Mobitex security issues

olleB - olle@toolcrypt.org

Introduction

The Mobitex wireless networking standard was developed jointly by Ericsson and the Swedish national telephone company nearly 30 years ago at a time when wireless networking was in its infancy. It specifies not just a wireless wide-area networking standard but extends to a hierarchal, centrally managed packet switched data network designed for national coverage. Since then it has undergone several major revisions, increasing wireless throughput and adding features such as power-saving and international roaming. According to the Mobitex Association[1] there are 30 networks operational on 5 different continents, two thirds of which are open commercial networks. This paper will attempt to shed some light on how Mobitex networks actually work focusing on the air interface and "security" features such as subscriber identification and access controls.

Previous work

Not much is known about Mobitex networks in the security community, despite the many business applications that use this technology. What little information exists is based on an anonymous Usenet posting made in 1997[2] detailing the reverse-engineering of the bit-scrambling and block-coding in the Mobitex air interface, basically describing OSI layer 1 of the Mobitex networking stack. This paper builds on that previous work and attempts to document the frame format of layer 2 (the ROSI protocol), a work that admittedly is far from complete. Parts of layer 3 will also be described, not in detail but to provide an understanding of the security challenges the Mobitex protocol stack presents.

The Mobitex network stack

The Mobitex networking stack roughly corresponds to OSI layers 1 through 4, although the official layer 4 protocols (MTP/1) were specified[3] several years after the initial Mobitex launch and seem to have gained little traction with the Mobitex application developer community.

Layer 1

The physical radio layer is 8kbaud GMSK with bit-scrambling as described in [2]. The link layer protocol is called ROSI and each frame is preceded by a frame header. The header contains the base station ID and 4 flag bits encoded as two octets with a (12,8) hamming code. If bit 2 in the flag field is set, then the frame header is a "roaming header" transmitted by base stations as a channel marker to aid mobile stations searching for an active channel. This "roaming header" is not followed by an actual ROSI frame. The ROSI frame is transmitted using one or more blocks of 18 data bytes + 16 bit CRC encoded using a (12,8) hamming code and interleaved as described in [2].

Layer 2

The first block in a frame contains the ROSI header where the recipient MAN address (or address of a network group), a 3-bit flag field, the 5-bit frame type and the frame length (by number of blocks) are specified. Byte 4 in the ROSI header is type specific but in most frame types contains a field specifying how many bytes are in the last block of the frame and a sequence number used for frame acknowledgment, see Fig. 1. Exceptions to this are the SVP, FRI and TST channel management frames which use byte 4 for other purposes.

The rest of the first block (bytes 6 through 17) can be considered the start of the frame payload data, the structure of which depends entirely on the frame type. The ROSI frame types are listed in table 1 where deprecated values associated with features present in the original (1200baud) Mobitex specification have been colored grey.

Fig. 1 The initial block of a ROSI frame

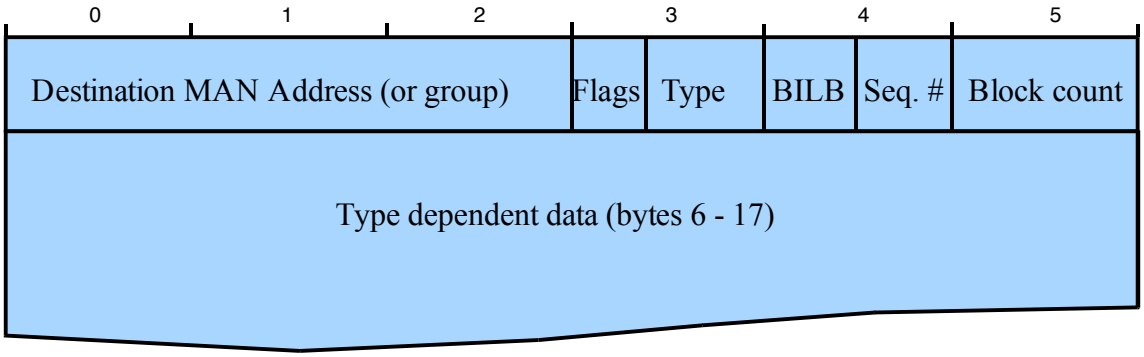

Table 1 ROSI frame types

Frame type	Value	Description
MRM	0x01	Mobitex packet (MPAK)
ACK	0x02	Acknowledgement
NACK	0x03	Negative Acknowledgement
REB	0x04	Request re-send of selected blocks
RES	0x05	Re-send of selected blocks
ABD	0x06	Access request for data traffic
ABT	0x07	Access request for voice traffic
ABL	0x08	Access request for emergency traffic
ATD	0x09	Access granted for data traffic
ATT	0x0a	Access granted for voice traffic
ATL	0x0b	Access granted for emergency traffic
BKD	0x0c	Change channel for data traffic
BKT	0x0d	Change channel for voice traffic
FRI	0x0e	Channel free marker
SVP	0x0f	Sweep frame (network parameters)
TST	0x10	Silence order (channel reservation)
AKT	0x11	Activity check
NAT	0x12	Access not granted for voice traffic
BBT	0x13	Change base station for voice traffic

The ROSI protocol uses a reserve-slotted ALOHA access mechanism, meaning the base station sends a FRI frame indicating it is ready to receive traffic from mobile stations in a number of time slots. Mobile stations can then choose a time slot at random and send a frame upstream. The base station can revoke the FRI status at any time by sending a silence order (TST) frame, for example to prevent interference with a mobile station already transmitting on the upstream channel. Should a mobile station need to send a large frame, such as an MRM frame containing a large data packet, it can reserve time on the upstream channel by sending an access request (ABD) frame with information about the size of the large frame.

Re-sends of missed or incompletely received frames are handled by positive or negative acknowledgement of received frames (ACK/NACK) and requests to repeat certain blocks of a particular frame (REB/RES). The sweep frame (SVP) is used by the base station to broadcast network parameters such as adjacent channels and signal threshold values. The activity check (AKT) frame is sent by a base station to determine if a mobile station is still active, the mobile station will send an acknowledgement (ACK) frame as a response.

Layer 3

The Mobitex packet switching network relays Mobitex packets or MPAKs. The MPAK is well documented in the open MIS document[4] available online from Mobitex Technology[5] who currently own the Mobitex specification. There are two classes of MPAK, the packet switched subscriber communications class (PSUBCOM) used to carry application data between subscribers, and the data terminal service communications class (DTESERV) which defines packet types used for network signaling between Mobitex terminals and Mobitex network nodes.

The MPAK header contains the sender MAN address, the destination MAN address, 8 bits of flags and the packet class and type encoded in 8 bits for a total of 8 bytes. Packet type-dependent data follows the header, unless the SENDLIST flag (bit 3) has been set in which case a 22 byte address list is inserted between the MPAK header and type-dependent data. Table 2 shows the different PSUBCOM class packet types that carry application data in the Mobitex packet switched network.

Table 2 PSUBCOM packet types

Packet type	Description
TEXT	Text formatted to be output on a printer or display at the terminal.
DATA	Arbitrary data of application-defined encoding.
STATUS	A one-byte status code, the meaning of which is defined by the application.
HPDATA	Protocol identified by an 8-bit ID. 0-127 assigned, 128-255 user/operator defined.
EXTPAK	Transparent data to be exchanged with an “external telecommunications network”.

Mobitex security issues

Several security issues with the Mobitex wireless protocol have been identified. These issues, concerning all aspects of security, are caused by the goals of the Mobitex designers who were much more concerned with problems such as naturally occurring radio interference and network performance than with any aspect of information security.

Confidentiality issues

The Velocita Wireless[6] "Mobitex System Overview" document explains in great detail how the Mobitex framing, error correction and interleaving works. Then it concludes:

> "Hence, eavesdropping on user data is a difficult task. One would require a great deal of experience, as well as sophisticated equipment to be able to break into each packet generation/transmission process."

The only part of the air-interface not described in sufficient detail in that document to be able to eavesdrop on user traffic is the bit-scrambling routine. This has been shown in [2] to be trivially reverse-engineered and the details had as such been publicly known for several years at the time of writing the Velocita document. This kind of misleading information from Mobitex network operators is not that uncommon. Many times Mobitex is touted as a "secure" network protocol when it was never designed with any other security than high availability in mind. To their credit, Velocita Wireless does go on to recommend that customers assess their security needs and implement application level security features such as encryption later in the same chapter.

Intercepting Mobitex user traffic by decoding individual Mobitex frame blocks has been done as early as 1997[2] but to the author's knowledge nobody has extended this work to decode the actual layer 1-3 Mobitex network traffic. The Toolcrypt.org Mobitex network monitor[8] project attempts to place full Mobitex protocol monitoring abilities in the hands of security professionals with little experience of wireless technology and using cheap, off the shelf radio equipment. By utilising the sophisticated A/D-converter of the average PC sound-card and feeding raw audio from an inexpensive commercial scanner into it, anyone can decode and monitor Mobitex networks in software running on a consumer PC.

Integrity and authentication issues

Since Mobitex was developed by the telecommunications industry, the subscriber identity features are similar to those used in mobile telephony at the time. But because this was before rampant toll-fraud in the 1G mobile telephony networks necessitated the use of strong identification, the subscriber identity mechanisms in Mobitex are rather weak.

The MAN address of a particular subscriber is tied to the ESN of the mobile terminal. This might have been enough had the designers invented some kind of challenge-response scheme, but the ESN is unfortunately just sent in DTESERV packets (ACTIVE, ROAM, ESNINFO, etc.) as an authenticating token. No protections against replay attacks are implemented. If the base station receives an invalid authentication token or the mobile station doesn't respond to ESN queries, the base station will send a "DIE" DTESERV packet to the mobile station. The mobile station should then immediately go off the air. Personal subscriptions that can be moved between different mobile terminals are protected by an 8 character password which is also sent in clear text when logging in.

Because of this weak authentication scheme, any terminal that can be monitored (i.e. attacker is within radio range) can also be impersonated at the attackers discretion (i.e. at any time in the future). The attacker may even force legitimate terminals to go off-air by spoofing base station traffic and sending a “DIE” DTESERV packet.

Mobitex packets do not contain any type of message authentication or integrity protection, making spoofing attacks even more simple. An attacker within base station coverage can send individual packets upstream that appear to be from another wireless terminal using that base station, effectively hijacking its “connection” without needing to authenticate to the base station at all. Clearly authentication needs to be addressed at the application layer by developers of Mobitex applications.

Availability issues

Most often when using the word “security” or “secure” in their marketing, Mobitex network operators are talking about the supposed high-availability of the Mobitex system. Unfortunately this high-availability goal of the design only manages to protect system traffic against temporary environmental interference and some equipment malfunctions. It is still trivial for a determined adversary to disrupt Mobitex communications either selectively or completely.

Normal wide-band jamming transmitters can for example be used to deny a Mobitex wireless terminal access to the network, a technique that could be used quite effectively against security alarm systems. Selective denial of service is also possible by spoofing base station traffic and getting a wireless terminal to “choose” your channel or simply drowning out the legitimate base station traffic with a sufficiently high-powered transmitter. Individual Mobitex terminals could then be forced off the network using the “security” features of the Mobitex protocol (DTESERV “DIE” packet, etc.).

Conclusions

The Mobitex wireless network is not secure and has large problems with its confidentiality, integrity and availability protections. In fact, Mobitex wireless networks provide no more protection against an attacker than an unencrypted IEEE802.11 “WiFi” network. Application developers and organisations relying on Mobitex wireless terminals for business applications should be made aware of these risks and start working on developing countermeasures at the application level.

Future work

Implementing a Mobitex wireless terminal and/or base station using software defined radio hardware such as the USRP[9] would be possible and presents an interesting path for further research of Mobitex wireless networking. Extending the MIS MPAK specification to include message authentication features and designing better subscriber authentication features to replace the ESN and password checks might also be a worthwhile exercise.

Bibliography

[1] http://www.mobitex.org/ - The Mobitex Association

[2] Message-ID: <332A0580.FB0@geocities.com> From arron5@geocities.com
Fri Mar 14 18:12:20 1997 Newsgroups: rec.radio.scanner Subject: Fun mobitex stuff

[3] Ericsson AB - Mobitex Transport Protocol 1 (MTP/1), Doc.no: 1914-FAY 107 417

[4] Ericsson AB - Mobitex Interface Specification – Open Version, Doc.no: 1551-CNH 160 013

[5] http://www.mobitex.com/ - Mobitex Technology AB

[6] http://www.velocitawireless.com/ - Velocita Wireless L.L.C.

[7] Velocita Wireless - Mobitex System Overview, Edition 1.2, 2005

[8] http://www.toolcrypt.org/index.html?mobitex

[9] The Universal Software Radio Peripheral, Ettus Research L.L.C. - http://www.ettus.com/