit from multiuser diversity. To achieve this goal, many networks require mobile devices to participate in managing network services. However, since mobile devices are outside the control of the network administrators, networks should not trust them to manage network operations [3]. Unfortunately, this principle is often violated, as in the case of the popular opportunistic scheduling algorithms, Proportional Fair (PF) [1], [2], [4], [5], [6], [7] and Temporal Fair (TF) [8], [9].Apropos, we discovered two vulnerabilities:1. PF and TF schedulers trust channel condition reports from mobile devices without verification.2. Both schedulers guarantee fairness only within a single cell. A malicious mobile device can exploit the first vulnerability by reporting bogus channel conditions, and can exploit the second vulnerability by initiating unnecessary handoffs to circumvent the per-cell fairness guarantee. As a result, the attack can usurp a large number of time slots at the expense of the other in the same cell. Our simulation shows that only one attacker per 50-user cell can occupy up to 92 percent of available time slots persistently, depending on the scheduling algorithm used. To put it in another perspective, when users are running VoIP applications, one attacker per cell can perpetuate a 1-second end-to-end packet transmission delay for every other user, while five attackers per cell can perpetuate a 2-second delay. Since any delay longer than 0.4 second would disrupt VoIP [10], this attack would render VoIP useless. In addition to describing and analyzing the attack, we discuss two defense strategies. First, we propose to augment the PF and TF schedulers with priority queue and round robin to mitigate the attack. However, as the current PF and TF schedulers operate within a single cell, they cannot guarantee long-term fairness to mobile devices that can handoff freely across cells, resulting in the second vulnerability mentioned above. Therefore, we propose a robust handoff procedure that ensures graceful handoff for honest users while preventing attackers from usurping bandwidth. Our simulation shows that under this handoff procedure, the percent of time slots that attackers can obtain, no matter how many arbitrary handoffs they initiate, is close to what they can get in a single cell. This result demonstrates that our robust handoff procedure effectively prevents attackers from gaining advantage by initiating arbitrary handoffs. We make the following contributions:

We identify vulnerabilities in two popular opportunistic schedulers. We analyze a series of attacks mathematically as well as through simulations to demonstrate that they could devastate victim mobile users by causing persistent delays, lowering throughput, and disrupting certain applications.

We propose defense strategies against these attacks. Our simulation shows that our proposed robust handoff procedure effectively removes attackers 'advantage during their malicious handoffs.

2. 3GDATA NETWORKS

One of the principal objectives of designing mobile devices is to improve functionality while reducing network-wide component count, complexity, and cost [11]. In this process, however, 3G cellular networks grant unwarranted trust to mobile devices, allowing them to report arbitrary channel conditions and to initiate handoffs at their discretion. By exploiting these vulnerabilities, malicious mobile devices can disrupt other mobile users severely.

2.1 HSDPA

Cellular providers have developed two new data services, HSDPA and EV-DO, to meet the increasing demands for mobile technologies as alternatives to traditional wired communications. In both services, the downlink utilizes time division multiplexing (TDM) by dividing the channel in time slots, or Transmission Time Intervals (TTIs). The scheduler at each base station selects a single user to transmit at each TTI. Both services rely on two main techniques to increase efficiency in the downlink direction: link adaptation and fast retransmissions. Link adaptation is a data rate regulating mechanism in which mobile devices report to base stations their quasi-instantaneous downlink channel quality information, channel quality indicator (CQI). Base stations can then establish data rate contingent on channel conditions: the better the channel condition, the higher the data rate [12]. Fast retransmissions (part of the Hybrid Automatic Repeat Request (HARQ) manager) allow mobile devices to NACK each erroneous downlink packet (and request a retransmission) from its base station instead of the send server.

2.2 Opportunistic Scheduling

Channel conditions of cellular mobile devices are time varying and location-dependent due to fading and shadowing.This causes the multiuser diversity effect [13]: since many users fade independently, at any given time, some subset of users will likely have strong channel conditions. As we have already stated, better channel conditions imply higher data rates. On the one hand, a good scheduling scheme can recognize and exploit favorable channel conditions of certain users to achieve higher utilization of wireless resources. On the other hand, the potential to exploit favorable channel conditions of a subset of users introduces a trade-off problem between resource efficiency and fairness. A very popular opportunistic scheduler is PF[6], [7], whose goal is to maximize the product of the throughput delivered to all users [14], [15]. In fact, Kushner and Whiting [16] have shown that PF is not an adhoc algorithm, but actually corresponds to a maximization problem. Another interesting opportunistic scheduler is TF[8], whose goal is to maximize the average system performance, given the time fraction assignment. Both PFand TF attempt to strike a balance between throughput andfairness within a single cell [4], [8], [14], [15], [17], [18].Channel quality indicators. Since instantaneous channel conditions derive the instantaneous data rates of mobile devices [19], mobile devices constantly measure and report heir CQIs to their base stations. In particular at every TTI, an opportunistic scheduler at a base station selects a user(or a subset of users) with a relatively good channel condition to transmit while maintaining predefined QoS or fairness constraints. By scheduling the users with the best channel condition, opportunistic schedulers utilize shared channel efficiently and often achieve higher network performance than other schedulers, such as round-robin.In the current HSDPA specification, each mobile device periodically measures its instantaneous channel conditions through pilot signals,1 estimates the achievable data rate under its channel condition and sends the information back to the base station.The CQI value is calculated by an iterative algorithm that takes as input the downlink channel quality and a number of tunable parameters. The algorithm iterates with carying parameter combinations until the block error rate is lesst han 10 percent. Note that it is up to the mobile device load these reports to the base station at its own timing. According to the specification [20], [21], the CQI report cycle can happen every 1, 2, 4, 5, 10, 20, 40, or 80 TTIs.

2.2.1 Proportional Fair

PF is a compromise scheduling algorithm. It tries to strike a balance between achieving maximum network throughput nd ensuring fairness. In doing so, PF scheduler maximizes the product of throughputs delivered to all users [22]. PF selects a user i to schedule at time slot t based on the following criterion

$$i = \arg\max_{1 \le k \le N} \frac{DRC_k(t)}{R_k(t)} = \arg\max_{1 \le k \le N} \frac{min\{CQI_k[t], \frac{B_k[t]}{TTI}\}}{R_k(t)},$$

The base station estimates Ri(t)as follows:

$$R_i(t) = \begin{cases} \alpha CQI_i(t) + (1-\alpha)R_i(t-1), & \text{if } i \text{ is scheduled,} \\ (1-\alpha)R_i(t-1), & \text{otherwise,} \end{cases}$$

While current 3G standards do not specify a particular opportunistic scheduler, PF is the most popular both in there search community [23], [24], [25], [26], [27], [28], [29] and industry [1], [2], [4], [5], [6], [7], [30]. Networks may implement a modified PF. For instance, a PF scheduler may apply code multiplexing by scheduling multiple users with in the same TTI. Researchers have also proposed combining the PF scheduler with a priority queue or the round-robin scheduler. For the rest of the paper, however,wewill focus on the original PF, discussed in detail above.

2.2.2 Temporal Fair

TF algorithm provides another way of balancing system and individual user performance. Its goal is to maximize the average system performance by exploiting time-varying channel conditions, given the time fraction requirements of all users [8]. Let ri denote the pre determined minimum fPraction of time when the user i should transmit. ri>0.TF scheduler's goal is to maximize the average system performance under individual users' resource sharing requirement

Opportunistic scheduler gain. Opportunistic scheduling gain G(N)illustrates the performance gain of an opportunistic scheduling scheme over that of the non opportunistic one, namely, round-robin. Typically, the larger the number of users sharing the same channel, the larger the gain. For example, when users experience Rayleigh fading with statistically identical and independent relative channel conditions,

$$G(N)=\log(N)$$

2.3 Handoffs

Cellular networks utilize handoffs to transfer connections from one base station to another. A mobile device continuously monitors candidate base stations with stronger signal strength using pilot signals. The base station controller, upon receiving pilot measurement reports, determines if the mobile device will benefit from a handoff. If so, the base station controller initiates a handoff procedure by instructing the mobile device to hand off to another base station [5].2 There are two types of handoffs: soft and hard handoffs. In a hard handoff, the network drops the connection to the current base station before initiating anew one. In a soft handoff, a mobile device can have connections from several base stations simultaneously. Our attacks apply to soft as well as hard handoffs.

3 OVERVIEW OF ATTACKS

Opportunistic schedulers for 3G networks require mobile device to participate in network management functions.However, attackers can modify mobile devices to perform actions that are undesirable to the providers, even when providers attempt tamper-proof techniques [6], [31], [32],[33]. For instance, attackers can modify their laptops' 3G PC cards, either through the accompanying SDKs [34] or the device firmware [35]. By trusting all mobile devices for network management, a system that implements either PF or TF scheduler suffers from two vulnerabilities, discussed in the following.

3.1 Fabricated CQIs

Opportunistic schedulers base their scheduling decisions on CQIs reported by mobile devices without verification. By reporting fabricated CQIs, malicious mobile devices can manipulate he scheduler in their own favor. Let us consider a naı¨ve attack on PF and TF, respectively, with one attacker.In the PF variety of the attack, the malicious mobile device reports an inflated CQI such that its ratio of currently supported data rate to average data rate is the highest mong all the devices in its cell; therefore, ensuring that it will be scheduled in the next time slot. To obtain consecutive time slots, the attacker must report monotonically increasing CQIs (because its average throughput is increasing, while other users' throughput is decreasing, according to (2)) until reported CQI exceeds the range of CQI values. In the TF variety of the attack, a malicious mobile device starts with an inflated CQI. Then, it continues misrepresenting its channel conditions and reporting monotonically increasing CQIs This action causes the scheduler to keep decreasing the malicious device's offset as well as its allotted time share to satisfy the overall fairness.

4 ATTACK ANALYSES

4.1 Threat Model

Our threat model assumes the following:

1. Attackers control one or a few mobile devices that a cellular network has admitted and authenticated.
2. Attackers have modified their 3G mobile devices or PC cards such that they may report any CQI value to the base station and to trigger a handoff at any time.
3. Attackers can be physically located anywhere with in cells under attack. We believe that this threat model is realistic. Attackers can buy network-approved mobile devices (or PC cards with accompanying SDKs) and prepaid data plans directly from providers, or can spread worms to take over existing mobile devices. Prepaid data plans, in particular, minimize the risk of discovery and punishment. Previous research has demonstrated ways to modify mobile devices to perform different actions than intended by the providers, even when providers attempted tamper-proof techniques[31], [32], [33]. Note, however, that our threat model does not assume hacking into the network. Instead, our attackexploits vulnerabilities in the network's scheduler by manipulating the information that malicious mobile devices report to the network.In the following sections, we describe the PF variety of attacks in

detail. First, we describe a naı¨ve attack, the intracell attack. Then, using this attack as a waypoint, we describe a more sophisticated and powerful attack, the intercell attack. Finally, to evaluate the intercell attack in amore realistic environment, we relax the requirement fort he attackers to know the victim users' channel conditions.For TF scheduler, we can design a similar attack strategy,which we will describe at the end of this section.

4.2 Proportional Fair Attacks

4.2.1 Intracell Attacks

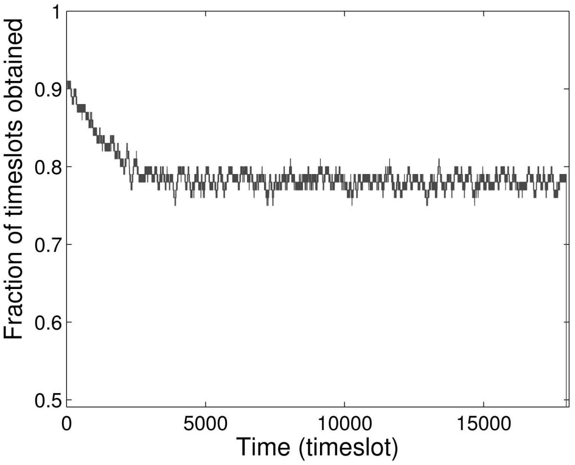
Consider a scenario where all attackers stay in the same cell.We assume that no user leaves or joins the cell during the attack. Although this assumption is not crucial to our attack,it simplifies our analysis. Additionally, for simplicity, we assume that the attackers know the channel conditions of all the users in the cell. Section 4.2.3 will describe an attack strategy which eliminates this assumption.As we have stated in the previous section, a single attacker can obtain consecutive time slots until his reported CQI exceeds the maximum CQI value. Naturally, attackers can increase the number of consecutive time slots obtained by using multiple colluding attackers. We discuss three possible ways for the attackers to collude

4.2.2 Intercell Attacks

The PF scheduler ensures long-term fairness within a cell. By transgressing cell boundaries, attackers can gain unfair share of network bandwidth. Our single-cell simulations show that an attacker's reported CQI and average throughput increase very fast during an attack. When a large average throughput the attacker to report a CQI larger than the maximum value, the attack stalls. However,when a user joins a cell, the scheduler assigns a typically small value as the user's initial average throughput, since the network does not transfer users' average throughput across cells during handoff [29]. Therefore, when an attacker cannot acquire more slots because its average throughput is too high, it can induce a handoff to receive a smaller initial average throughput in the new cell. For example, consider two attackers MA and MB sitting in the overlapping area of cells CA and CB. Initially, MA attacks CA, and MB attacks CB. When one of the attackers fails to acquire consecutive slots, MA hands off to CB and MB hands off to CA to continue their attacks. Alternatively, consider a targeted cell attack. In this case, the attacker can use handoff as a bridge to reset its attack. In particular, he or she attacks the target cell as long as possible, handoffs to a neighboring cell and back immediately. This way, it resets the average throughput value and can continue the attack.Since the choice of this initial value is unspecified, wee explore three reasonable schemes that, although not all inclusive, illustrate behavior of the PF scheduler. Average of average throughputs. A simple scheme is to choose the average of average throughputs of all existing users in this cell as the initial average throughput of the new user.Minimum of average throughputs. Since new users often join a cell from the edge of the cell, they are expected to have the poorest channel condition. Therefore, this scheme chooses the minimum of average throughputs of all existing users as the initial average throughput of the new user. Determined by the user. Finally, since users perform tasks such as measuring channel quality and pilot for multiple cells, an intuitive scheme is to let users report average throughput.

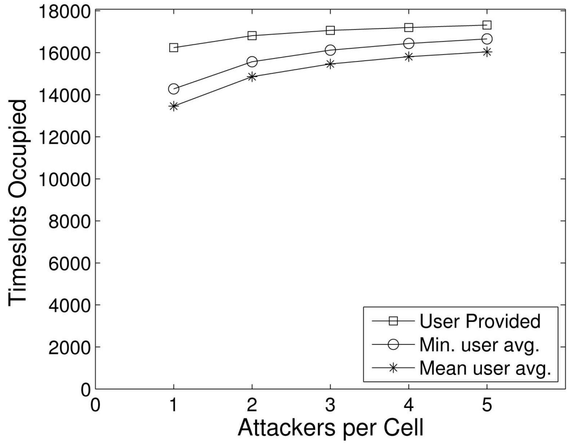
Attack results:

Fig. 1a shows the fraction of time slots that the attackers acquired where there was one attacker per cell of 50 users and the attackers determined their initial throughput. It shows that after about 2,000 timeslots, the attackers consistently obtained about 78 percent of all the slots, a condition that we call the stabilization of the attack. In simulating different number of attackers per



(a)

Fig. 1b shows the total number of time slots that the attackers obtained in 36 seconds. Unsurprisingly, the more attackers per cell, the more time slots they can obtained. However, even with just one attacker per cell, the attackers obtained from 13,459 (74 percent) to 16,241 (90 percent) timeslots, depending on the scheme by which the scheduler assigns the initial average throughput. Among the three schemes, the scheme that let the user provide this initial value is the most vulnerable, where one attacker obtained16,241 (90 percent) time slots, while five attackers obtained17,317 (96 percent) time slots.



(b)

5 DEFENSE STRATEGIES

To defend against attacks on opportunistic schedulers, we irst evaluate a set of variations of the PF and TF scheduler. Then, we propose a new handoff scheme that can effectively prevent the attacks.

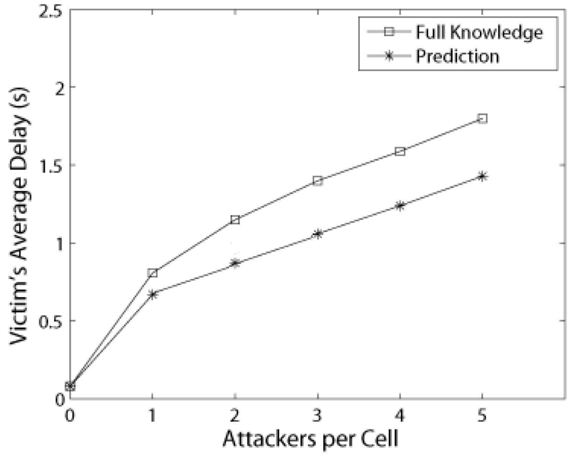
5.1 Scheduler Modifications

We have discussed the pure PF and TF schedulers so far.T here are, however, variations of the PF (TF) scheduler, known as hybrid PF (TF) schedulers. These hybrid PF (TF)schedulers were proposed for Quality of Service (QoS).

Here, we examine how resilient they are against the attacks discussed in previous sections.

5.1.1 Priority Queue

The base station can use priority queues to alleviate the impact of attacks outlined in the previous section. In particular, the base station can schedule traffic with delay constraints, such as VoIP traffic, with high priority while scheduling other traffic, such as Web browsing, with low priority. For instance, the scheduler can update a priority scheduling candidate set with devices that have VoIP packets buffered at the base station, that have pending retransmissions in their HARQ manager, or whose head-oflinepacket delay is greater than some value [40]. Becauset he number of high-priority users is relatively small, these users have much better delay performance. Thus, the effect of the attack will be mitigated. The actual impact of priority queue depends on the extent of system manipulation by the attacker. For instance, an attacker may opt out of the lower his average throughput value. He can achieve this by keeping his buffer at the base station empty or by reporting extremely low CQI values. During the attack, the attacker can opt into the priority set through one of the following methods :masquerading as a high-priority user (such as a VoIP user)triggering fast transmissions, and under flowing the buffer at the base station (if the queue length is considered in scheduling decisions).



7 CONCLUSION

We have shown that cellular data networks are vulnerable to DoS attacks by malicious mobile devices because of the following vulnerabilities:

. The network trusts mobile devices to report CQIs, which the PF and TF schedulers use without verification for assigning time slots. However, malicious mobile devices can manipulate their reported CQIs to gain a large number of time slots.

. The network does not track the average throughput of mobile devices across different cells. Therefore, malicious devices can maintain perpetual scheduling priority by frequent handoffs.

Our simulations show that just one attacker per cell can decrease the throughput and increase the delay of victim users significantly enough to disrupt time-sensitive data services, such as VoIP. Moreover, multiple attackers can collaborate to aggravate the attack. To defend against the attacks, we discuss modifications to the PF and TF schedulers, and propose a robust handoff procedure. Simulations show that our robust handoff procedure effectively enforces long-term fairness and prevents the attacks.

REFERENCES

[1] H. Holma and A. Toskala, HSDPA/HSUPA for UMTS. John Wiley& Sons, 2006.

[2] V. Vanghi, A. Damnjanovic, and B. Vojcic, The CDMA2000 Systemfor Mobile Communications. Prentice Hall, 2004.

[3] 3GPP, "3G Wlan—Trust Model," http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_25_Munich/Docs/PDF/S3-020523.pdf, 2008.

[4] Ericsson, "WCDMA Evolved—The First Step—HSDPA," http://www.ericsson.com/technology/whitepapers/wcdma_evolved.pdf, 2008.

[5] Qualcomm, “HSDPA for Improved Downlink Data Transfer,”Oct. 2004.

[6] S. Bali, S. Machiraju, H. Zang, and V. Frost, “On the Performance Implications of Proportional Fairness (PF) in 3G Wireless Networks,”Proc.PassiveandActive easurements Conf., 2007.

[7] S.Z. Asif, “Aligning Business and Technology Strategies—An Evolution of a Third Generation Wireless Technology,” Proc. Eng.Management Conf., 2002.

[8] X. Liu, E.K.P. Chong, and N.B. Shroff, “Opportunistic Transmission Scheduling with Resource-Sharing Constraints in Wireless Networks,” IEEE J. Selected Area in Comm., vol. 19, no. 10, pp. 2053-2064, Oct. 2001.

[9] S.S. Kulkarni and C. Rosenberg, “Opportunistic SchedulingPolicies for Wireless Systems with Short Term Fairness Constraints,”Proc. IEEE Global Telecomm. Conf. (Globecom), 2003.

[10] ITU-T, “One-Way Transmission Time,” ITU-T RecommendationG.114, 1996.

[11] G. Varrall and R. Belcher, 3G Handset and Network Design. Wileyand Sons, 2004.

[12] HSDPA Mobile Broadband Data, Agere Systems, 2005.

[13] M. Grosslauser and D. Tse, “Mobility Increases the Capacity ofWireless Ad Hoc Networks,” Proc. IEEE INFOCOM, Apr. 2001.

[14] A. Jalali, R. Padovani, and R. Pankaj, “Data Throughput ofCDMA-HDR a High Efficiency-High Data Rate Personal CommunicationWireless System,” Proc. IEEE Vehicular TechnologyConf., vol. 3, 2000.

[15] E.F. Chaponniere, P. Black, J.M. Holtzman, and D. Tse, TransmitterDirected Multiple Receiver System Using Path Diversity to EquitablyMaximize Throughput, US Patent No. 6449490, 2002.