October 2001

Towards securing 3G mobile phones

R. Safavi-Naini
University of Wollongong, rei@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

G. Taban
University of Wollongong

Towards securing 3G mobile phones

Abstract

Third-generation (3G) mobile phones are capable of high data rate Internet connection and promise seamless connectivity for a free roaming user. They can provide an "always on" Internet, and make a range of services, traditionally available on desktop computers, accessible to mobile users, irrespective of their location. Providing adequate security for these phones and the services that they offer is a central concern for their acceptability and uptake. We briefly review the security of second generation mobile phones and then discuss security architecture proposed for 3G phones. The new security issues that are of importance because of the combination of their advanced capabilities and limitations are discussed.

Disciplines

Physical Sciences and Mathematics

Publication Details

This paper originally appeared as: Safavi-Naini, R, Susilo, W & Taban, G, Towards Securing 3G Mobile Phones, Proceedings. Ninth IEEE International Conference on Networks, 10-12 October 2001, 222-227.

Towards Securing 3G Mobile Phones (extended abstract)

Rei Safavi-Naini, Willy Susilo
Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, AUSTRALIA
Email: {rei, wsusilo}@uow.edu.au

Gelareh Taban
Wollongong, AUSTRALIA
Email: gt06@uow.edu.au

Abstract

We briefly review security of the second generation mobile phones and then discuss security architecture proposed for the third generation phones and the new security issues that will be of importance because of the combination of their advanced capabilities and limitations.

1 Introduction

Mobile phones are becoming an indispensable part of everyday communication. They provide the flexibility that is needed by an increasing number of mobile work force, and equipped with a wide range of advanced functionalities, are predicted to overtake other forms of communication in near future.

Third-generation (3G) mobile phones will have Internet connection of high data rate and promise seamless connectivity for a free roaming user. They will provide an 'always on' Internet, and make a range of services, traditionally available on desktop computers, accessible to mobile users, irrespective of their location. Providing adequate security for these phones and the services that they offer is a central concern for their acceptability and uptake.

In this paper we first give a brief overview of security features of second generation (2G) mobile phones and then discuss security issues in 3G systems.

2 Security in 2G Cellular systems

Security in cellular networks can be seen from the view point of operators and customers. The main concern of the operator is *correct billing* and ensuring that services cannot be stolen. From customers' view point, the requirements are (i) *confidentiality and privacy of communication*, (ii) *authentication of information* and (iii) *correct billing*.

The two widely adopted mobile phone systems are GSM and CDMA (and also TDMA).

GSM

The aim of GSM has been to make *the system as secure as the public switched telephone network*. With this goal security mechanisms prevent unauthorised network access and impersonation of subscribers, and protect confidentiality (preventing eavesdropping) and privacy (tracking of the user based on his/her phone signal) of the mobile users. In GSM system, a smart card will be the *Subscriber Identity Module (SIM)* that is used to identify the subscriber. GSM system uses this information and a challenge-response protocol to authenticate the user, and an algorithm called A5 to encrypt the communication. The system has databases that contain administrative information and the current location of each active subscriber in the network. To prevent the user's identity to be revealed, or his calls to be linked, the user will receive a different temporary identity by the system in each call. However the user's identity information and location can always be obtained from the network operator.

Cryptographic algorithms used in GSM were initially kept secret with the aim of providing higher security. However they were gradually leaked or reverse engineered and subsequently shown to be insecure. This includes encryption and authentication algorithms A3, A8, A5/1 and A5/2 [6, 4, 15].

CDMA/TDMA

In CDMA each user is assigned a unique code sequence that is used to encode his signal and decode the signal sent to him. The encoding process enlarges (spreads) the spectrum of the signal and is therefore known as *spread-spectrum modulation (SS)*. SS signals allow *multiple access* to the communication channel because the receiver can dis-

1531-2216/01 $10.00 © 2001 IEEE

tinguish between the users who are assigned different codes.

SS is particularly attractive because it provides higher security for air signals. It *increases privacy* because the data can only be recovered if the code is known to the receiver. It also provides *anti-jamming capability* and *low probability of interception (LPI)* because of wide spectrum and low power.

Similar to GSM systems, CDMA systems provide user authentication and encryption of data, but use different cryptographic algorithms and protocols. Eavesdropping in CDMA and TDMA is a lesser threat, because firstly the eavesdropper must know the type of the system, TDMA or CDMA, and secondly, in digital systems the voice is vocoded and so the sound is not only digitised but also compressed.

Service Theft

The main concern of the cellular service providers is service theft. By far the *cloning* has been the most widely used attack against mobile phones. It is easy to clone an analog handset by simply using a scanner to learn the mobile phone numbers of the handsets in the area, and the electronic serial numbers that go with them, and program these numbers into another handset.

A number of protective measures are used [16]. This includes laws against possession of scanning receivers, use of personal identification number (PIN) that must be entered before making a call, *RF fingerprinting* to distinguish transmitters, challenge-response authentication, and finally *call counting* where the handset and the network both keep track of the number of calls made by the handset and the number is checked before a new call is accepted. Combination of the above technologies has effectively reduced cloning fraud. However with the introduction of services that allow purchase of the phones over the Internet, no real verification of ID is possible and *subscriber fraud* has emerged as a new type of fraud. One method of detecting fraud has been by storing calling patterns of users and raising an alarm when a new user has the calling pattern of a previously disconnected user. Another kind of fraud is *subsidy fraud* where a phone whose cost is heavily subsided by a cellular carrier is activated on a different network.

3 3G Systems - An Overview

The 3G standardisation process started in 1995 when the International Telecommunication Union (ITU) began developing IMT-2000 (International Mobile Telecommunications for the year 2000). The main requirements of the IMT-2000 include support for a data rate of 144 kb/s for users in motor vehicles moving fast over large areas, 384 kb/s for pedestrians and 2.048 Mb/s operation for office use. Moreover, it must provide voice quality comparable to that of the public switch telephone network (PSTN), more efficient usage of bandwidth and provision of new services. 3G networks will support both packet switched and circuit switched data services.

The main two contenders for this standard that use terrestrial radio transmission technologies (RTTs) are the European-backed Universal Mobile Telecommunications System (UMTS) and the US-backed cdma2000. Both systems use Code Division Multiple Access (CDMA) technology for their radio interface.

To prepare, approve and maintain globally applicable technical specifications and technical reports for third generation mobile systems, the Third Generation Partnership Project (also known as 3GPP) was founded. The 3GPP Technical Specifications and Technical Reports will form the basis of standards of the partners [3].

Software

Software technologies have been developed to effectively use the Internet access provided by 3G phones.

An operating system for a mobile phone must provide fast access to applications. It must be modular so that various modules can be added or removed depending on the needs of the users, and it must be able to run on low power and not to drain the battery.

Currently, there are four Operating Systems that have been used widely in mobile devices: Palm OS, Windows CE, GeOS and Symbian EPOC. The OS provides protection for the stored data, such as Address and Date Book in Palm OS. Applications may provide their own security. For example Microsoft Pocket Internet Explorer that is shipped with a Pocket PC operating system supports encryption via secure socket layer (SSL).

There are several development systems for mobile devices. Palm OS applications are mainly developed using C language, although there are other development tools that can be used by non-programmers [8]. Windows CE applications use Microsoft Software Development Kit (SDK). GeOS and Symbian EPOC have their own SDK.

WAP

Wireless Application Protocol, WAP for short, is based on XML and HTTP and allows many lower network layer protocols, such as SMS or CDMA (3G) to deliver their content. To make WAP to work with existing HTTP servers, a WAP gateway is required. The gateway translates the communication between the server and the handset. That is, it converts the queries sent by the handset into appropriate HTTP format handled by the server, and in reverse translates the HTTP responses sent to the host into a compact binary format understandable by the WAP client. The WAE (Wireless Application Environment) User Agent which resides on the WAP client uses WML (Wireless Markup Language) as the format to display the content.

4 Security in 3G Systems

A 3G mobile phone resembles a desktop computer directly connected to the Internet. In has capabilities of the desktop without any protection provided for a desktop through the LAN connection and the firewall systems that protect the LAN from outside world. The phone it is directly connected to the Internet.

Security becomes particularly important because data connection is always on and the phone can be subject to attack at any time. The risk of all time open connection is similar to attacks mounted on hosts connected to the Internet. An unprotected connection can be used by malicious hackers to access data stored on the host, and/or run malicios codes to use the storage or computing power of the host for a range of attacks and unauthorised usages. The damages that can be caused by malicious codes, such as viruses and worms, become more pronounced because of the vast reach of the phone through the Internet and other wireless devices.

One of the main challenges in securing the system is the physical, and hence computational, limitations of a handset that puts severe limits on the choice of security algorithms that can be used. Moreover many applications require fast response time which puts yet another restriction on the kind of algorithm that can be used. On the other hand some services such as Internet banking or access to medical databases require a very high level of security. It is the combination of these factors, that makes provision of security a very challenging task.

The Third Generation Partnership Project (3GPP) working party on security has proposed a security architecture for 3G mobile phones [1]. The security enhancement compared with 2G systems are introduced because of (1) combination of known attacks on cellular phones and those on hosts connected to the Internet, (2) increasingly sophisticated software and devices used by attackers and (3) lack of physical security in some network elements. The security architecture defines five feature groups where each group achieves certain security objectives. The attacks counteracted in the proposed architecture include eavesdropping, impersonation of the user and *the network*, *man-in-the-middle attack*, and *compromising authentication vector*. In [2] a range of attacks on the system is considered and the protection offered by the architecture is evaluated with the conclusion that with correct implementation and configuration of the proposed architecture the majority of the attacks can be prevented. Because of the reach and functionality of mobile phones, defining a clear security policy and controlling access to resources is of the highest priority. Another important security risk to the phones is through the management and control subsystem. 3G network elements must support remote management and communication with other systems such as billing system which would be ideal targets for attacking the system. The nodes must be sufficiently protected and detailed security log for after-the-fact investigation must be planned. Another major risk area is the inter network security where signalling systems with plain messages for transfer of various kinds of information are used. Subverting these messages could result in complete collapse of the system and so control messages must be carefully secured.

Authentication protocol proposed by 3GPP

In 3GPP proposal, a new block cipher algorithm called Kasumi [10] is used. Kasumi is based on one of Matsui's proposed algorithms, Misty, and has a 128 bit key. Misty has been a public algorithm that has withstood public scrutiny for some years.

The basic authentication is performed by VLR (Visitor Location Register). The HLR (Home Location Register) is replaced by *Home Environment (HE)* and the SIM is called the *UMTS SIM (USIM)*. As in GSM, the *HE* chooses a random challenge *RAND* and encrypt it with the $USIM$ authentication key K to generate a response RES, a confidentiality key CK, an integrity key IK, and an anonymity key AK. The relation among these entities is

$$\{RAND\}_K = (RES||CK||IK||AK)$$

There is also a sequence number SEQ that is known to the HE and the USIM. A MAC (Message Authentication Code) is computed on $RAND$ and SEQ and the sequence number is masked by exclusive or-ing it with the AK. The challenge $RAND$, the expected response RES, CK, IK and the masked sequence number are made up into an *authentication vector AV* which is sent from the HE to the VLR. Next, VLR sends $(RAND, masked\ SEQ, MAC)$ to the mobile station, and the mobile station computes the response and the keys, unmasks the SEQ, verifies the MAC, and if it is correct, returns the response RES to the VLR.

Security in OS and WAP

Capabilities such as viewing and playing multimedia information in real-time, and/or performing complex transactions require high level of functionalities and support in the handset. Securing stored information requires access control mechanisms similar to what is offered in the operating systems. Protections offered by Palm OS and Window CE and possible attacks on them are good examples of OS security in future 3G systems.

WAP provides a layered architecture [9] with security layer called WTLS (Wireless Transport Layer Security). A WAP gateway uses WTLS to provide privacy, integrity and authentication between itself and a WAP browser client. WTLS provides the functionality of a strong Internet security standard over a wireless airlink and is based on TLS 1.0 (Transport Layer Security) which is in turn based on SSL

3.0.

WAP gateway uses SSL to communicate securely with a Web server over the Internet on one side, and takes SSL-encrypted messages from Web and translates them for transmission over wireless using WTLS. It also converts messages form the handset from WTLS to SSL. The WTLS protocol uses digital certificates to create a secure communication pipe between a mobile phone and a WAP server. When Alice visits a site secured by a WTLS, her micro-browser sends a message to WAP server requesting a session. The WAP server sends its signed certificate, which is verifiable by Alice's handset that has stored the public key of the certificate authority. Alice's micro-browser generates a key which is encrypted by the server key and is sent to the server. Now micro-browser and the server can communicate encrypted messages using their shared key.

In some applications that work across many wireless networks, content must remain encrypted from the time it leaves their application server until it arrives at the WAP handset. During translation between SSL and WTLS, messages will become in plaintext form and can be exposed. Care must be taken in the design of translator to minimise the threat. WTLS goes beyond TLS 1.0 and offers such features as datagram support, dynamic key refreshing and optimised handshake [14].

5 New Security Services and Risks

3G phones will enable a range of new services and will rise many new security concerns. In the following we outline a number of emerging risk areas of risk that either did not exist in 2G systems or the level of risk attached to them was an order of magnitude lower, because the 2G systems' limited functionalities.

User authentication is the first step in securing a mobile system and forms an integral part of security in all 2G systems. In 3G systems, authentication requires a considerably higher level of assurance. This is because the phones support many more complex and security critical applications such as Internet banking and access to databases of sensitive information (for example, medical databases). Biometric technologies for user identification offer a high level of assurance and combined with other authentication methods such as PIN number can guarantee the required security. In [18] a fingerprinting technology for verification of user identity is proposed. A sensor embedded in the surface of the cell phone captures an image of user's fingerprint which is analysed and converted into a unique representation of the user's fingerprint and stored in the phone and at a later stage use to identify the user. Combination of biometric methods and cryptographic user identification protocols could provide a very high level of security. Again, limitations on computational power of the handset and delay introduced by the protocols must be carefully taken into account.

In some high security applications user authentication must be end-to-end and so obtaining the agreement of the bank, the cellular provider and the handset on the same solution is required. This adds a new dimension to the secure implementation of the system.

Securing Multimedia Services

High bandwidth and fast data transfer enable 3G mobile phone to support multimedia information and so provide a wide range of services such as CD-quality music, video information and multi-user games.

Processing multimedia information in real time and on limited bandwidth and highly constrained computational environment of a cell phone requires sophisticated coding methods and powerful signal processing techniques. Adding security to the multimedia delivery systems, adds a new dimension to the complexity of the system and demands specially designed algorithms to provide adequate security and at the same time reasonable quality that is adjustable to the capabilities of the receiving device. In many applications, multimedia information are copyright protected. This means that the cell phone not only has to provide access control but also handle watermarking systems that are proposed for the protection of copyright. A possible solution would be combining two or more functionalities in an attempt to reduce the computation cost. For example combining encryption and compression into one system, instead of conventional method of encrypting compressed data and effectively applying the two processes consecutively, could result in less overall computation. However the combining operation must be carefully analysed so the performance (compression and security in this case) of the system is not drastically affected. We note that a requirement of encryption algorithms is that they do not spread channel error. This is because multimedia information is firstly compressed and then encrypted and so if the encryption algorithm spreads channel error the decompressed signal will become completely unintelligible.

Billing and Electronic Payment

In 3G systems, one of the main challenges comes from the fact that it is not necessary to bill on a "per minute" basis. Packet switching means that users will be charged by the amount of data they send and receive and not by the time. Small prices add up to the phone bills. DoCoMo's customer pay around 4.2 yen for a 250-character email message and 14.7 yen for a news item. Companies providing the service pay 9 per cent of the revenue. Services such as above require very small amount of money to be paid electronically. This requires electronic payment systems that allow a customer to freely move in the cyber world and purchase without the need for a prior account to be setup, while the cost of payment is only a small fraction of the actual purchase. The system must ensure that the risk to the merchant

remains 'controlled', that it highly unlikely to be above a specified limit.

The phone will also be used for medium valued purchases from e-shops and also high valued Internet banking which may involve transfer of large sums of money. That is the full range of electronic payment mechanisms, including credit card, electronic cash and micro-payment, in a computationally restricted environment must be implemented. Again, the challenge in this case is the implementation of protocols which provide a high level of security in an environment with strict limitation on computational resources.

Position Fixing and Big Brother

Position information allows provision of useful services such us finding the location of *the closest* petrol station or restaurant, when a user visits an unknown place. Analysts believe that location fixing will open-up a multi billion-dollar market. A number of competing technologies have been proposed. Adding a Global Positioning System (GPS) chip and an antenna to the mobile phone will give accurate position information but it might not work if walls or car roof block direct communication. *Server-aided* GPS allows position fixing from anywhere, and also reduces the problems of extra weight and power of the mobile by shifting most of the processing to the server. There are earthbound techniques that measure the distance between a mobile and 3 base stations and use that to locate the mobile.

The main concern with using position fixing is the potential to breach privacy. For example a car equipped with position fixing devices for protection against theft, can be potentially used in an invasive way to track people's movement. In some systems, such as GPS, position can be found without any data recorded by the system while in others such as the earthbound systems users must trust the network operator not to track them. It is also worth noting that finding positions might be invaluable in tracing criminals and so mechanisms that provide accurate position fixing in lawful situations are required. Cryptographic systems with *revocable anonymity* where identity information can be recoverable under specified conditions have been studied in the context of electronic payment systems. Similar approaches can be adapted to location fixing to allow restricted anonymity while providing accountability for mobile users.

All-time Connectivity ("always-on"*)*

'All-time connectivity' and high functionality will inevitably mean an increased risk of attack by mobile viruses and worms as well as malicious hackers. Malicious codes may be embedded in mail attachments, or be inadvertently downloaded with other data from a Web site. Even in the very short life of hand-held devices a number of viruses and worms for hand-held devices have already been written. *Liberty Crack*, first released on an Internet Relay Chat, was a *Trojan Horse:* it looked harmless but included malicious code [11]. Malicious code can not only wipe out data, applications and the operating system, but can also infect software to keep Liberty Crack from spreading to PCs, and from there to hand-held devices.

Viruses infection can spread in many ways: for example through sharing a removable storage cards, infrared transmission, or through an email attachment. In June 2000 a hacker attacked DoCoMo mobile phones an email message containing a malicious script. The message claimed to be a test and asked a question and when the user answered 'yes', a script was run that dialled 110 which is the emergency service. In the same month Timofonica, a Visual Basic script worm attacked cellular phones in Spain. The worm spread via attachment to email messages sent to PCs. From a PC it sent an email that was receivable by a mobile device. When the victim opened the attachment it changed the devices registry. In the next boot of the system the worm erase the system information and leave the device unable to boot again.

Protecting against Device Theft

One of the main differences between a desktop computer and a 3G mobile phone when providing protection for the system, is threat to physical security. A mobile phone can be easily stolen or even lost. This requires provisions to ensure the secrets and data stored in the device are protected and cannot be mis-used.

In particular identity information stored in the device cannot allow an attacker to impersonate the owner and misuse his privileges. Using multiple source identity verification methods, that is, requiring more than one piece of evidence to prove identity could limit the attacker. That is the secrets stored in the mobile must be complemented with other secret information, such as fingerprint or PIN, to form the full identity.

Today SIM identifies users to the phone system. In future it may act as a universal identification card. Loss of a phone must safely lock up the secrets stored in it. A solution is to store important information on secure servers and make them accessible via WAP connection. The SIM will only store a personal identifier which is the private key of the user and is protected by the PIN. The card will shut itself if wrong numbers are keyed in three times. To switch it back on, the owner must take it to the police station. A private key will replace hard-to-remember logins passwords for websites as well as credit cards and pins.

Important data in the mobile must be kept in encrypted forms however this will increase the access time of the owner and puts extra load on the processor. Protection of resident data must be provided without affecting performance of the mobile.

Physical Limitation and Implementing Security

A successful security technology for mobile phones must satisfy the following requirements.

Security processes must not, (i) delay to the call set-up

and subsequent communication, (ii) increase channel bandwidth, (iii) increase the effective error rate of the communication, and (iv) add complexity in operating the device.

Mobile devices have limited computational power and memory. Currently, mobile devices are equipped with around 2 - 32 MBytes RAM to store the data and processors ranging from Motorolla EZ Dragonball with 16 MHz (for Palm OS) to Intel embedded 386 processor. This means that traditional cryptographic algorithms takes a long time which could not only add unacceptable delay to the communication but also drain the battery of the mobile.

Public key crypto algorithm are the main cryptographic tool for unique identification of users and digitally signing electronic documents. Both of these operation are are indispensable in a building trust in transactions. The amount of computation required by the mostly widely adopted public key algorithm, that is RSA, immediately rules out rules its direct application. Server-aided versions of this algorithm [5] distributes the computation between the mobile and the server such that the server will not learn the secret stored in the card and at the same time the more expensive part of the computation is performed by the server. Elliptic curve cryptography (ECC) algorithms provide high security with much shorter keys and have been proposed. ECC algorithms provide high security with much shorter keys compared to RSA. The level of security offered by 1,024 bits key RSA algorithm can be achieved with only 160 bits ECC algorithm [7]. This has enabled ECC to be implemented in low powered devices such as smart cards [7].

Encrypting files and data for storage require a symmetric key algorithm. Algorithms such as Data Encryption Standard [12] will be too costly in terms of the required computation and memory. Stream ciphers can be designed to have high security and operate at high speed. Most proposed encryption algorithms for mobile devices, including A5 algorithms, are stream cipher.

Security by Obscurity
It is strongly argued that hiding algorithms and methods would increase security of the systems. Experience has taught us differently. GSM and CDMA algorithms were all initially confidential and subject to export limitations. However as noted earlier, all the algorithms were eventually leaked, or reverse-engineered, and then cryptanalysed. Another prominent example of the failure of 'security by obscurity' is compromise of the encryption system of DVD standard [17] and the watermarking system proposed for audio. Recent development of Advanced Encryption Standard [13] through a public process provides much higher assurance on the underlying algorithms used for providing security.

6 Conclusion

Securing 3G mobile phones is a daunting task. Combination of advanced functionality and vast reach through the Internet and create an ideal medium for attackers to infiltrate computer systems and networks without being tracked. On the other hand, acceptability and take-up of the advanced services that could be supported by these phones will ultimately depends on providing assurance about the security. These factors make provision of security of highest priority in 3G systems.

References

[1] 3GPP. 3G Security Architecture version 3.0.0 TS33.102. *Available online at http://www.3gpp.org.*

[2] 3GPP. 3G TR 33.900 version 1.0.0. *Available online at http://www.3gpp.org.*

[3] 3GPP. Third generation partnership project agreement. *Available online at http://www.3gpp.org.*

[4] E. Biham and O. Dunkelman. Cryptanalysis of the A5/1 GSM stream cipher. *Indocrypt 2000, LNCS 1977*, pages 43 – 51, 2000.

[5] D. Boneh, N. Modadugu, and M. Kim. Generating RSA keys on a handheld using an untrusted server. *Indocrypt 2000, LNCS 1977*, pages 271 – 282, 2000.

[6] M. Briceno. Breaking COM128 report. *available online at* http://jya.com/crack-a5.htm#mb, 1998.

[7] Certicom. Elliptic curve cryptosystem for smart cards. *Available online at http://www.certicom.com/research.html.*

[8] L. R. Foster. *PalmOS Programming Bible.* IDG Books Worldwide, USA, 2000.

[9] U. Hansmann, L. Merk, M. S. Nickous, and T. Stober. *Pervasive Computing Handbook.* Springer-Verlag, 2001.

[10] KASUMI Spec. Kasumi. *ETSI/SAGE vol. 1, 23 December 1999, Available online at* http://www.etsi.org/dvbandca/.

[11] N. Leavitt. Malicious code moves to mobile devices. *Computer, December 2000*, pages 16 – 19, 2000.

[12] National Bureau of Standards. Data encryption standards (DES). *FIPS Publication 46*, 1977.

[13] National Institute of Standards and Technology (NIST). Advances Encryption Standard development effort. *Available online at http://csrc.nist.gov/encryption/aes/.*

[14] Openwave Systems Inc. Openwave. *Available online at http://www.phone.com.*

[15] S. Petrovic and A. Fuster-Sabater. Cryptanalysis of the A5/2 Algorithm. *Cryptology ePrint Archive, available online at http://eprint.iacr.org/2000/052.pdf.*

[16] M. J. Riezenman. Cellular security: better, but foes still lurk. *IEEE Spectrum, June 2000*, pages 39 – 42, 2000.

[17] F. A. Stevenson. Cryptanalysis of Contents Scrambling System. *Available online at http://www.cs.cmu.edu/ dst/DeCSS/FrankStevenson/ analysis.html.*

[18] U. Varshney and R. Vetter. Emerging Mobile and Wireless Networks. *Communications of the ACM vol. 43 no. 6*, pages 73 – 81, June 2000.