IEEE P802.11

Wireless Access Method and Physical Layer Specification

MAC Subgroup Minutes
January, 1995 Interim Meeting

Minutes take by:

Michael Fischer
Digital Ocean, Inc.
4242–3 Medical Drive
San Antonio, TX 78229
Telephone: +1–210–614–4096
Facsimile: +1–210–614–8192
email: mfischer@CHILD.com

Minutes of the MAC Subgroup meeting, held January 10, 1995

The MAC subgroup meeting was called to order by Kerry Lynn, MAC Vice–chair, at approximately 3:00 P.M. Eleven people were present at the beginning of the meeting, a few more came in later.

Agenda topics from opening session:

- PICS Proforma for MAC

  Briefly discussed, but no recommendations generated.
  The point was made that the PICS is hard to do until the MAC functionality is clear.
  The point was also made that failing to start one reduces the chance of getting done on schedule.
- Conformance testing

  Not addressed because several of the relevant people were not present.

Other agenda topics suggested by MAC group members:

- Security topics

  WEP issues and TBDs in the current draft were an issue of concern to more than half the attendees. This, plus the presence of Kerry Lynn, who made several of the original security proposals, lead to a decision to spend some time on these issues.
- Inter–Frame Space Issues

  The question was raised of whether the MAC group should address the IFS issues discussed in the Full WG session. The decision was that this belonged in the joint MAC/PHY session.
- Letter Ballot Issues

  The point was raised that we should plan the procedures for resolution of letter ballot comments in advance of the March Plenary meeting. Otherwise we will end up wasting time at the beginning of that meeting dealing with procedural issues. No specific recommendations were made, but discussion on the reflector was encouraged.

Discussion of Security Topics

The discussion began with Kerry L. stating some background of his original security proposal that introduced the basis behind much of what ended up in the security proposal subsequently adopted. This was followed by a summary of the 802.11 Wired–Equivalent Privacy (WEP) mechanism (Section 5.4 in the current draft) in terms of the 802.10 SDE model by Leon S.

Layering Nomenclature:

LLC (802.2)
------LLC_PDU
------SDE_SDU
SDE (802.10)
------SDE_PDU
------MSDU
MAC (802.11)
------MPDU
------Ph_SDU
PHY (802.11)
------ wireless medium ------

Leon S: The overall 802.10 security model includes many things besides frame level security. Some of those, such as key management, are at much higher layers (up through application layer). The relevant part is Secure Data Exchange (SDE). SDE is viewed as a transparent sub–layer that sits between MAC and LLC. The WEP facility described in Section of 5.4 of the draft standard can be viewed as an SDE entity.

- Normally 802.10 is attached to the bottom of LLC, but we break nothing by attaching 802.10 to the top of MAC instead.
- The design of 802.10 specifically allows for multiple, stacked SDE entities, so if an 802.11 MAC with WEP is placed below an 802.2 LLC with SDE things will work. Usually in such cases the lowest (n) SDE entities are turned off (encipherment=0) to avoid multiple encryption.
- 802.10 specifies its own security MIB and its own management transactions. If we want to fit in with 802.10 we should adopt security entries in the 802.11 MAC MIB that match the relevant SMIB entries.

Kerry L: The 802.11 security model says that a thin SDE is attached (mandatory?) to the top of 802.11 because of the greater need for security on the wireless medium. This is important in part because many of the large organizations which would be likely customers for large quantities of WLAN equipment have internal IS policies that preclude purchase of unsecure, wireless communication equipment.

Bob O: Why not leave this out of the MAC and just put in a pointer to 802.10?

Michael F: To promte interoperability we need to have a common subset of 802.10 and common privacy algorithm that all 802.11 MACs can include if they include any privacy. If we require full 802.10 generality, and possible use of all optional fields and arbitrary algorithms there is good likelihood that nobody will implement the WEP option, leaving us without any basic privacy.

Kerry L: A hole in the current subset is the lack of the concept of a network key. The direct mechanism for network keys in 802.10 appears to require security associations {hence SAIDs, hence SDE designators, hence much more per–MSDU overhear} to have the appropriate alternatives in the 802.10 receiver state machine.

Leon S: We can use a network key without SAIDs, etc. as long as the goal is privacy, since the way to do this is to have all stations in the ESS have the default key {loaded by a mechanism not specified as part of WEP — key management is not a layer 2 problem} that is used whenever you don't have another key for the sender's station address on file. This is a bad approach for message security, but is quite acceptable for privacy. To turn the default security off you set SDE=False. You also can set SDE=Flase for bootstrap activities, and to reduce overhead with multiple, stacked SDEs {the lower ones are the ones to be turned off}.

Kerry L: The default security with an ESS–wide key is good enough to overcome the "no security" objection that would otherwise preclude purchase by many such organizations.

Greg E: We need to have interoperable key distribution to really make WEP useful

{ Some inconclusive discussion on key management followed. Among the comments were that key management does not belong in the MAC; that for WEP to serve its intended purpose, key management must to be in the MAC; and that if we tried to get approval on a key management mechanism we would be lucky to get the standard done this century. }

{ It was decided to move forward in the discussion by assuming that a key distribution mechanism exists, whether within the MAC or elsewhere. Under this assumption, the stations are considered to have their WEP keys loaded by an unspecified mechanism. Possible mechanisms include in–band approaches (using the wireless medium) and other, possibly manual, approaches. }

Rick W: Why are MAC headers sent in the clear?

(answers): (a) So that adjacent ESS stations can correctly deal with probes, beacons, duration fields in various frames, etc. (b) Because that is how 802.10 defines the rules.

Kerry L: Reintroduces the concept, proposed almost 2 years ago by NCR, of "implicit authentification" — where the frames are sent encrypted, and successful decryption provides implicit evidence validity.

Bob O: The current draft requires authentification before association. There is no mechanism to allow the posession of the key to authenticate.

Kerry L: This could be an instance of pre-authentification (section 2.4.3.1.1 of the D1 draft).

An attempt to define the SDE subset required in the MAC to support WEP:

Clear header:	=0 (not used)
Protected header:	=0 (not used)

Data: = (IV followed by MSDU)

There was some discussion of whether the IV, which is sent in the clear, could appear in this field, which SDE places within the part of the SDE_PDU which is encrypted. Leon S. said yes, because SDE permits expansion of the MSDU to incorporate information needed to synchronize the code. It was also mentioned that if is possible meet the letter of the rules by defining the encryption algorithm such that the first N octets (the length of the IV) are not modified in the encryption process.

Pad: =0 (not used)

ICV: 4 octets, generated using CRC–32

Michael F. suggested that other ICV algorithms be considered,

Usage policy: If an encrypted frame (received with valid FCS) fails the ICV check after decryption, that frame is discarded (or passed to MAC management) without an indication to LLC. Only frames with good ICV check are passed to LLC.

Which frames: Data frames always encrypted (when WEP is enabled)

Management frames never encrypted

It was discussed that certain types of management frames could be encrypted, but that certain others (e.g. Beacons, Probes, Probe Responses) could not. After some discussion it was concluded that there were no privacy holes created by the use of non–encrypted management frames given the usage policy regarding data frames listed above.

Control frames never encrypted

Key length: 40 bits

Kerry L. said that this is the longest NSA will accept under their guidelines for expedited export approval (although these guidelines are for shrink–wrapped software).

IV length: 16 or 32 bits

The original RT proposal used 24 bits, to yield a 64–bit PRNG seed when concatenated with the 40–bit key. The current draft says 16 bits. Kerry L. believes that 16 bits is inadequate, primarily because it does an insufficient job of protecting the first few octets of the MSDU. These octets are especially vulnerable to directed attack because they generally contain rather–predictable information from higher–layer protocol headers. There was a consensus that 24 bits is a bad idea (unless another byte is added to the IV field) so that the MSDU remains aligned within the frame. A straw poll favored a 32–bit ICV by 3 votes to 1 with many present but not voting.

ICV length: 32 bits

Kerry L. says this is the shortest that NSA will accept for export approval. The ICV exists to let the receiver determine that the key is valid.

Recommendations to Plenary at the March, 1995 Meeting:

1. If privacy is optional, there should be an indication in the MAC header as to whether privacy has been applied to this frame.
    - There is a reserved bit in the FC field that could be used for this purpose. (More bits would be needed if more than one WEP algorithm were defined for the MAC.)

2. Privacy only applies to the MSDU, not to the MAC header.

3. Data frames are optionally encrypted. Management and control frames are not encrypted.

4. If the ICV of an encrypted data frame does not check, the MSDU is not passed to LLC.
    - The erroneous MSDU may be passed to MAC management.

5. 802.10 SDE settings
    - clear header length =0
    - protected header length =0
    - pad =none
    - ICV =32 bits, algorithm TBD

6. If the IV length exceeds the currently specified 16 bits, the IV shall occupy an even number of octets. (A straw poll favored a 32–bit IV, 3 votes to 1 vote.)

7. The privacy model assumes a default, ESS–wide key to permit implict authentification.
    - Any station in possession of the default key is considered pre–authentificated (e.g. in State 2 of figure 2–8 of the D1 draft)
    - This is fully compatible with the 802.10 concept of receivers having tables that associate keys with station addresses. The default key is used in cases where there is no table entry for the sender's address. Therefore, more comprehensive security, or different algorithms, can be directly applied by users that want to provide a full 802.10 implementation above the 802.11 MAC.

A motion to adjourn was passed unanimously at approximately 6:30 P.M.