Global Information Assurance Certification Paper

GIAC Security Essentials Certification(GSEC)

Version 1.4b

An In-depth Look at Wireless WAN Security: Cellular Digital Packet Data Networks and their Security Issues

By Farid Hatefi

August 21st 2003

Abstract

Today's technology imposes restricted requirements on the corporate users for constant access to their corporate resources. Few instances of these resources are corporate e-mail or web services. Many of these corporate users are mobile, either traveling far or near the physical location of their office. Sometimes it is essential for these remote users to have immediate access to their company resources. Wireless WANs provide the most rapid way of accessing these resources. Cellular Digital Packet Data (CDPD) network is one of the most common wireless infrastructures that is being implemented nationwide today. A CDPD network is an overlay service on top of the existing AMPS (Advanced Mobile Phone Systems) cellular voice networks. A mobile unit in a CDPD network, also known, as Mobile End System (MES) is a computer with a CDPD modem. It has adequate capability for being mobile while connected to the CDPD network. The CDPD network, on the other hand, guaranties the packet delivery to the MES, while MES constantly changes its physical location. In order for an MES to have access to a CDPD network it must be authenticated either directly by Mobile Data Intermediate System's (MDIS) Mobile Home Function (MHF), while an MES' is in its home area or through MDIS's Mobile Serving Function (MSF) while roaming. After a successful authentication MES can access public networks such as internet. Although CDPD networks provide some level of encryption and authentication, the authentication scheme is unilateral, i.e. only MES are being authenticated by MHF. Neither MHF nor MSF will be authenticated by MES. In the meantime the traffic encryption is only available over the radio frequency. The lack of a bilateral authentication and partial route encryption are two of the major security concerns in CDPD networks. In this paper the security architecture of a CDPD network will be scrutinized and some possible solutions will be investigated.

1. Introduction to CDPD Network Infrastructure

1.1. CDPD Background

Today's technology imposes restricted requirements on the corporate users for constant access to the corporate resources. Few instances, of these resources are e-mail access or information service access to a centralized IS server. Many of these corporate users are mobile either traveling far or near the physical location of their office. In any case they don't have access to the corporate resources any more. It is sometimes essential for a user to have immediate access to this information. For instance law enforcement agents may need a rapid response for a background check of a suspect. Having the ability to access corporate resources on the fly with minimal wait time is one of the ideas behind CDPD wireless network. CDPD network infrastructure is an overlay service on the existing Advance Mobile Phone Systems. AMPS cellular voice structure (also known as first generation cellular networks). The worldwide availability of AMPS network makes the implementation of CDPD infrastructure much easier. The AMPS hardware technology, including antennas and base stations, is already installed in different geographical areas [15]. There is no need for major

hardware installations or new radio frequency re-assignment, e.g. frequency channels. The CDPD standard took into consideration these facts and it is build upon the AMPS resources availability. However, This does not mean that CDPD is another diversion of AMPS technology. In contrary, it is an open air standard for data transmission over the voice channels [1].

CDPD shares the same radio frequency as the AMPS voice channel. However, it does not cause any interference with the voice communication channels. This is accomplished by using a channel-hopping algorithm. If an incoming voice call is assigned to the same channel that is already being used by data, it causes the data transmission hops to the next available voice channel. Such mechanism ensures that neither the AMPS nor CDPD user will notice any interruption in an on going voice or data transmission. Fig 1 shows how CDPD data traffic can hop from one channel to another upon a new voice traffic .

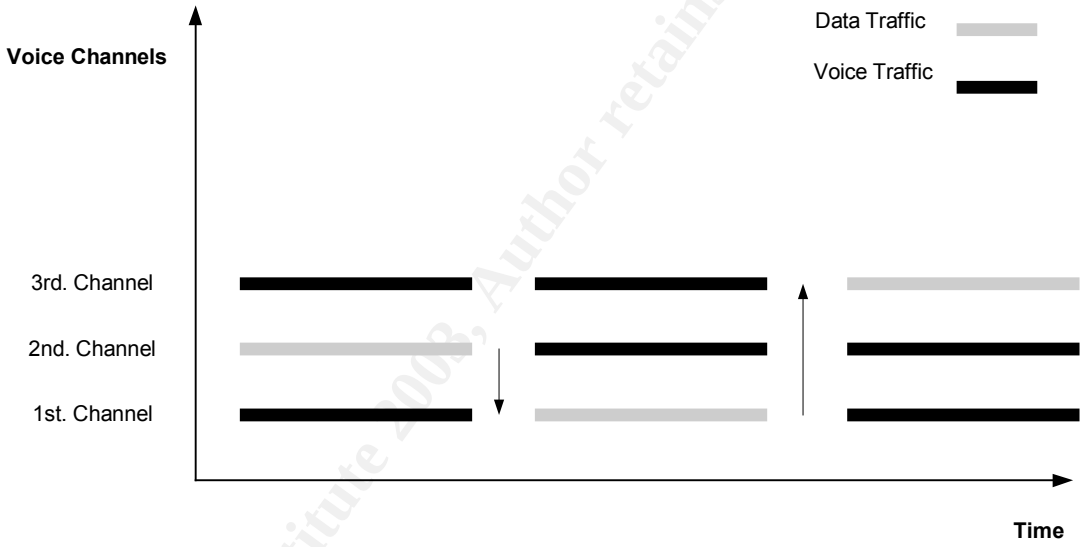

Fig. 1 Channel hopping in a CDPD network

1.2. CDPD Architecture

The CDPD standard defines three logical interfaces to the CDPD network where other components of the network can interact with either each other or the network to perform a specific function. Each one of these interfaces provide some services to other components of the CDPD network or vice versa. The A-interface, or Airlink, provides service through RF signal to the subscriber or Mobile End System (MES) [3]. The I-interface or inter service provider, provides service access points (SAP) to the other CDPD networks either nationwide or worldwide. The I-interface helps a user from one CDPD network to access another CDPD network resources and the E-interface, or External, provides an interface to external networks such as Internet. External application service providers can interface with CDPD end user through E-interface. Fig. 2 illustrates how these interfaces interact with other components of the network. [2]. There are several major components in a typical CDPD network. All these components

work together through A, E and I-interface [1,2]. In the next section these components will be explained in more detail.

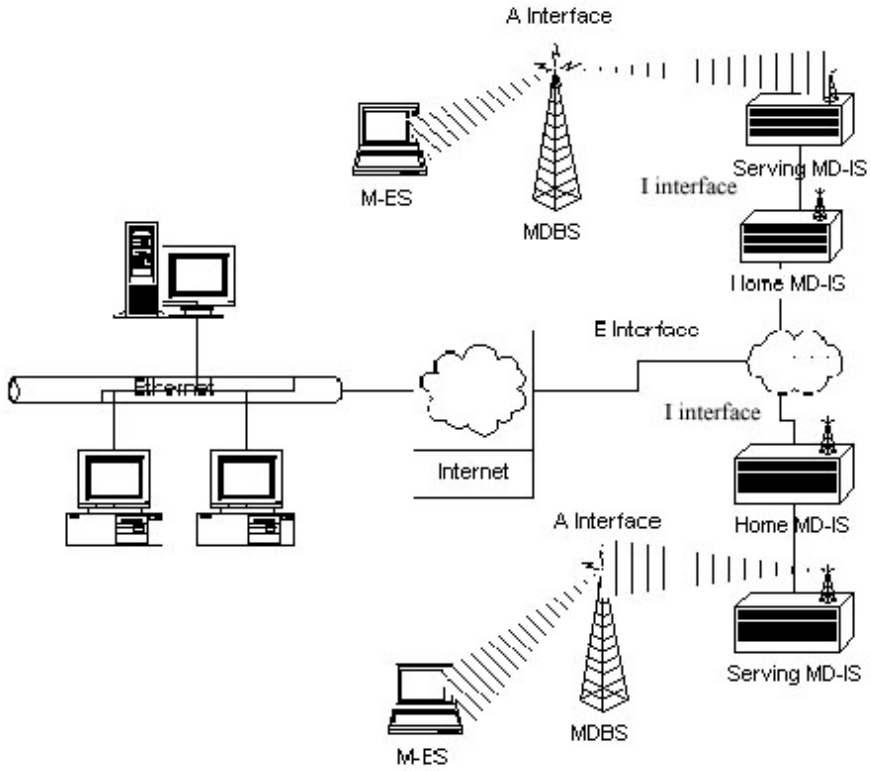

Fig.2 Interaction between different components of CDPD network

1.3. CDPD network components

1.3.1. Mobile end system (MES)

The mobile unit, also known as Mobile End System (MES) is an independent network component, which helps a network end user to have access to CDPD network [15]. Usually it is in a form of a specialized modem with a small footprint that can be used by a computer system for wireless access to CDPD network. MES communicates through the airlink with other network components. The CDPD network, on the other hand, guaranties the packet delivery to the MES. Providing such services by the network it is required to identify each individual M-ES in different locations. Mobile end systems use protocols defined up to OSI layer 3 [2,8], which makes MES capable of having an IP address. This method uniquely identifies each individual MES. This address combined with network id creates an identifier known as Network Entity Identifier that will be used during MES authentication process [2]. Internally, MES can be decomposed into three sub-components. Mobile application subsystem (MAS) includes all the components that are independent of the CDPD environment, e.g. software application and transport level software. Next, is subscriber unit (SU), which establishes and maintains communication with CDPD network. Finally, the

subscriber identity module (SIM). The SIM module is a database holding authentication and credential identities of a subscriber unit. SIM unit may or may not be a separable module. In case it is removable, the subscriber must carry the SIM module with the MES all the time in the form of a smart card [3].

1.3.2. Mobile database station (MDBS)

Mobile Data Base Station (MDBS) performs two functions. First, it is a device that arbitrates the activities on a channel that it manages. In a CDPD network much like the Ethernet, an RF channel is shared between several MES. In this case MDBS is an arbitrator in CDPD MAC scheme, also known as digital sense multiple access. Upon successful reception of bit stream it relays everything back to mobile data intermediate system. Second, MDBS may act as a bridge between MES and CDPD network. It communicates with all MES at one end and modulates data bits into RF signal and at the other end it demodulates RF signal into data bit stream [2,8].

1.3.3. Intermediate system (IS)

Intermediate System is a physical device responsible for routing and forwarding packets either using a Connectionless Network Protocol (CLNP) or Internet Protocol (IP) [2, 8]. CLNP is being used for routing datagrams between Mobile Data Intermediate Systems. However, IP can be used for forwarding and routing of datagrams between MDIS and MES. Other functions of IS are route calculation, fragmentation and congestion mitigation. In other words IS is a multi-protocol router.

1.3.4. Mobile data intermediate system (MDIS)

MDIS is responsible for routing functions based on the MES location [1,2,15]. It employs two different routing functions: Mobile Home Function (MHF) and Mobile Serving Function (MSF), which provide network services to MES regardless of its location. The idea behind the MHF is that each MES logically belong to a home area managed by home MDIS. The MHF keeps track of all of its MES community, either when they are in the home area or a in serving area while roaming. When MES are roaming the packets that are addressed to them will be forwarded to the MSF in each serving area. On the other hand the MSF of an MDIS acting as a routing function for the visiting MES and it provides the necessary services for those MES. During the MES registration the MSF forwards all the registration requests to home MDIS's MHF module.[1,3].

1.3.5. Fixed end system (F-ES)

FES is any system that is not mobile. It may be external or internal to the CDPD networks. The external F-ES may be located on any network anywhere in the world connected over a landline. For instance some of the external FES are the hosts that mobile end users connect to send email or accessing some web pages. Internal FES can be used by CDPD service providers to operate administrative services on the network[1,2,].

2. Problem definitions

2.1. Security handling in CDPD networks

In contrast to many other network protocols, CDPD specifications took into consideration the potential security issues [13] and it supports a set of primary security functions over the air link. These functions are:

1- Confidentiality of the data link, after determining a secret key all the traffic between the MES and MD-IS are encrypted in both ways [6,14,15]
2- Key management. The encryption algorithm guaranties the message privacy over the A interface. The key exchange and management is based on Diffie-Hellman [4,5] algorithm.
3- MES authentication. The MHF module of the home MDIS authenticates the MES based on a shared historical record (SHR) and NEI. SHR is a tuple of two numbers: a 16 bit authentication sequence number (ASN) and a 64 bit authentication random number (ARN)[2,3,6].

2.2. Encryption and authentication in CDPD networks

During MES registration process and while it is roaming through Mobile Network Registration Protocol (MNRP) MES requests for a temporary network identification number (TEI) from MSF module of the serving MDIS. In response the serving MDIS assigns a TEI to the MES and establishes a link. After the assignment of TEI the serving MDIS initiates a key exchange algorithm. The key management is based on Diffie and Hellman [3] key exchange procedure. The key exchange procedure is initiated by sending a MDIS key exchange (IKE) datagram also known as protocol data unit (PDU) to MES. The IKE PDU contains a triplet of:

$$(a, p, a^y \bmod p)$$

Where *a* is a base number and *p* is modulus number. The *y* quantity is a secret number to the serving MDIS. Upon receiving IKE request the MES creates another secret quantity *x* and sends MES key exchange (EKE) PDU to the serving MDIS. EKE PDU contains the following pieces of information

$$(a^x \bmod p)$$

Upon receiving this information both M-ES and MD-IS generate the following shared quantity:

$$(a^{x.y} \bmod p)$$

After computing this shared quantity both MES and serving MDIS derive two secret keys *k1 and k0*, where *k0* at MES is the same as *k1* at MDIS. Due to this property the encryption key at one end is the decryption key at the other end. After this phase all the data will be encrypted between the MES and the serving MDIS. The next step after providing confidentiality is the authentication phase, which must be done by the home MDIS. MES initiates the authentication phase by sending its encrypted credentials tuple (NEI, SHR) to the serving MDIS in the form of end system hello (ESH) PDU. Serving MDIS decrypt the ESH PDU and extracts the NEI and SHR and forms another PDU known as redirect request (RDR) and sends this PDU to the home MDIS. Upon receiving this information

the home MDIS authenticates MES by the credentials it has in its database. If the MES passes the authentication phase at the home MDIS, then the MHF constructs another PDU known as redirect confirmed (RDC) and includes a new SHR in that message. This new SHR contains a new Authentication Random Number (ARN) and incremented Authentication Sequence Number (ASN). Upon receiving RDC PDU at the serving MDIS, the new SHR will be extracted and encrypted and will be placed in a new PDU knows intermediate system conform (ISC) and will be sent to the visiting M-ES [1,2,3]

Fig. 3 illustrates all the steps that take place in encryption and authentication procedure in a CDPD network. It is important to notice that there is no encryption process between MSF and MSH. The connection between the serving MD-IS to the home MD-IS can be any leased terrestrial line, e.g. T1, Frame relay, multiple ISDN lines [6,7].

STEP	M-ES		MSF		MHF
1		TEI REQ. →			
2		← TEI Assigned			
3		← $a, p, a^y \bmod p$ IKE			
4		→ $a^x \bmod p$ EKE			
5	$a^{xy} \bmod p$	Shared Secret Quantity	$a^{xy} \bmod p$		
6		ESH <NEI,SHR> → Encrypted Message	Decrypt	RDR <NEI,SHR> → Clear Text	M-ES Authentication
7		ISC <NEI,SHR> ← Encrypted Message	Encrypt	RDC <NEI,SHR> ←	

Fig. 3 Required steps for M-ES authentication and message encryption

2.3. Security loopholes in CDPD network

CDPD specs is designed so that all MES can be authenticated by home MDIS [13]. Besides, the traffic on the A-interface is also encrypted and privacy of the messages between the MES and serving MDIS is provided by the MSF. However, as it is illustrated in Fig. 3, CDPD network does not provide any bilateral authentication between all parties. For instance, neither MES authenticates the MSF nor MSF authenticates MES. In other words, there is no bilateral authentication process between the visiting MES and serving MDIS. The provided security in CDPD networks blocks all the static attacks on the A-interface, but this security mechanism does not protect the user from dynamic attacks. The cost of dynamic attack are very high, but if the value of data that can be snooped off the A-interface is higher than the cost of the attack then the dynamic attack is highly probable. In another words if there is vulnerability in a system and also there is a threat the risk will be high. In CDPD network a

dynamic attack can be initiated by masquerading the serving MDIS. A disguised serving MDIS must over power the real serving MDIS RF signal strength. When the visiting MES observes an acceptable received signal strength indication it will participate in the handshake and key exchange procedure with the disguised serving MDIS. Upon, accepting the shared secret parameter from the fraudulent entity and calculating the encryption/decryption secret keys, the real MES reveals its NEI and SHR to the wrong MDIS. At this point the disguised entity not only have full access to the CDPD network, but form that time the real MES will be denied by the home MDIS the next time it tries to access the network. This is due to the lack of knowledge of the latest SHR by the real MES, which will be altered each time by home MDIS. The only entity that has the full knowledge about the updated SHR is the fraudulent MDIS, which now acts as the legitimate MES [13]. The end result of such attack is denial of service to the legitimate MES.

Another security problem with CDPD network raises when an attacker snoops the traffic between the serving and home MD-IS [10,6,13]. As it is being illustrated in Fig. 3, all the traffics between MSF and MHF are exchanged on the terrestrial line. There is no encryption or authentication mechanism between these two entities. The RDR and RDC are exchanged in clear text. It is easy to snoop the MES's NEI, and the latest ASN and ARN, or in another words the SHR. Some CDPD service providers today offer a private network to their customers in order to prevent such attack. They restrict their end user NEIs to access the Internet so they are only confined within the CDPD network.

In the following section two possible security mechanisms are being investigated that can authenticate and protect all the entities that are involved in the CDPD network. Both methods provide bilateral end-to end authentication as well as a strong message encryption [6,11].

3. Solutions for CDPD security issues

3.1. Basic bilateral authentication method

In the protocol that is proposed in [6] both MES and MSF are being authenticated by MHF and MHF itself will be authenticated by MES and MSF. The protocol consists of 4 steps. In the first step MES uses a shared non secret value known as S_{HM} or a nonce (use only once), which is created by MHF. In order to initiate the secure communication the MSF must send its ID (ID_S). Upon receiving the TEI in response, MES sends a message to MHF. The message, T_{MH}, contains of two parts, a nonce challenge value R_{MH} generated by MES and an encrypted payload consisting of S_{HM}, R_{MH}, and ID_S. This encrypted payload can be decrypted by MHF based on the assumption that the encryption and decryption keys have already been distributed between MES and MHF. This message will be routed to MSF, where the message itself will be used as a payload of a relay message to MHF by MSF. In the second step, upon receiving this message, MSF creates another message T_{SH}, and send it to MHF. This message consists of three parts, the received message from MES, i.e. T_{MH}, a nonce challenge value

R_{SH} created by MSF, and an encrypted payload, which consists of the encrypted payload of T_{MH}, R_{SH}, and MES's ID (ID_M). This encrypted payload can be decrypted by MHF based on the assumption that the encryption and decryption keys have already been distributed between MSF and MHF.

In the third step, upon receiving T_{SH}, MHF extracts T_{MH} and decrypts both T_{MH} and T_{SH} encrypted payloads. After validating S_{HM} value, which was sent by MES, MHF creates a new shared value for MES, known as S'_{HM}. This value will be used in a reply message, T_{HS}, to MSF. T_{HS} consists of three parts, S'_{HM}, T'_{HM}, which is an encrypted payload, consisting of the response to MES's initial nonce challenge value, R_{MH}, S'_{HM}, and a verified ID_S. The third part of T_{HS} is another encrypted payload, T'_{HS}. This part of the message consists of the response to MSF's initial nonce challenge value, R_{SH}, T'_{HM}, and the verified ID_M. The encrypted payload of T_{HS} can be decrypted by MFF based on the assumption that the encryption and decryption keys have already been distributed between MSF and MHF.

Finally in the fourth step, upon receiving T_{SH}, MSF decrypts T'_{HS} and validates R_{SH} and also makes sure that ID_M has been verified by MHF. Through this mechanism MES can be authenticated by MSF. Next it extracts S'_{HM} and T'_{HM} and creates a new message, T_{HM}, which consists of S'_{HM} and T'_{HM} Finally T_{HM} will be sent to MES. When MES receives T_{HM}, it decrypts the encrypted payload, T'_{HM}, and validates R_{MH} and also makes sure that ID_S has been verified by MHF. Through this mechanism MSF will be authenticated by MES.

3.3. Enhanced bilateral authentication method

In another proposed solution in [11] a PKI infrastructure is being used for enhancing the authentication and encryption operations in a CDPD network. Turning on the MES initiates the communication between MES and MSF by sending a TEI PDU request. In return the MSF sends a TEI, its certificate (issued by a trusted CA [CA digitally signs this certificate with its private key]), and an intermediate system challenge number (ICN) to the visiting MES. Upon receiving TEI PDU, the MES uses the CA's public key to confirm the CA's digital signature. After confirming it MES extracts the MSF's public key from the certificate and then generates two random prime numbers known as master key (MK) and end system challenge number (ECN). After creating ECN, the MES uses MK to create two secret keys known as read and write keys, which are used in RC4 symmetric cryptography algorithm. Later on, the MSF performs the same type of procedure and creates similar keys. It is needless to mention that the MES read key is the same as MSF's write key. Next, MES uses the write key and encrypts the ICN and then creates a PDU consisting of the encrypted ICN, ECN and MK and encrypts the whole PDU with the MSF's public key and sends the PDU back to MSF. Upon receiving this tuple MSF uses its own private key and decrypts the data and extracts the MK and ECN and encrypted ICN. At this stage MSF use the same method that MES used and creates two secret keys based on the MK (read and write secret keys). Next, MSF uses the read key and decrypts the

encrypted ICN and confirms that this is the same ICN that itself has created before. This insures that the MK is issued by the authentic MES who requested the connection. After confirming the ICN, the serving MDIS uses its write key and encrypts the ECN and sends it back to the MES. Upon receiving this message the MES uses its read key and decrypts the message and reconfirms the ECN. This insures that the MSF is the authentic party who issued the TEI. At this point the A-interface (air channel) is secure between the MES and MSF and MES may send the ESH PDU.

A similar type of security handshake can be used for securing the channel between MSF and MFH. If additional layer of security is needed it is possible to have certificate for both entities involved in the communication, e.g. MES sends its certificate to MSF for higher level of authentication. However, this is not necessary because MES will be authenticated by the MHF anyway, which is one of the requirements in CDPD specifications.

This solution protects MES against masquerading MSF. In case a fraudulent MSF, who tries to deceive its authenticity by sending a wrong certificate, the MES will realize that as soon is it reconfirms the CA's digital signature. It is impossible to counterfeit the CA's digital signature because the digital signature is the CA's encrypted MD-5 [9] hash value of the contents of the certificate. CA uses its own RSA private key to encrypt the hash value. Theoretically, the only entity who knows the CA's private key is CA's itself. Without the knowledge of the CA's private key the fraudulent MSF must use a different pair of public/private key for encryption. If this happens the confirmation of the CA's digital signature fails by the MES. If the fraudulent MSF captures the previous sessions' packets during the handshake and tries to replay them, MES will accept the digital signature but the masqueraded MSF wouldn't be able to extract the MK from MES reply message. This causes the fraudulent MSF not being able to create the read/write session's keys [11].

This solution also protects MSF and MHF against static attacks during the exchange of RDR and RDC. After, both parties are authenticated they are the only entities who know the session read/write key. This will creates a fully secure channel between them. In case an eavesdropper tries to capture the ongoing packet between MSF and MHF, everything would be encrypted and meaningless.

5. Conclusion

The wireless WAN networks are the most efficient and the fasted deployment method for accessing corporate recourses, where the twisted pair is not available. Wireless WAN is an adopted technology by road worriers. Cellular Digital Packet Data networks (CDPD) are one of the implementations of wireless WANs. CDPD standard provides some level of privacy and security in the means of end user authentication and traffic encryption over the RF signal. However, there are two major security issues in CDPD networks. First, it lacks a bilateral

authentication mechanism. The mobile end systems are the only entities in the CDPD network that are being authenticated. The current bilateral authentication scheme does not protect the mobile end systems from sending their secret credentials to unauthorized mobile serving station. The second issue in CDPD networks is the clear text traffic transmission from the mobile serving station to mobile home stations. Adding extra security layers such as using digital certificated or additional authentication methods to the current CDPD infrastructure can solve these two issues.

References

1. J. Agusta, T. Russel 1997 *CDPD Cellular Digital Packet Data Standards and Technology*. New York, McGraw-Hill.

2. M. Sreetharan, R. Kumar 1996 *Cellular Digital Packet Data.* Boston, Artech House.

3. M. Banan, et al 1996 *Internetwork Mobility The CDPD Approach*. NJ, Prentice-Hall.

4. W. Stallings 1993. *SNMP, SNMPv2, and CMIP The Practical Guide to Network Management Standards*. New Yourk: Addison Wesley.

5. D. Russell and G. T. Gangemi 1992. *Computer Security Basics*. California: O'Reilly & Associates.

6. Y. Frankel 1997 *Security Issues in a CDPD Wireless Network,* http://swig.stanford.edu/pub/summaries/wireless/security_cdpd.html.

7. D. Smith, et al 1995 *Trails of Wireless Secure Electronic Mail*. IEEE Personal Communication.

8. D. Pharr, et al..2001.. *The Growing Acceptance of Cellular Digital Packet Data as a Communication Method for Oil and Gas Telemetry* http://www.bandwidthmarket.com/resources/speeches/sat/pharr/paper.doc

9. Rivest 1992 *The MD-5 Message-Digest Algorithm.* Request for Comments 1321, Internet Activity Board.

10. MobileInfo 2001 *Wireless and Mobile Computing Security,* http://www.mobileinfo.com/Security/problems.htm

11. F. Hatefi et al 2001 *Prospect of Secure Real-Time Video Transmission over CDPD network,* NSF Workshop on an Infrastructure for Mobile and Wireless Systems

12. SierraWireless 2002 *Wireless Security: Data Security in Wireless Networks* http://www.sierrawireless.com/news/docs/2130223_Wireless_Security.pdf,

13. Lightweight and Efficient Application Protocols (LEAP) Forum 2000 *CDPD Security* http://www.leapforum.org/published/internetworkMobility/split/node97.html

14. S. Issacson 1997 *CDPD Security,* http://www.refreq.com/downloads/cdpdsec.pdf

15. J. Geier 2000 *CDPD Concepts,*
http://www.wireless-nets.com/articles/whitepaper_cdpd.htm