A Survey of WiMAX and Mobile Broadband Security

Emily Yang, emy1@cec.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

This paper covers the security mechanisms and issues in WiMAX, as well as universal threats to wireless networks. It also examines similar wireless and mobile broadband technologies, WLAN, MBWA, and 3G and the security measures that are taken. Awareness is raised of the current as well as future security implications of an increasingly wireless world.

Table of Contents

1.0 Introduction

Consider a scenario in which a person wakes up and walks around with her laptop connected to a local area network in her house as she gets ready, checking email, and using it to read the news as she eats breakfast. On the bus on her way to work, she pulls out her iPhone to browse the internet, check the scores of her favorite sports teams, watch some funny YouTube videos, and call a friend. She then stops at Starbucks, connects to the Wi-Fi, and answers some email while sipping some coffee. Once at work, she pulls out her laptop to connect to the WLAN at the office and starts work.

The fact that this scenario sounds fairly normal and typical is interesting, not only because of how technology and internet-centered our lives have become, but because every network connection that this person used was wireless. Most people use multiple types of wireless internet every day without even realizing it. It's fast and convenient, but how do we know that the data we send and receive is secure? As it turns out, there are many

mechanisms in place to provide security, but there are also many weaknesses and threats, especially since wireless and mobile broadband service is a fairly new and still developing technology. The IEEE 802.16 standard and its implementation, WiMAX, provide an interesting case of the evolving nature of mobile broadband use and security as well as problems that are continuously being found.

In this paper we discuss the inherent and fairly universal weaknesses and security threats of wireless networks, take a thorough look at WiMAX's security mechanisms and issues, and then examine some similar wireless and mobile broadband technologies and their security. Through discussion of common security problems as well as in-depth study of real world examples, like WiMAX, we can come to a better understanding of the threats we face now and the implications for the future of mobile broadband security.

2.0 Background on Wireless Security

There are several security concerns and development implications that arise from the varying nature of mobile communication and the fast-paced increase in usage of mobile devices for m-commerce, email, and other functionality that require secure connections. Mobile security poses an interesting problem, largely because it requires an enormous amount of compatibility over different access media, as well as a wide range of end user devices, with different capacities and capabilities. Users expect to be able to use their mobile devices spontaneously in many different environments, and sometimes continuously while going through multiple types of access points, for example, in a moving car. Despite the frequent need for even more security than is provided to their counterparts that are within a fixed network, mobile devices have much less processing ability and also need to comply with reasonable cost, size and weight restrictions as well as usability requirements. To make matters even more complicated, mobile devices are also often lost or stolen, which calls for even higher protection of sensitive information. Through more detailed discussion of the security challenges it becomes clear that there are many hurdles that engineers must consider when designing mobile communication architectures. [Raghunathan03]

Figure 1: Major Mobile Security Concerns

2.1 Mobile Security Concerns

Several issues have been identified that must be taken into account when evaluating the security of mobile communication. Some of the most important and universal ones are discussed below (also seen above in Figure 1).

2.1.1 Authorization Techniques

Especially because the devices are mobile, there is a large risk that they might fall into the wrong hands. Here, a usability issue arises where people expect to be able to conveniently and frequently use their devices, which often rules out the idea of a login procedure. Also, there are a variety of data types flowing to and from the devices, both public and private, that need different types of authentication, such as encryption, Message Authentication Codes (MAC), or digital signatures. It may even be the case that different network levels require different authentication. [Jurjens08]

2.1.2 Storage of Sensitive Information

There is an increasing amount of sensitive information that can be stored on mobile devices, from passwords, to credit card information, to certificates that must be secure. The performance and physical capabilities of the device can make it hard or impossible to sufficiently encrypt data. [Jurjens08]

2.1.3 Application Environment

Like any computer, mobile devices must be able to defend against software attacks such as viruses, but unlike

a machine in an unchanging network, they do have constant access to software patches or updates. Sometimes even established security mechanisms are not possible on handhelds due to their limited performance capabilities. [Jurjens08]

2.1.4 Network Availability

A network or service should only allow certain authorized devices to connect to it, which requires strictly observed and verified user privileges and defense against denial-of-service attacks and other misuse of the network services. [Raghunathan03]

2.1.5 Interoperability

Mobile devices are used in many different environments and thus must be able to accommodate a vast array of security protocol standards, for example, those required for both 3G and LAN networks. There may also be the need to communicate with servers that use different cipher suite and key exchange algorithm arrangements, so it is desirable for the appliance to be as flexible as possible for the allowable combinations. [Raghunathan03]

2.1.6 Computational Requirements and Battery Life

Not only do mobile devices have significantly less processing capability than a laptop or desktop computer, but the energy consumption of running complex cryptographic algorithms must be taken into account to avoid severely affecting battery life. [Raghunathan03]

2.1.7 Usability

Mobile communication differs from wired network use in that it is expected to be always accessible, but used spontaneously, for shorter amounts of time, in and across different environmental conditions. Therefore, a mobile user expects seamless transitions between network media and the ultimate amount of convenience. Because of this, common design practice calls for transparent security services, which often leads to insufficient security. Also, mobile devices have smaller screens and keyboards that make it hard to have convenient security measures.[Josang03]

3.0 IEEE 802.16 Metropolitan Area Network (WMAN and WiMAX)

The IEEE 802.16 standard, used by WiMAX, supports fixed broadband wireless access with target transmission rates of around 100 Mbps, over long distances of up to 30 miles, where subscriber stations are within range. Other potential uses include using WiMAX as backhaul for Wi-Fi hotspots or 3G networks [Andrews, Ghosh, Muhamed 07]. IEEE 802.16e is built upon the original IEEE 802.16 standard but allows for mobile broadband access with the allowance of nomadic subscriber stations that can move at slow speeds while still receiving services [Andrews, Ghosh, Muhamed 07]. This is a possible innovative way to provide faster data rate capabilities to mobile subscribers who use IP based services on their devices. IEEE 802.16 incorporates a pre-existing standard, Data Over Cable Service Interface Specifications (DOCSIS), which has led to many security issues because WiMAX is not a wired technology like Cable, and therefore is vulnerable to many issues like the ones above that may not have been considered [Andrews07]. The security mechanisms that are included in 802.16 include encryption of data, security associations, certificate-based authentication, and privacy key management protocol. [Eklund06] There have been security holes and problems identified within the standard that leave it at risk for forgery and man-in-the-middle attacks due to lack of proper authentication as well as replay and denial-of-service attacks. Some of these security concerns

have already been addressed in the amendment of the standard presented in 802.16e

3.1 Security Mechanisms

In order to provide data integrity and privacy over an open radio channel, the MAC layer of 802.16 includes a security sub layer. The security mechanisms include the encryption of data between the base station (BS) and subscriber station (SS), certificate-based authentication of the SS, and privacy key management (PKM) as an authenticated client-server key management protocol. In order to patch up some major security issues described below and to account for the addition of mobile services, the standard 802.16e has specified some changes in the security measures. [Huang08]

3.1.1 Encryption

802.16 includes RSA (Rivest Shamir Adleman), DES-CBC (Data Encryption Standard- Cipher Block Chaining) and AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) as the standard encryption algorithms and HMAC (Hashed Message Authentication Code) and CMAC (Cipher-based Message Authentication Code) as the cryptographic algorithms. These algorithms are used for the encryption of traffic encryption keys (TEKs), traffic data, and Authorization Reply messages. [Nuaymi07]

3.1.2 Security Associations

Security Associations (SAs) are information sets that support secure communication that is shared between a Base Station (BS) and its client SSs or mobile stations (MSs). [Nuaymi07]This may include information such as the cryptographic suite used for the SA, data encryption methods, and TEKs along with their lifetimes and state information. Upon entering a network, an SS will set up a primary SA, and then may add static and dynamic SAs depending on specific service flows. [Eklund06]

3.1.3 Certificate-Based Authentication

X.509 Version 3 certificate formats must be used by SSs in order to comply with the 802.16 standard. The manufacturer provides and installs a unique X.509 certificate in each SS, which contains the SS RSA public key and SS MAC address. In standards 802.16-2004 and above there is also an X.509 certificate for the BS so that both the SS and BS can mutually verify authenticity. [Nuaymi07]

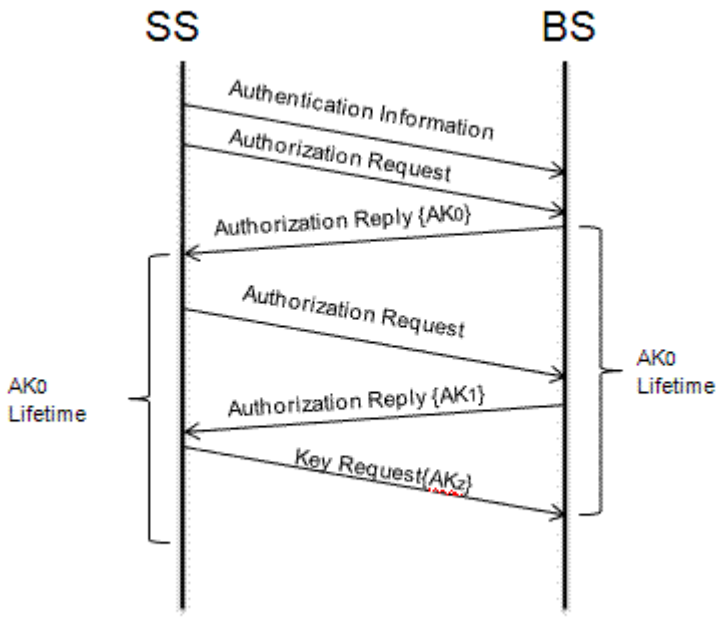


Figure 2: BS and SS AK Management

[Eklund06]

3.1.4 Privacy Key Management Protocol (PKM)

PKM establishes a shared secret between the SSs and BS to allow the BS to distribute keying materials such as Authorization Keys (AKs) and SAs to client SSs as well as periodic renewal and reauthorization of keys. The authorization and TEK state machines manage keys in the SS. PKM request and Response messages are sent between the BS and SS as MAC management messages to handle transmission of the AKs (see Figure 2). A new instance of the TKE state machine is started by the SS for each SA that it receives from the BS. [Eklund06]

PKMv1 is used in the standard up until 802.16e when PKMv2 was introduced to provide stronger security. The greatest difference between the two is that in PKMv1 the BS authenticates the SS and then enables the ciphering of data by providing it with keying material, whereas in PKMv2 there is mutual authentication between the BS and MS. Also, in PKMv1, public key cryptography is used for the establishment of a shared secret between the SS and BS, but in PKMv2 RSA-based or EAP-based authentication protocols are used along with RSA and EAP as sources of keying materials. [Nuaymi07]

3.2 Security Issues

There are many security threats that have been found in the 802.16 standard. Because of the focus on the MAC level security, the PHY level is left vulnerable to attacks, especially with the addition of mobility in 802.16e. 802.16 also shares 802.11's data confidentiality insecurity due to WEP. [Johnston04] The most serious security problems arise in relation to the lack of BS Authentication in earlier versions of the standard, as well as the high risk of replay and DoS attacks.

3.2.1 BS Authentication

One of the major holes in the initial versions of the 802.16 standard was the lack of authentication of the BS by the SS. This left WiMAX very vulnerable to Forgery and Man-in-the-Middle attacks where the SS would

not know whether or not it was communicating with a legitimate BS. [Eren07] This problem has been patched in 802.16e by adding the mutual authentication described above in PKMv2.

3.2.2 Replay and DOS Attacks

It is possible for an attacker to intercept and store an Authorization Reply Message and then repeatedly send the message to the BS. Since the BS will find that the message is from an authorized SS, its resources will be consumed, resulting in a Denial-of-Service Attack. Also, a replay attack is possible wherein an attacker intercepts TEK messages and then replays them in order to gain the information needed to decrypt traffic data by using the two-bit Key Sequence Number of the TEK.[Eren07] Another threat arises from the lack of explicit definitions of the authorization SA, which leads to the possibility of encryption key reuse because the SSs cannot distinguish reused SAs. [Huang08]

3.3 Security Patches in Later Versions

In standards IEEE 802.16e and above some of the above stated security flaws have been or are being addressed. The goals for improvement include changing from DES in CBC mode for encryption to AES used in a well-understood mode of operation, an Extensible Authentication Protocol (EAP)-based authentication scheme, specification and first class concept status of the authorization SA, and stronger authorization and key management. [Maccari07]

Security mechanisms such as encryption, security associations, certificate-based authentication, and private key management protocol are included in the 802.16 standard to provide protection. Still, weaknesses have been found in the standard's security leading to attacks that take advantage of the lack of BS authentication, and utilize replay and DoS attack strategies. Although fairly extensive measures have been taken to secure and authenticate data, the wireless medium creates a continually challenging security problem for designers of the standard. Amendments like 802.16e and later continue to attempt to patch holes that have been found, but still there is much risk that remains, especially in the PHY layer for attackers who are able to be in close proximity to the vulnerable parties. For now, increased use of AES is encouraged, as it has not yet been cracked and is memory and computationally efficient. Examination of other closely related technologies such as 802.11 (WLAN), 802.20 (MBWA) and Third Generation Cellular (3G), shows similar security techniques and issues.

4.0 Overview of and Security in Other Closely Related Technologies

The three most closely related technologies to IEEE 802.16 are IEEE 802.11, IEEE 802.20, and 3G, the first two of which are wireless data technologies, and the third of which is voice-based. Because they are all based on unwired architectures, using any of them for packet-based delivery services results in many of the security concerns described above.

4.1 IEEE 802.11 Wireless Local Area Network (WLAN)

Also implemented as Wi-Fi, this network utilizes radio frequency technology rather than traditional coaxial and is very fast, handy and cost efficient. It is especially popular in home or office situations where people want to conveniently connect, and stay connected to the Internet while moving around freely inside a space that usually has a range within 100 meters. It is, however, highly vulnerable to eavesdropping and packet loss because of its electromagnetic wave transmission medium. [Andrews07]

4.1.1 Security

The three security technologies that the IEEE 802.11 standard specifies in order to ensure data security are Service Set Identifier (SSID), Media Access Controller (MAC) and Wired Equivalent Protection (WEP). All of these technologies have been found to have severe weaknesses, especially if not handled correctly. [Wang08]

4.1.1.1 SSID

The use of the SSID is meant to prevent unlicensed users from entering the WLAN by setting different SSIDs for each access point and identifying groups of users with different access permissions. Each sub-network has its own authentication. A security issue arises, however, in the fact that the technology consists of a simple password that can easily be leaked by anyone who uses the WLAN. [Wang08]

4.1.1.2 MAC

This security mechanism uses the unique MAC addresses of each wireless workstation, which consists of a binary string of 48 bits in the network card. Each access point holds an address list of the permitted users, and turns away any user not specified in the list. Because of the need for fast updates of the MAC address list, scalability becomes an issue. Authentication is also questionable because of the possibility of forging a MAC address. [Wang08]

4.1.1.3 WEP

WEP is a static encryption algorithm based on the RC4 algorithm that protects the link data transmitted in WLAN and depends on a shared key. It is meant to provide authentication, encryption and integrity but many flaws in its security have been exposed since its release. These weaknesses can be found in its careless use of RC4, a lack of effective key management, insufficient IV space, use of CRC, and insecure authentication mechanisms. [Wang08]

4.2 IEEE 802.20 Mobile Broadband Wireless Access (MBWA or MobileFi)

The stated mission of IEEE 802.20 is *to develop a specification for an efficient packet-based air interface optimized for IP-based services, with the goal of enabling world-wide deployment of affordable, ubiquitous, always-on, and interoperable multivendor mobile broadband wireless access networks* [Yang07]. These fully mobile broadband wireless networks will have a layered architecture, similar to other IEEE 802 specifications, consisting of the physical (PHY), medium access control (MAC), and logical link control (LLC) layers. [Bakmaz07] Other networks that are not IP-based are more expensive and will not perform as well, which will provide broad market potential for MobileFi. Another unique specification of IEEE 802.20 is that it must be able to support mobility classes of above 200 kilometers per hour, for example someone riding in a high-speed train or a very fast car. [Greenspan08] The standard must conform to IEEE 802.1D (MAC Bridges) and 802.1F (Virtual LAN Bridges), and will support intertechnology roaming and handoff, quick intercell and intersector handoff, fast resource allocation, as well as support of both IPv4 and IPv6. It will have the ability to be deployed alongside existing cellular systems and will operate in bands below 3.5 GHz, with a peak data rate of over 1 Mb/s.

4.2.1 Security Issues

Because MBWA is wireless, it falls victim to many of the security issues described above. The major concerns that are focused on for mobile broadband are *protecting against theft of service on behalf of the service provider, protecting the privacy of the user, and deterring denial-of-service attacks* [Yang07]. Another important issue involves the authentication of the mobile stations and base stations. Because the

standard has not yet been implemented on a large scale, there have not been many significant security issues found.

4.2.1.1 Encryption Method

The encryption algorithm that has been chosen to protect private information is AES due to its strong and undisputed reputation. Either stream or block ciphers will be used and will provide user anonymity as well as four different combinations of privacy and integrity for different appropriate situations. [Yang07]

4.2.1.2 Authentication

The RSA algorithm will be used to authenticate the base and mobile stations using digital signatures to ensure that unauthorized third parties are protected against. Key exchange will be public and will use elliptic curve cryptography because it requires less storage, power, memory, and bandwidth than other similar systems. [Yang07]

4.3 Third Generation (3G) Networks

3G technology is fundamentally voice-based, [Bakmaz07] but it also delivers broadband applications to subscribers with high-speed data services as well as support for multimedia services. Universal mobile telephone system (UMTS) and high-speed downlink packet access (HSDPA) are being deployed by mobile operators who use the global system for mobile communications (GSM). Other 3G solutions include the use of 1 x evolution data optimized (1x EV-DO) or time division synchronous CDMA (TD-SCDMA). These solutions all provide between a few hundred kilobits to a few megabits per second of data throughput. 3G technology continues to become more and more refined, with future goals of supporting a peak data rate of 100 Mbps in the downlink and 50 Mbps in the uplink with three to four times the amount of average spectral efficiency as previous versions. [Andrews07] 3G technology allows for global mobility but suffers deficiencies in spectral efficiency and latency in comparison with its packet-based wireless counterparts described above. Although it is a fairly different technology, 3G also falls victim to many of the universal wireless security threats described in section 2.

4.3.1 3G Security Protocols

3G systems require the ASPeCT (Variant B) Protocol, which includes *mutual authentication of user and network, exchange of certified public keys, session key agreement, joint control of session key, mutual implicit key authentication, mutual key confirmation, mutual assurance of key freshness, confidentiality, initialization of payment mechanism, and non-repudiation of origin* [Newe03]. Also the establishment of a secret session key is required for authentication and initialization of payment between a mobile user and service provider. [Newe03]

5.0 Summary and Conclusion

In this paper we have discussed the major security threats to wireless networks, taken a close look at WiMAX, and also examined some similar technologies such as 802.11, 802.20, and 3G. All of these technologies are threatened by similar weaknesses simply because of their air interfaces. Current solutions involve encryption, authentication using certificates, and the use of private keys, as in WiMAX. Man-in-the-middle attacks, denial-of-service attacks and replay attacks all pose significant threats to the security of these technologies. It seems that mutual authentication of receivers and transmitters as well as using extremely secure encryption algorithms are important to providing higher levels of security. 802.11 and 3G

have provided and will continue to provide useful, real-world information to aid in the evolution of security measures for 802.16 and 802.20. It appears that 802.16 will continue to be developed to become closer to the standards set for 802.20, which may mean that 802.20 will never be implemented on a very large scale, but has at least set the bar for what should be expected in the future from mobility and security in WiMAX.

It appears that the world is becoming increasingly dependent on wireless technology, for convenience in urban areas, and for providing service to more remote areas. This drive towards wireless networking will prove to be very challenging, both in the types of networks that are successful, functionally and in the market, as well as the implications that will arise involving how to keep our data secure and defend against increasing numbers of attacks. It is an exciting, but definitely not easy shift in security concerns for developers.

References

1. [Andrews07] Andrews, Jeffrey G.; Ghosh, Arunabha; Muhamed, Rias; "Fundamentals of WiMAX: Understanding Broadband Wireless Networking," Prentice Hall, 2007

2. [Nuaymi07] Nuaymi, Loutfi; "WiMAX: Technology for Broadband Wireless Access," Wiley, 2007

3. [Eklund06] Eklund, Carl; Marks, Roger B.; Ponuswamy, Subbu; Stanwood, Kenneth L.; van Waes, Nico J.M.; "WirelessMAN: Inside the IEEE 802.16 Standard for Wireless Metropolitan Networks," IEEE, 2006

4. [Newe03] Newe, T.; Coffey, T.; "Security protocols for 2G and 3G wireless communications," ACM International Converence Proceeding Series Vol. 49, 2003, Pages 335-340, http://portal.acm.org/citation.cfm?id=963666

5. [Maccari07] Maccari, Leonardo; Paoli, Matteo; Fantacci, Romano; "Security Analysis of IEEE 802.16," IEEE International Converence on Communications , 2007, p 1160-1165, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4288868

6. [Johnston04] Johnston, David; Walker, Jesse; "Overview of IEEE 802.16 security," IEEE Security and Privacy, v 2, n 3, 2004, Pages 40-48, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1306971

7. [Wang08] Wang, Maocai; Dai, Guangming; Hu, Hanping; Pen, Lei; "Security Analysis for IEEE802.11," 2008 International Conference on Wireless Communications (WICOM 2008), 2008, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4678636

8. [Greenspan08] Greenspan, Arnold; Klerer, Mark; Tomcik, Jim; Canchi, Radhakrihna; Wilson, Joanne; "IEEE 802.20: Mobile broadband wireless access for the twenty-first century," IEEE Communications Magazine, v 46, n 7, 2008, Pages 56-63, http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=4557031

9. [Bakmaz07] Bakmaz, Bojan M.; Bojkovic, Zoran S.; Milovanovic, Dragorad A.; Bakmaz, Miodrag R.; "Mobile broadband networking based on IEEE 802.20 standard," 8th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2007, Pages 243-246, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4375983

10. [Yang07] Bolton, Walker; Yang, Xiao; Guizani, Mohsen; "IEEE 802.20 Mobile broadband wireless access," IEEE wireless Communications, v 14, n 1, 2007, Pages 84-95,

http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&isnumber=4107923&arnumber=4107937

11. [Raghunathan03] Raghunathan, Anand; Ravi, Srivaths; Hattangady, Sunil; Quisquater, Jean-Jacques; "Securing Mobile Appliances: New Challenges for the System Designer," Design, Automation and Test in Europe, V 1; 2003 pg 10176, http://portal.acm.org/citation.cfm?id=789083.1022723

12. [Josang03] Josang, Audun; Sanderud, Gunnar; "Security in mobile communications: challenges and opportunities," Conferences in Research and Practice in Information Technology Series, V 34; 2003, http://portal.acm.org/citation.cfm?id=827993

13. [Jurjens08] Jurjens, Jan; Schreck, Jeorg; Bartmann, Peter; "Model-based security analysis for mobile communications," International Conference on Software Engineering, 2008, Pages 683-692, http://portal.acm.org/citation.cfm?id=1368088.1368186

14. [Eren07] Eren, Evren; "WiMAX security architecture - Analysis and assessment," 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, 2007, Pages 673-677, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4488507

15. [Huang08] 15. Huang, Chin-Tser; Chang, J. Morris; "Responding to security issues in WiMAX networks," IT Professional, v 10, n 5, 2008, Pages 15-21, http://www.ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=4629835&isYear=

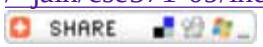
List of Acronymns

WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity
3G	Third Generation
MBWA	Mobile Broadband Wireless Access
M- Commerce	Mobile Commerce
MAC	message authentication codes
LAN	local area network
IEEE	Institute of Electrical and Electronics Engineers
DOCSIS	Data Over Cable Service Interface Specifications
BS	Base Station
SS	Subscriber Station
MS	Mobile Station
PKM	Privacy Key Management
PKMv1	Privacy Key Management Version 1
PKMv2	Privacy Key Management Version 2
RSA	Rivest Shamir Adleman
DES-CBC	Data Encryption Standard- Cipher Block Chaining
AES-CCM	Advanced Encryption Standard in Counter with CBC-MAC
AES	Advanced Encryption Standard

HMAC	Hashed Message Authentication Code
CMAC	Cipher-based Message Authentication Code
TEK	Traffic Encryption Key
SA	Security Association
AK	Authorization Key
EAP	Extensible Authentication Protocol
PHY	physical
WEP	Wired Equivalent Protection
DoS	Denial of Service
SSID	Service Set Identifier
MAC	Media Access Controller
LLC	Logical Link Control
UMTS	Universal mobile telephone system
HSDPA	high speed downlink packet access
GSM	global system for mobile communications
1x EV-DO	1 x evolution data optimized
TD-SCDMA	Time Division Synchronous CDMA

Last Modified: April 19, 2009.

This and other papers on latest advances in network security are available on line at http://www.cse.wustl.edu/~jain/cse571-09/index.html



Back to Raj Jain's Home Page