Data Security In Wireless Networks

ABSTRACT: -

Wireless Wide Area Networks (WAN) are a popular method of wirelessly accessing data over the Internet. A major concern for many corporate users of wireless WANs is data security and how to protect data that is transmitted over these wireless networks.

There are many features of these wireless networks, which provide user and data security. This paper discusses the security features for CDPD, CDMA, and GPRS networks, as well as an introduction to virtual private networks (VPN) and how these applications can be used to enhance the overall security of data on wireless networks.

For each of the technologies presented in this paper, a brief overview of the wireless network is given, followed by a discussion of each of the features of that network that contribute to the overall security of the network.

CONTENTS

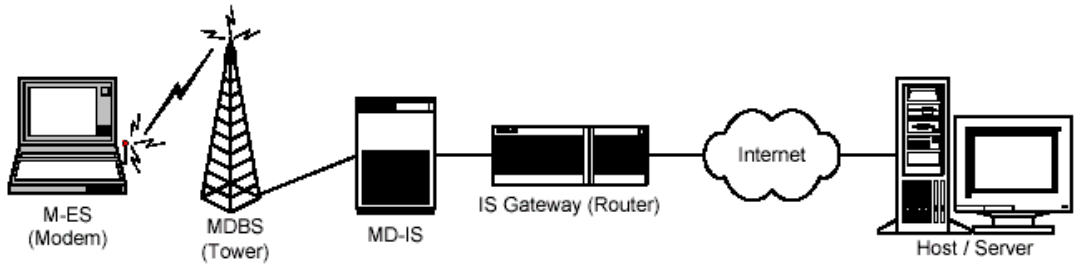
1. CELLULAR DIGITAL PACKET DATA (CDPD)

1.1 INTRODUCTION: -

CDPD is a secure, proven, and reliable protocol that has been used for several years by law enforcement, public safety, and mobile professionals to securely access critical, private information. CDPD has several features to enhance the security of the mobile end user's data and these are discussed below.

1.2 OPERATION OF CDPD: -

A brief overview of the operation of the CDPD network is as follows: A wireless modem (or Mobile End System—M-ES) communicates by radio with the Mobile Data Base Station (MDBS). The MDBS transfers this data by landline and microwave to the Mobile Data Intermediate Systems (MD-IS), which processes and sends the information, by Intermediate System gateways (routers), to the appropriate destination.



CDPD network structure

The modem refers to the wireless modem in the CDPD network. The MDBS is the cellular tower serving a specific geographical area. The MD-IS is a computer device that serves as the control point for CDPD in a specific region (usually covering several MDBSs).

1.3 FEATURES OF CDPD: -

1.3.1 Subscriber equipment security: -

Each modem on a CDPD network is identified by a unique Network Entity Identifier (NEI) assigned by the CDPD carrier, which gives the CDPD modem an Internet Protocol (IP) address visible to the rest of the Internet.

Each modem device also has an Equipment Identifier (EID), which is a fixed number, unique to that modem. No two devices in CDPD can have the same EID. When a user signs up for service with a CDPD service provider, the user gives the EID to the service provider. This EID then becomes part of the Subscriber Directory Profile that the service provider maintains for each subscriber. A subscriber, who replaces their modem with a newer one, must report the new EID to the CDPD carrier. Until the carrier assigns this new EID to the subscriber's NEI, the new modem will not work on the CDPD network.

1.3.2 Authentication: -

In order to prevent piracy and "cloning" of CDPD devices, and thus fraudulent network use and billing, the CDPD standard provides sophisticated mechanisms for NEI authentication and verification. It can confirm that only the authorized modem, with the assigned NEI, is using that NEI.

Using the Diffie-Hellman Electronic Key Exchange mechanism, the authentication process uses three numbers: the NEI, the Authentication Sequence Number (ASN), and the Authentication Random Number (ARN),

which together form the credentials of that modem. Although a subscriber can determine their NEI, they cannot obtain the ASN or ARN.

When a subscriber's modem performs the authentication procedure during network registration, the MD-IS checks these credentials against the current values of the ASN and ARN. If the stored values do not match those provided by the modem, then the modem is not allowed to connect.

From time to time, the MD-IS generates a new (random) value for the ARN, and it then increments the ASN by one. The MD-IS delivers the new ARN to the modem in the final step of the encrypted registration process. The modem stores this ARN internally and increments its local ASN by one.

1.3.3 Airlink encryption: -

CDPD is a public wireless data communications service that could be susceptible to eavesdropping, all data (except broadcast messages) transferred between the modem and the MD-IS is encrypted by CDPD's Encryption Services. This encryption uses RSA algorithms and is managed by the Sub-network Dependent Convergence Protocol (SNDCP), which provides compression, encryption, and segmentation for data transferred over the network. It takes standard Internet packets, compresses their header information, segments them for transfer over the CDPD network, and encrypts the segments.

1.3.4 Network security: -

On a CDPD network, data is encrypted from the modem to the MD-IS. Beyond the MD-IS data is generally not encrypted, much as general Internet traffic remains unencrypted unless the end user provides it. If

necessary, the carrier or end user may encrypt data traveling over other portions of the network using other mechanisms.

1.3.5 Private networks: -

For CDPD customers requiring additional security, many service providers offer an additional service, which restricts the Internet access of the user's NEIs to form a private network. This means that when data is sent from the modem to the MD-IS, the traffic is not then routed onto the public Internet, but is restricted to within the service providers network and routed directly to the customer's host computer. This means that the data is never publicly available on the Internet, enhancing privacy and security even further.

2. CODE DIVISION MULTIPLE ACCESS (CDMA)

2.1 INTRODUCTION: -

CDMA is a recently patented technology but dates back to before World War II, when inventors patented a way of sending signals over different radio frequencies using random patterns to control torpedoes. The idea was later used to secure communications for the U.S. government during the Cuban Missile Crisis. The U.S. military declassified the technology in the 1980's and it has now become CDMA cellular technology.

Spread-spectrum technology works by taking the conversations or data and attaching a code (known only to the sender and receiver) to it. The coded information is then split into packets and transmitted along with multiple other conversations or data packets over the network. The receiver

then reassembles and decodes the data. This result in extremely secure transmissions, because the coded information is spread over the same bandwidth, resulting in trillions of possible combinations of coded messages.

2.2 Spread spectrum: -

CDMA is a "spread spectrum" technology, which means that the user data is assigned a unique code and then "spread" over a greater bandwidth than the original signal. The data bits of each call are then transmitted in combination with the data bits of all the other calls in the cell. At the receiving end, the digital codes are separated from the data, leaving only the original information that was sent.

Spread spectrum technology was traditionally used in military applications. It was secure enough for military applications, because the signal is difficult to identify, jam, or interfere with, due to the wide bandwidth of a spread spectrum signal. A spread spectrum signal is very hard to detect, and appears as nothing more than a slight rise in the background noise. Other technologies have the signal power concentrated in a narrower band and are easier to detect.

CDMA phone calls are secure from casual eavesdroppers since a radio receiver would not be able to pick individual digital conversations out of the overall RF radiation in a frequency band. Even if eavesdroppers intercepted a CDMA signal it would be almost impossible to decipher.

2.3 Features of CDMA

2.3.1 *Lock codes*: -

A unique feature of CDMA handsets and modems is a unique code, which acts as a network security lock. If your phone or modem is lost or stolen, it cannot be used on another CDMA network.

2.3.2 *ESN and MIN numbers*: -

Each mobile device on a CDMA network has a unique Electronic Serial Number (ESN) and Mobile Identification Number (MIN) associated with it. The network is able to compare the ESN/MIN combination each time a user connects to the network, and so increase security by not allowing cloned or unauthorized devices onto the network.

2.3.3 *A-keys*: -

An A-key is a secret 64-bit number used during authentication and encryption on the network. It is never revealed to the end user and is never transmitted over the air. The A-Key is stored in the memory on the phone or modem and is only ever known to the mobile device and Authentication Center on the network.

2.3.4 *Authentication*: -

Authentication of a mobile device on the network is enabled by the base station, which sends a 32-bit random number to the mobile device. The

mobile device then uses a combination of the A-key, ESN, MIN, and the random number to compute an authentication signature, which is returned to the base station. The A-key values are also stored on the network in the Authentication Center (AC), so the base station can also calculate the authentication signature.

Upon receipt of a Registration message, phone call or data transmission, the network compares the Authentication signature sent by the mobile device to the one that is stored on the network. If the two match, the mobile device is allowed onto the network.

2.3.5 *Authentication challenge*: -

The authentication challenge is another mechanism that the base station can use to authenticate the mobile device at any time. The base station sends an authentication challenge to the mobile device, which then calculates its authentication signature and sends it to the base station that issued the authentication challenge. The base station compares the authentication signature received from the mobile to the one stored in the Authentication Center to determine the mobile device's validity on the network.

2.3.6 *Voice privacy*: -

On a CDMA network, voice privacy is provided on both the forward and reverse channels by a pseudo-random sequence of bits, known to the mobile device and base station. Voice privacy makes it difficult to listen to the channel and so it protects not only voice traffic, but any data or signaling information that is transmitted as well.

2.3.7 *Signaling Message Encryption*: -

Signaling Message Encryption is similar to voice privacy in that it encrypts the signal messages sent over the network. A key generated by the mobile and the base station during the call setup does this encryption.

2.4 Smart card technology: -

A recent development is that CDMA technology now allows for the use of smart cards on CDMA-based networks. The R-UIM (Removable User Identity Module) is similar to the SIM (Subscriber Identity Module) cards used on GSM and GPRS networks.

Advantages of a R-UIM include:

- **Easier replacement and exchange of handsets of mobile devices**
- **The Ability to move user profiles and personal data between devices**
- **Secure network connection**
- **Potential for cross-standard roaming capabilities**

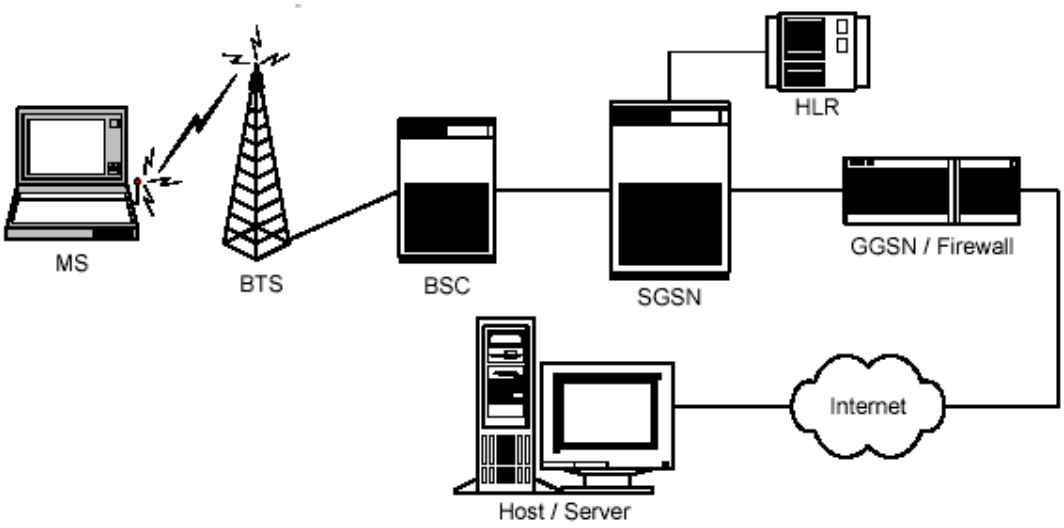
3. GENERAL PACKET RADIO SERVICE (GPRS)

3.1 Introduction: -

GPRS is based on GSM technology; the most widely used global wireless technology. The security architecture is therefore a solid, proven technology. GPRS networks have many security features that ensure protection of user identities, subscriber equipment, and user data.

3.2 Operation of GPRS: -

A Brief overview of the operation of the GPRS network is as follows: A wireless modem (or Mobile Station—MS) communicates via a radio link with the Base Transceiver Subsystem (BTS). The BTS transfers this data to a Base Station Controller (BSC), which separates voice and data traffic. Data is then transferred to the Serving GPRS Support Node (SGSN), which authenticates the MS, and then on to the Gateway GPRS Support Node (GGSN), which acts as the gateway to external networks (such as the Internet or the service provider's network). The data is then sent, via routers, to the appropriate destination.



3.3 Features of GPRS: -

3.3.1 *Subscriber security*: -

One of the security features on GPRS networks is the Subscriber Identity Module (SIM) Card. This is a small electronic card that fits into the Mobile Station (MS) phone or data device. All of the user's network account information is contained on this SIM Card (as well as data such as personal phone book entries). Without having a valid SIM card in the MS, it is not

possible for the device to access the GSM/GPRS network. The SIM card can also be locked with a user-defined password (Personal Identification Number or PIN) for additional security.

3.3.2 *Authentication*: -

The SGSN controls the ciphering (encryption) and authentication of the MS. The GPRS authentication and ciphering are similar to GSM networks, with a few modifications.

When the GPRS subscriber first connects to the network, the SGSN authenticates the MS using data contained in the SIM card. It compares this information with the authentication data from a database on the network, known as the Home Location Register (HLR). During this authentication process, a non-predictable random number is used to generate an authentication key as part of the authentication process, further enhancing security. Although used in the authentication process, this authentication key is never transmitted over any part of the network.

3.3.3 *Encryption*: -

All data transferred between the MS and the SGSN is encrypted on GPRS networks. During the authentication process, it can also be decided whether ciphering (encryption) is to be used. Encryption is then established by the generation of an encryption key. All data communication between the MS and SGSN is encrypted using the GPRS Encryption Algorithm (GEA) a version of the A5 algorithm used on GSM networks.

3.3.4 *Network security*: -

The point where the service provider's GPRS network connects to the Internet is the GGSN. At this point, GPRS networks have a GGSN firewall that allows user data to pass outside of the GPRS network, while at the same time blocking attempts to connect to the MS from the outside. The GGSN firewall protects the MS from attacks coming from outside the GPRS network, while the SGSN protects the user against other MS's.

Network address translation is also done by the GGSN, thus hiding the private IP addresses of the MS from users outside of the GPRS network.

3.3.5 *Additional encryption*: -

Data is generally not encrypted beyond the GGSN, much as general Internet traffic remains unencrypted unless the end user provides it. If necessary, the carrier or end user may encrypt data traveling over other portions of the network using other mechanisms.

An example is to create a VPN between the GGSN and the corporate intranet being accessed. The traffic is encrypted at a VPN server and is transported in encrypted form over the Internet to access the corporate intranet.

Another option would be a dedicated connection or leased line, which would provide additional security and constant bandwidth, from the GGSN to the corporate intranet, completely bypassing the Internet.

3.3.6 *Private APN*: -

Many GPRS service providers offer a separate Access Point Name (APN) for secure access. A standard APN will not encrypt traffic beyond the GGSN, whereas a private APN will encrypt the traffic, using one of the methods described above, depending on the configuration of the network.

4. VIRTUAL PRIVATE NETWORKS (VPN)

4.1 INTRODUCTION: -

Even though each of the wireless networks discussed provides a high level of security to prevent eavesdropping or interception of data, many users require an end-to-end security solution. This would protect data integrity at all points from the mobile user's computer to the host network.

For customers wanting additional security, an end-to-end VPN connection provides the best security. Traffic is encrypted at the VPN client on the mobile device and is decrypted at the corporate VPN server. Thus, all traffic is encrypted as it travels through the whole connection. Authentication is also in the hands of the subscriber's organization.

4.2 VPN overview: -

An IP-based VPN (that is, not a frame relay or leased line VPN) allows you to temporarily create or join a private network across an existing public network by creating an encrypted tunnel between two hosts. This tunnel allows you to securely transfer information and access remote resources. A

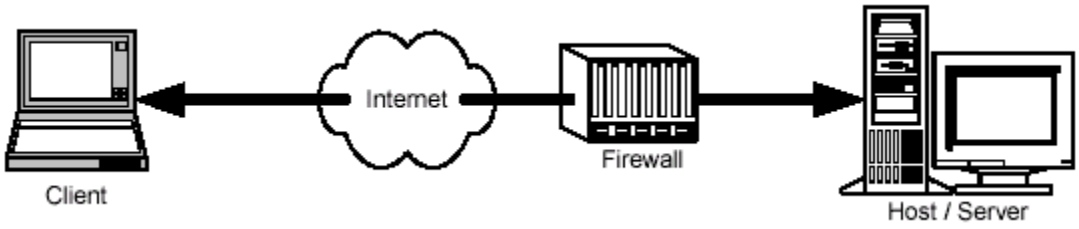
VPN has the benefits of being a secure method of transmitting data, while still being cost effective.

4.3 Example of a VPN connection: -

To connect to a corporate network, a user connects to their wireless service provider's network as usual. The user then initiates software on their mobile device, which requests a VPN tunnel to the VPN server on the corporate network. The VPN server authenticates the user and creates the secure VPN tunnel. The VPN software encrypts any data that the user sends over the wireless connection and the VPN server then decrypts the data and forwards it to the corporate network.

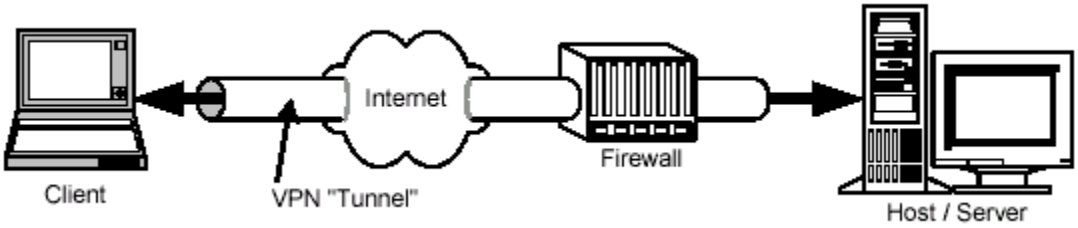
The VPN server encrypts data sent to the remote user before being sent over the wireless network and the VPN software on the user's computer then decrypts it.

Without a VPN connection, the connection is only protected on the wireless network, and may not be secured over the Internet.



Without a VPN

With a VPN connection, traffic is encrypted (or "tunneled") over the whole connection from the mobile user's computer to the host network.



With a VPN "tunnel"

4.4 VPN vendors: -

There are a number of companies that offer a variety of VPN solutions. Checkpoint, Cisco, Nortel, Intel, and Microsoft are all companies that provide popular VPN solutions.

Companies like Certicom and Net motion Wireless provide solutions that are optimized for wireless connections and mobile users.

4.5 Strengths of a VPN: -

A VPN is able to offer secure access to data and provides different levels of security that include tunneling, encryption, authentication, and authorization. VPNs allow remote users seamless, low-cost access to corporate networks, all over a secure connection.

VPNs have lower hardware, software, and network costs, which reduce the total cost of a secure a network. Operating costs are also lower, since there are no leased lines, or long-distance telephone charges for remote access. VPN infrastructure is easily adapted and expanded as an organization, and its networking requirements, grow. VPNs that utilize the Internet avoid increasing infrastructure costs by using existing infrastructure.

Because VPNs are standards-based, users can access a variety of applications or services and entire networks can be easily integrated with one another. A VPN is more flexible than a fixed network and can be reconfigured by changing software parameters, without changing the physical network.

5. Conclusion

There are many features of wireless WANs that provide user authentication and data security. These are intended to provide data protection within the carrier's network but do not extend to the Internet and beyond. When a VPN is used with these networks, it provides end-to-end security for all data sent over the Internet.

6.Bibliography

1. www.sirreawireless.com
2. www.bitpipe.com
3. www.itpapers.com
4. www.google.com
5. "Mobile communication" by Schilfer