may effectively use power for better channels. However, such a scheme experiences a time delay when the channel gain is low, which is not appropriate for real-time (constant rate) transmission. We also note that when $S_{\max}/S_{\mathrm{T}} = 3$ dB, the combined scheme does not satisfy the average power constraint (24), indicating that the combined MRT and truncated channel inversion cannot be employed for transmitters with very low peak-power limit.

In 3G wireless systems [1], the TAD is mostly adopted at the base station (BS), because it is cost effective and practical to employ multiple transmit antennas at the BS rather than at the mobile station (MS). The power amplifier employed at the BS can have a relatively higher peak-to-average power ratio than that at the MS. Therefore, the TAD in the downlink cannot be affected by the peak transmit power limit on the most practical range of system parameters. However, the implementation of multiple antennas at the MS is in considerable demand for high-performance next-generation wireless communications [23], [24]. The transmission parameters of an uplink TAD require careful design consideration due to substantial limitation of the peak-to-average power ratio at the MS.

REFERENCES

[1] R. T. Derryberry, S. D. Gray, D. M. Ionescu, G. Mandyam, and B. Raghothaman, "Transmit diversity in 3G CDMA systems," *IEEE Commun. Mag.*, vol. 40, no. 4, pp. 68–75, Apr. 2002.

[2] T. Lo, "Maximum ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.

[3] J. K. Cavers, "Single-user and multiuser adaptive maximal ratio transmission for Rayleigh channels," *IEEE Trans. Veh. Technol.*, vol. 49, no. 6, pp. 2043–2050, Nov. 2000.

[4] J. Choi, "Performance analysis for transmit antenna diversity with/without channel information," *IEEE Trans. Veh. Technol.*, vol. 51, no. 1, pp. 101–113, Jan. 2002.

[5] A. F. Naguib, A. Paulraj, and T. Kailath, "Capacity improvement with base station antenna arrays in cellular CDMA," *IEEE Trans. Veh. Technol.*, vol. 43, no. 3, pp. 691–698, Aug. 1994.

[6] F. Rashid-Farrokhi, L. Tassiulas, and K. Liu, "Joint optimal power control and beamforming in wireless networks using antenna arrays," *IEEE Trans. Commun.*, vol. 46, no. 10, pp. 1313–1324, Oct. 1998.

[7] F. Rashid-Farrokhi, K. Liu, and L. Tassiulas, "Transmit beamforming and power control for cellular wireless systems," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1437–1450, Oct. 1998.

[8] M. Schubert and H. Boche, "An efficient algorithm for optimum joint downlink beamforming and power control," in *Proc. IEEE VTC—Spring*, May 2002, pp. 1911–1915.

[9] M. Schubert, D. Karadoulamas, H. Boche, and G. Lehmann, "Joint downlink beamforming and power control for 3G CDMA," in *Proc. IEEE VTC—Spring*, Apr. 2003, pp. 331–335.

[10] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, Nov. 1997.

[11] A. J. Goldsmith and S. G. Chua, "Variable-rate variable-power MQAM for fading channels," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1218–1230, Oct. 1997.

[12] R. Knopp and G. Caire, "Power control and beamforming for systems with multiple transmit and receive antennas," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 638–648, Oct. 2002.

[13] S. T. Chung and A. J. Goldsmith, "Degrees of freedom in adaptive modulation: A unified view," *IEEE Trans. Commun.*, vol. 49, no. 9, pp. 1561–1571, Sep. 2001.

[14] E. N. Onggosanusi, A. Gatherer, A. Dabak, and S. Hosur, "Performance analysis of closed-loop transmit diversity in the presence of feedback delay," *IEEE Trans. Commun.*, vol. 49, no. 9, pp. 1618–1630, Sep. 2001.

[15] M. Schwartz, W. R. Bennett, and S. Stein, *Communication Systems and Techniques*. New York: McGraw-Hill, 1966.

[16] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.

[17] G. S. G. Beveridge and R. S. Schechter, *Optimization: Theory and Practice*. New York: McGraw-Hill, 1970.

[18] Y. H. Lee, "Power and rate adaptation in CDMA communications," Ph.D. dissertation, Inf. Transmiss. Lab, Korea Adv. Inst. Sci. Technol. (KAIST), Daejeon, Korea, Feb. 2000.

[19] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the Lambert W function," *Adv. Comput. Math.*, vol. 5, no. 4, pp. 329–359, 1996.

[20] A. Heck, *Introduction to Maple*. New York: Springer-Verlag, 1993.

[21] D. A. Barry, P. J. Cullingan-Hensley, and S. J. Barry, "Real values of the W-function," *ACM Trans. Math. Softw.*, vol. 21, no. 2, pp. 161–171, 1995.

[22] D. A. Barry, J.-Y. Parlange, L. Li, H. Prommer, C. J. Cunningham, and F. Stagnitti, "Analytical approximations for real values of the Lambert W-function," *Math. Comput. Simul.*, vol. 53, no. 1/2, pp. 95–103, Aug. 2000.

[23] Y. Kim *et al.*, "Beyond 3G: Vision, requirements, and enabling technologies," *IEEE Commun. Mag.*, vol. 41, no. 3, pp. 120–124, Mar. 2003.

[24] H. Sampath, S. Talwar, J. Tellado, V. Erceg, and A. Paulraj, "A fourth-generation MIMO-OFDM broadband wireless system: Design, performance, and field trial results," *IEEE Commun. Mag.*, vol. 40, no. 9, pp. 143–149, Sep. 2002.

Eavesdropping Through Mobile Phone

Yi-Bing Lin, *Fellow, IEEE*, and
Meng-Hsun Tsai, *Student Member, IEEE*

***Abstract*—Mobile telecommunication services have become very popular recently, and many people bring mobile phones with them wherever they go. However, we observe that mobile phones can be modified to become remote microphones for eavesdropping. The eavesdropping technique only requires modifications to the mobile phone to be spied on and does not require any network changes. This paper describes mobile-phone eavesdropping and analyzes how serious it can be. Based on our study, we provide suggestions to avoid being eavesdropped upon.**

***Index Terms*—Eavesdropping, session initiation protocol (SIP), signaling system number 7 (SS7), voice over IP (VoIP).**

I. INTRODUCTION

Mary was curious about John's everyday life. She decided to eavesdrop on John through his mobile phone. She purchased a pair of "spy" mobile phones: a spying phone and a spied-on phone. She gave the spied-on phone to John as a birthday gift. When she wanted to eavesdrop on John, she used the spying phone to dial the number of the spied-on phone. Thus, the spied-on phone of John became a remote microphone through which Mary could hear all sounds around John when he was not using the spied-on phone for conversation. Based on the technique, we will describe later that John (the victim) is typically

Manuscript received April 17, 2006; revised July 10, 2006, November 3, 2006, and February 20, 2007. The work of Y.-B. Lin was supported in part by NSC Excellence Project Grants NSC 95-2752-E-009-005-PAE, NSC 95-2218-E-009-201-MY3, NSC 94-2219-E-009-001, and NSC 94-2219-E-009-024, by the NTP SIP-based B3G Project under Grant NSC 95-2219-E-009-010, by the NTP IMS Integration Project under Grant NSC 95-2219-E-009-019, by Intel, by Chung Hwa Telecom, by IIS/Academia Sinica, by the ITRI/NCTU Joint Research Center, and by MoE ATU. The work of M.-H. Tsai was supported by a Microsoft Fellowship and by a ZyXEL Fellowship. The review of this paper was coordinated by Dr. Q. Zhang.

Y.-B. Lin is with the Department of Computer Science, National Chiao Tung University, Hsinchu 300, Taiwan, R.O.C., and also with the Institute of Information Science, Academia Sinica, Nankang, Taipei 115, Taiwan, R.O.C. (e-mail: liny@csie.nctu.edu.tw).

M.-H. Tsai is with the Department of Computer Science, National Chiao Tung University, Hsinchu 300, Taiwan, R.O.C. (e-mail: tsaimh@csie.nctu.edu.tw).

Digital Object Identifier 10.1109/TVT.2007.901060

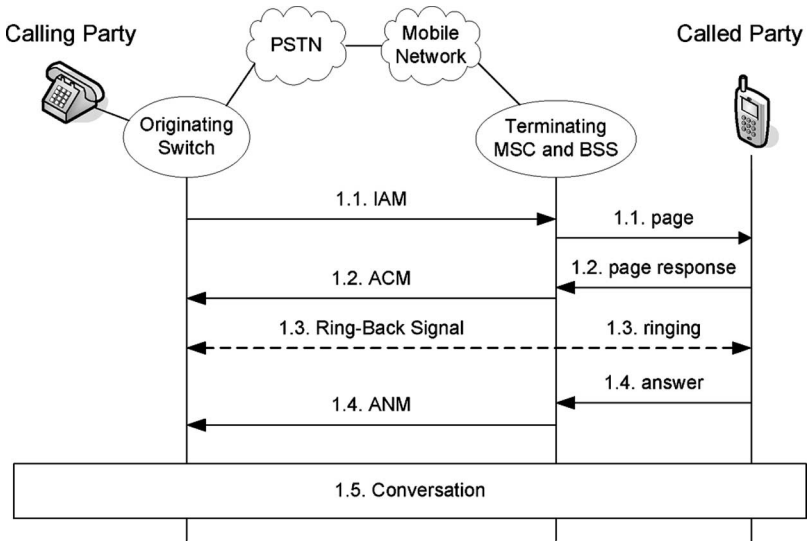

Fig. 1. Mobile call termination message flow.

not spied on (overheard) when he is using the spied-on phone for conversation.

Mobile telecommunication services have become very popular recently, and many people bring mobile phones with them wherever they go. However, we observe that mobile phones can be modified to become remote microphones for eavesdropping as we just showed in the aforementioned scenario. This paper describes mobile-phone eavesdropping [1] and analyzes how serious it can be.

II. Mobile-Phone Eavesdropping

Fig. 1 shows the simplified setup for mobile call termination [2] with the following steps.

1.1) The calling party dials the phone number of the called party. The signaling system number 7 (SS7) **Initial Address Message** (**IAM**) is sent from the originating switch to the terminating mobile switching center (MSC) of the called party. The terminating base station system (BSS) pages the called party.

1.2) If the called party is in the radio's coverage, it sends the page response signal to the terminating BSS. The terminating MSC then returns the SS7 **Address Complete Message** (**ACM**) to the originating switch.

1.3) If the spied-on phone is not busy, a ringing signal is sent to the called party, and a ringback signal is sent to the calling party. Both the calling and called phones are ringing.

1.4) When the called party picks up the handset, an answer signal is sent to the terminating MSC. The terminating MSC sends the SS7 **Answer Message** (**ANM**) to the originating switch. The ringing and the ringback tones are removed, and the conversation starts.

To eavesdrop through a mobile phone, the software of the spied-on phone is modified to accommodate the eavesdropping procedure shown in Fig. 2.

2.1) The eavesdropper dials the phone number of the spied-on phone. The **IAM** message is sent from the originating switch to the terminating MSC of the spied-on phone. The terminating BSS pages the called party.

2.2) If the called party is in the radio's coverage, it sends the page response signal to the terminating BSS. The terminating MSC returns the **ACM** message to the originating switch.

2.3) If the spied-on phone is not busy, a ringing signal is sent to the spied-on phone, and a ringback signal is sent to the spying phone.

2.4) The spied-on phone obtains the caller ID from the ringing signal. It checks if the caller ID is the phone number of the spying phone. If not, the normal call setup procedure is performed [step 1.4) in Fig. 1]. If the caller ID matches, the spied-on phone disables the ringing tone and turns off the speaker such that the victim is not alerted.

2.5) Without having the victim to pick up the handset, the spied-on phone automatically turns on the transmitter (microphone) and sends an answer signal to the terminating MSC. The terminating MSC considers that the called party (the victim) has picked up the phone, and it sends the **ANM** message to the originating switch. The ringing tone is removed.

2.6) At this point, the call is connected, and the eavesdropper can hear all sounds from the spied-on phone. Since the speaker of the spied-on phone is disabled, any noise generated by the eavesdropper will not be detected by the victim.

In this scenario, the originating switch and the terminating MSC exercise the standard SS7 call setup procedure [i.e., steps 2.1), 2.2), 2.3), and 2.5) are exactly the same as steps 1.1), 1.2), 1.3), and 1.4)] and do not detect the eavesdropping activity. If the calling party is not the eavesdropper, the call is set up as a normal call [as described in step 1.4)]. Therefore, the victim can receive calls from other normal calling parties. When an incoming call arrives during an eavesdropping session, the eavesdropping session is immediately terminated, and the newly arrived call is connected. Therefore, the victim will not lose any normal calls.

Note that the victim will detect abnormal call records if the billing method is called-party-pay (e.g., if the spied-on phone is a cellular phone in the U.S.). If the billing method is calling-party-pay (e.g., if the spied-on phone is a fixed-line phone or if the spied-on phone is a cellular phone in Taiwan, R.O.C.), the eavesdropped calls will not be shown up on the telephone bill. Based on the aforementioned discussion, the eavesdropping scenario works as follows.

1) The eavesdropper purchases the spied-on mobile phone. The phone is initially set up with the eavesdropper's phone number as the caller ID that will trigger the eavesdropping procedure shown in Fig. 2.

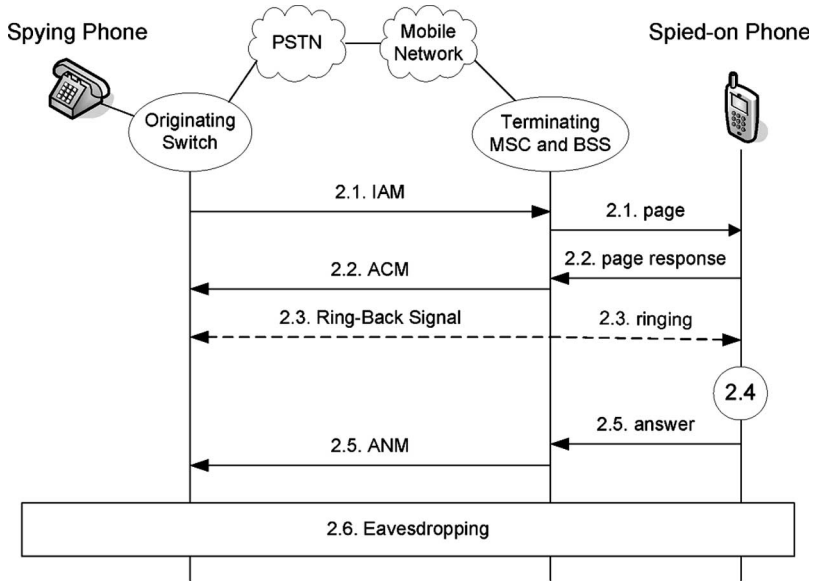

Fig. 2. Mobile-phone eavesdropping.

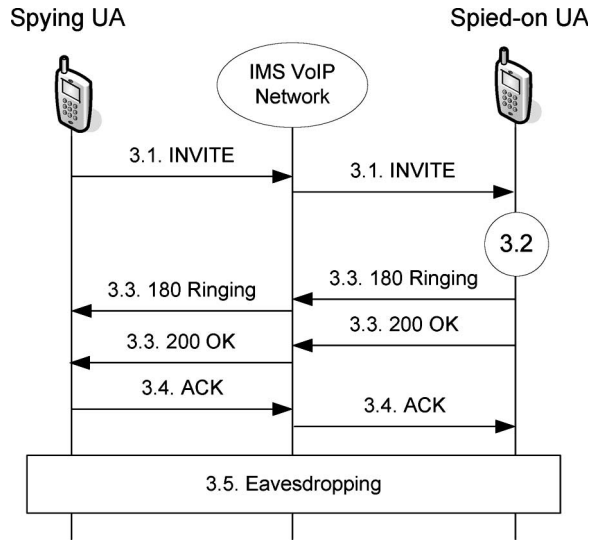

Fig. 3. VoIP eavesdropping.

2) The eavesdropper gives this mobile phone to the victim (e.g., as a birthday gift). In the countries exercising called-party-pay, the eavesdropper should also cover the billing of this spied-on phone so that the telephone bill will not go to the victim.

III. Voice Over IP (VoIP) Eavesdropping

In advanced mobile networks (3G or 4G systems), voice services may be provided through packet-switched domain, i.e., through VoIP [1]. In mobile all-IP network, such as IP Multimedia Core Network Subsystem (IMS), VoIP is provisioned through session initiation protocol (SIP). Fig. 3 shows the call flow for the SIP-based VoIP call eavesdropping, and the steps are described as follows.

3.1) The SIP **INVITE** message is sent from the spying user agent (UA) to the spied-on UA. The spying UA and the spied-on UA may be directly or indirectly connected through the IMS VoIP network.

3.2) From the caller ID, the spied-on UA detects the eavesdropping event.

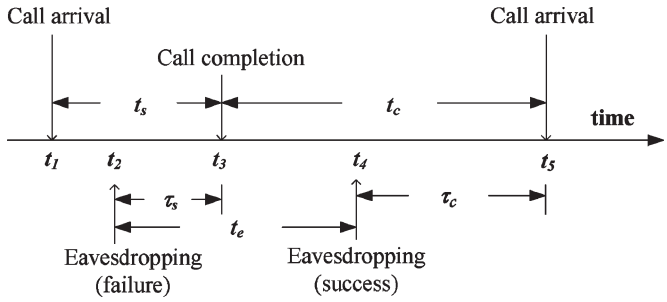

Fig. 4. Timing diagram for eavesdropping behavior.

3.3) Without alerting the victim, the spied-on UA automatically disables the ringing tone, turns off the speaker, turns on the transmitter (microphone), and returns the SIP **180 Ringing** and the SIP **200 OK** messages to the spying UA.

3.4) The spying UA sends the SIP **ACK** message to the spied-on UA, and the connection is then established for eavesdropping.

Like circuit-switched mobile-phone eavesdropping, the VoIP signaling messages that are exchanged between the spying and the spied-on UAs follow the standard SIP call setup procedure, and intermediate nodes (of the IMS VoIP network) in the call path do not detect the eavesdropping activity.

IV. Analysis of Eavesdropping Behavior

This section proposes an analytic model to investigate eavesdropping behavior. We first derive the probability of successful eavesdropping in Section IV-A and then derive the expected potential eavesdropping period in Section IV-B.

A. Probability of Successful Eavesdropping

Fig. 4 shows the timing diagram for the normal telephone usage and eavesdropping activities. Let $t_s = t_3 - t_1$ be the call holding time and $t_c = t_5 - t_3$ be the interval between the call completion and the next call arrival. It is clear that t_c is the period that can be spied on. Suppose that the eavesdropper attempts to eavesdrop at times t_2 and t_4, respectively. Since the spied-on phone is busy at t_2 and idle at t_4, the

attempt at t_2 fails, and the attempt at t_4 succeeds. The call activities of the spied-on phone can be modeled by an alternating renewal process where the sequence of random variables t_s and t_c is independently and identically distributed. Let α be the probability of successful eavesdropping. Since the eavesdropping attempt is a random observer, from [3, Th. 3.4.4], we have

$$\alpha = \frac{E[t_c]}{E[t_s] + E[t_c]}.$$

Probability α is affected only by the expected length of t_s and t_c.

When an eavesdropping attempt fails, the eavesdropper may retry after some random time t_e. Let β be the probability of successful next eavesdropping; then

$$\beta = \Pr[t_e > \tau_s]$$

where τ_s is the excess life of t_s. Consider the call holding time random variable t_s with the mean $1/\mu$, the density function $f(\cdot)$, and the Laplace transform $f^*(s)$. The excess life τ_s has the distribution function $R(\cdot)$, the density function $r(\cdot)$, and the Laplace transform $r^*(s)$. Since the eavesdropping attempt is a random observer, from the excess life theorem [4], we have

$$r^*(s) = \left(\frac{\mu}{s}\right)[1 - f^*(s)]. \tag{1}$$

Suppose that t_e has an exponential distribution with mean $1/\gamma$. Based on (1), we derive β as

$$\begin{aligned}\beta &= \Pr[t_e > \tau_e] \\ &= \int_{t_e=0}^{\infty}\int_{\tau_s=0}^{t_e} r(\tau_s)\gamma e^{-\gamma t_e} d\tau_s dt_e \\ &= \left.\frac{\gamma r^*(s)}{s}\right|_{s=\gamma} \\ &= \left(\frac{\mu}{\gamma}\right)[1 - f^*(\gamma)]. \end{aligned} \tag{2}$$

Assume that t_s has a Gamma distribution with the mean $1/\mu$, the variance V_s, and the Laplace transform

$$f^*(s) = \left(\frac{1}{V_s\mu s + 1}\right)^{\frac{1}{V_s\mu^2}}.$$

Then, (2) is rewritten as

$$\beta = \left(\frac{\mu}{\gamma}\right)\left[1 - \left(\frac{1}{V_s\mu\gamma + 1}\right)^{\frac{1}{V_s\mu^2}}\right].$$

The Gamma distribution is selected because it has been shown that the distribution of any positive random variable can be approximated by a mixture of Gamma distributions (see [5, Lemma 3.9]). Following the past experience [6]–[8], we can measure the call holding times from the field and then generate the Gamma distribution from the measured data. Fig. 5 plots β for the Gamma call holding time with different variance values. The figure indicates that β decreases as V_s increases. This phenomenon is explained as follows. When the call holding times become more irregular, more longer and shorter call holding times are observed. Since the failed eavesdropping attempts more likely fall on longer call holding times, more longer τ_s periods are observed (this is called the inspection paradox). These longer τ_s periods make it more difficult to retry. Therefore, the next eavesdropping attempt more likely fails when the call holding times become more irregular.

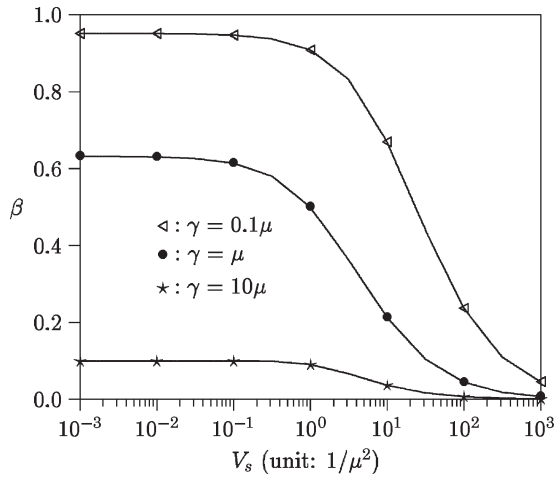

Fig. 5. Effects of the variance of the call holding time on β.

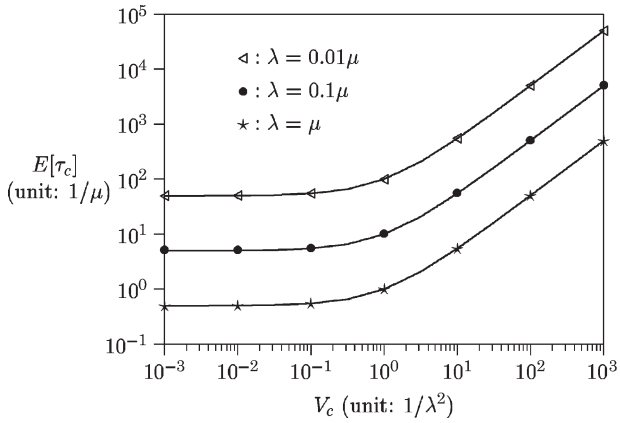

Fig. 6. Effects of the variance of t_c on $E[\tau_c]$.

B. Expected Potential Eavesdropping Period

The potential eavesdropping period $\tau_c = t_5 - t_4$ in Fig. 4 is the excess life of t_c. Since the eavesdropping attempt is a random observer, the expected potential eavesdropping period $E[\tau_c]$ can be expressed as [4]

$$E[\tau_c] = \frac{E[t_c^2]}{2E[t_c]}. \tag{3}$$

Suppose that t_c has an arbitrary distribution with the mean $1/\lambda$ and the variance V_c. Since $E[t_c] = 1/\lambda$ and $V_c = E[t_c^2] - E[t_c]^2$, (3) is rewritten as

$$E[\tau_c] = \frac{1}{2\lambda} + \frac{\lambda V_c}{2}.$$

The $E[\tau_c]$ curves are shown in Fig. 6. The figure indicates that $E[\tau_c]$ is an increasing function of V_c. As V_c increases, more longer and shorter t_c periods are observed. Since the successful eavesdropping attempts more likely fall on longer t_c periods, more longer τ_c periods

are observed. Therefore, the expected potential eavesdropping period increases as V_c increases.

V. Conclusion

Mobile telecommunication services have become very popular recently. We observe that mobile phones can be modified to become remote microphones for eavesdropping.

For the eavesdropping techniques described in this paper, only the spied-on phone is modified. The network is left unchanged. On the Internet, the SIP UA is usually implemented as a computer program, which can be easily distributed through free software download. On the other hand, all cellular/public switched telephone network (PSTN) phones for eavesdropping are "hard phones" with a built-in software that cannot be easily obtained through, for example, free software download. Therefore, installing spied-on cellular/PSTN phones is not as easy as installing VoIP "spyware."

Since people bring mobile phones with them, the eavesdropping events can be triggered any place the victim goes. Therefore, the eavesdropping targets a specific person. On the other hand, the PSTN/VoIP phones are fixed at their locations, and eavesdropping targets the surrounding areas where the "fixed" spied-on phones are located.

To avoid eavesdropping, it is always safer for the cellular/PSTN users to purchase their own handsets and investigate/pay their own telephone bills. A VoIP user should read the license carefully before downloading the VoIP software and turn off the microphone after each phone conversation (and also ensures that the camera and the microphone programs of the computer are not illegally turned on remotely).

References

[1] Y.-B. Lin and A.-C. Pang, *Wireless and Mobile All-IP Networks*. Hoboken, NJ: Wiley, 2005.

[2] Y.-B. Lin and I. Chlamtac, *Wireless and Mobile Network Architectures*. Hoboken, NJ: Wiley, 2001.

[3] S. M. Ross, *Stochastic Processes*, 2nd ed. New York: Wiley, 1996.

[4] Y.-B. Lin, "Performance modeling for mobile telephone networks," *IEEE Netw.*, vol. 11, no. 6, pp. 63–68, Nov./Dec. 1997.

[5] F. P. Kelly, *Reversibility and Stochastic Networks*. Hoboken, NJ: Wiley, 1979.

[6] FarEasTone Telecom, private communication, 2003.

[7] I. Chlamtac, Y. Fang, and H. Zeng, "Call blocking analysis for PCS networks under general cell residence time," in *Proc. IEEE WCNC*, New Orleans, LA, Sep. 1999, pp. 550–554.

[8] H. Zeng and I. Chlamtac, "Handoff traffic distribution in cellular networks," in *Proc. IEEE WCNC*, New Orleans, LA, Sep. 1999, pp. 413–417.

Suboptimal Search Algorithm in Conjunction With Polynomial-Expanded Linear Multiuser Detector for FDD WCDMA Mobile Uplink

Mahdi Mozaffaripour and Rahim Tafazolli

***Abstract*—A suboptimum search algorithm that considers the users' power profile in conjunction with a primary stage of polynomial-expanded (PE) linear multiuser detector for mobile uplink is proposed to suppress interference level. The initial stage is improved by mathematical analysis using two new ideas based on the Rayleigh–Ritz and Gershgorin theorems for both synchronous and asynchronous users. The performance of the PE structure is further enhanced by a new suboptimum search algorithm as the second stage. The structure of the search algorithm is based on starting from a point close to the optimum search and performing sequential steps to modify it. The proposed structures of the PE method and the suboptimum search algorithm are well suited together and make them collaboratively work without encountering a high level of complexity, since they use similar information as the correlation matrix. The power profile of the users is also considered in the suboptimum search algorithm, which led to more than a 50% reduction of the complexity, while keeping the performance almost the same. The performance of the final structure is carried out by means of computer simulations, and it has been compared to a partial parallel interference cancellation method with optimized partial coefficients. One of the main features of the structure proposed in this paper is that it performs its operations on the canonical formulation of the system, which makes it highly suitable for a broad range of systems such as multicarrier code division multiple access and multiinput multioutput.**

***Index Terms*—Direct-sequence code division multiple access (DS-CDMA), polynomial-expanded (PE) multiuser detection (MUD), suboptimum search algorithm.**

I. Introduction

Conventional detectors for direct-sequence code division multiple access (DS-CDMA) systems are composed of a bank of matched filters, which suffer from multiple access interference (MAI). Since the work of Verdu [1] on the optimum detector, several suboptimum multiuser detectors have been proposed to improve the capacity and mitigate the MAI problem of the conventional method [2]–[4]; among them are the decorrelator and minimum mean square error (MMSE) [5]–[7]. Although these methods have several attractive properties, they suffer from implementation complexity, which is mainly due to a need to invert a large matrix. Some research has been carried out for approximating the inverse matrix [8]–[15]. The polynomial-expansion (PE) method is one of these methods, which needs to calculate a set of coefficients. Lei and Lim [9] have proposed a simplified PE, in which, according to its inaccurate parameter estimation, the convergence rate is rather slow. Another approach uses random matrix theories and is addressed in [13]. Reference [27] addresses the use of polynomial detectors for CDMA systems. However, it confines its limit to downlink scenarios.

Manuscript received April 13, 2006; revised October 23, 2006, February 18, 2007, and February 19, 2007. The review of this paper was coordinated by Prof. T. J. Lim.

M. Mozaffaripour was with the University of Surrey, GU2 7XH Surrey, U.K. He is now with ArrayComm LLC, Guildford GU2 7YD Surrey, U.K. (e-mail: mahdi@arraycomm.com).

R. Tafazolli is with the Centre for Communication Systems Research, University of Surrey, Guildford GU2 7XH Surrey, U.K. (e-mail: R.Tafazolli@surrey.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2007.901064