IEEE P802.11
Wireless LANs

Security in Wireless LANs

May 6, 1993

Jan Kruys
NCR WCND
POBox 492
3430 AL, Nieuwegein, The Netherlands
Phone: + 31 3402 76529
Fax: + 31 3402 39125
e-Mail: jan.kruys@utrecht.ncr.com

Abstract

This contribution shows why 802.10 SDE is not a suitable solution for a base line security capability in Wireless LANs. Instead a MAC level confidentiality service is needed to provide such a capability at the level of a logical network. This relates to issuse 6.1, 6.2, 6.6 and 6.8

Also addressed is the question of device authentication which was discussed inconclusively in the March meeting. This relates to issues 6.4 and 6.7.

Contribution

A - General Security Provision

1 Introduction

As has been argued in a previous paper (802.11-93/21, information security is a systems level concern and requires systems level solutions. The same applies to communications security which is a subset of information security. ISO has developed a model for communications security in the Security Architecture of the OSI Reference Model (IS 7498, Part 2).

Wireless LAN standards in development in IEEE 802.11 and in ETSI RES 10 are not systems standard but they address only the two lower layers of the communications stack. In the OSI Reference Model, communications security functionality in the lower 2 layers only addresses confidentiality. Other security functions are allocated to higher layers, notably the Network layer, the Transport layer and the Presentation and Application layers.

2 IEEE 802.10 SDE

IEEE 802.10 has developed an intermediate solution - the Secure Data Exchange standard - that duplicates many of the functions defined for the Network layer in the OSI model. The primary characteristics of the SDE standard are:

a) the definition of an intermediate protocol layer - the SDE layer - between MAC and LLC; this layer is full transparent to MAC and LLC.
b) security associations between SDE entities
c) four security services: data confidentiality, connectionless data integrity , access control and data origin authentication

The security associations allow selective application of the security services defined by the SDE standard. The (initial) distribution of key material is described as a systems management function and therefore something that occurs at layer 7 and outside the MAC.

Because the security associations are between SDE entities, MAC bridges are not aware of the SDE protocol elements and need not act upon it. See Figure 1A.

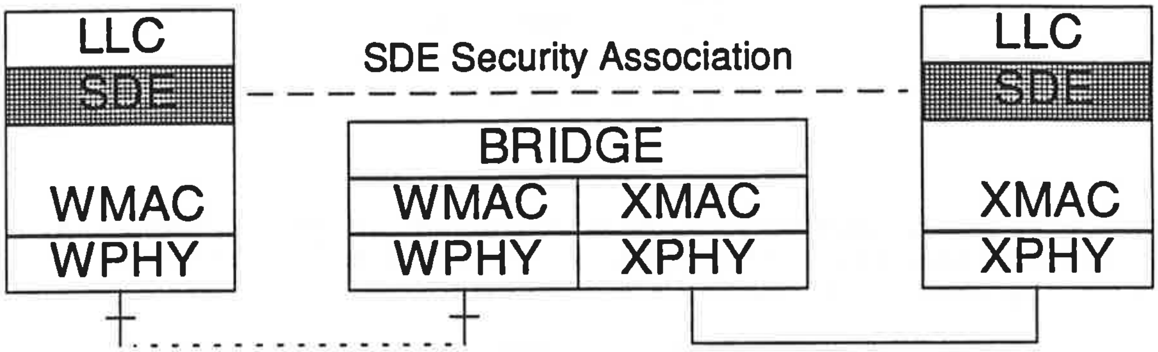

Figure 1A: 802.10 SDE in a mixed Radio/Wired LAN

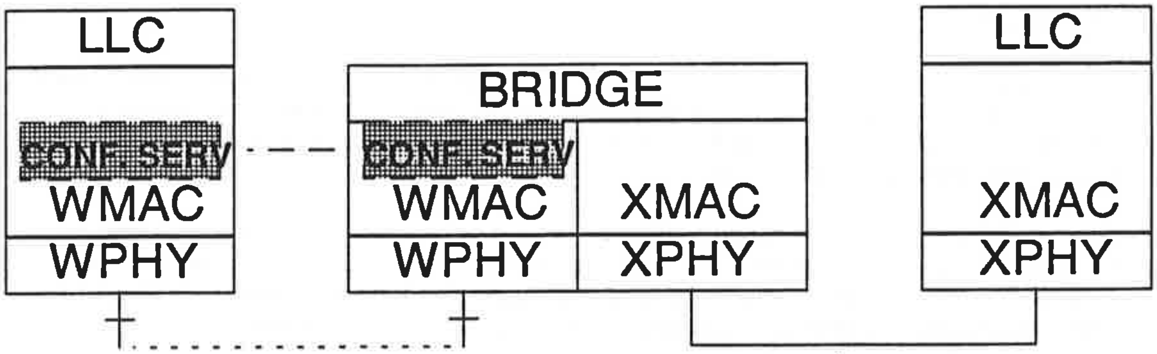

Figure 1B: MAC level Confidentiality Service in a mixed Radio/Wired LAN

The SDE standard has been proposed to ISO but so far the latter have not accepted this. The installed base of SDE is very limited and is only a small fraction of the total installed base of LAN systems. The likely reasons for this low level of penetration are the difficulty and cost of retrofitting SDE onto existing LAN network operating systems as well as the complexity of the SDE provided services and their management.

3 Security in Wireless LANs

The main concern of users of wireless LANs is eavesdropping on their wireless communications; they require a low cost, easy to manage solution that does not affect their installed systems. Since the majority of Wireless LANs will be mixed Wireless/ Wired systems, the latter aspect is a major concern.

To prevent eavesdropping on wireless links, a confidentiality service is needed in wireless stations. Because SDE is an "end-to-end" solution, it requires that all wired stations that may communicate with wireless stations implement SDE. Therefore, SDE as such cannot be used to provide the desired wireless security capability: it forces users to retrofit SDE on their installed base.

What is needed is shown in Figure 1B: a simple confidentiality service at MAC level. By restricting this service to the MAC, the scope of protection is limited to where it is needed: the wireless link. The installed base is not affected.

Although SDE cannot be used *in toto* , the confidentiality service in the MAC layer can be very similar to the SDE confidentiality service: protocol elements are needed for key identification and for carrying encrypted data. The details can be worked out once all requirements have been identified and agreed.

4 Requirements for a MAC level Confidentiality Service

- "group" security associations

  Like wired LANs, wireless LANs will be divided into logical subnetworks that are operated and controlled by different administrative entities even though they share the same medium. A simple but effective way to support this requirement is to use of separate keys for different logical groups.

- key synchronisation

  It is good security practice to change crypto keys over time. Since key distribution in networks cannot be exactly synchronised (clock shifts between stations, "spread" delivery times), a mechanism is needed in the MAC protocol to indicate which key is being used for a given message. This allows the use of specific keys to be synchronised exactly. The actual method of key synchronisation depend on the number of keys in a given used in a given logical subnetwork. A simple method is to use a two key roll-over scheme in combination with a time window: while one key is in use, another can be distributed throughout the subnetwork; whenever it is time to change keys a station will use the new key and indicate this in the message. The receiver can than select the appropriate key to decrypt the message.

- independent of hardware or software implementation

  Although crypto hardware can readily be integrated with MAC functionality, low cost products may not implement it at all or implement the crypto capability in software. The implication is that the crypto function must not affect protocol elements that are likely to be processed in hardware. The addressing information in the header and the CRC are the most important of such elements.

Summary r.e. security issues list:

R.e. issue 6.1: This issue may have to be re-opened since it sets the scope for subesequent issues.

R.e. issue 6.2: A confidentiality service should not be placed in the PHY for many reasons, including the fact that doing so would prevent isolation of logical networks through cryptographic means.

R.e. issue 6.6 The answer should be yes: SDE can not serve the needs of a large majortity of (wired/wireless networks) users because it forces them to retrofit SDE on their installed base. SDE is also overkill. Only a MAC level confidentiality service can provide the appropriate level of security at the appropriate levels of cost and (lack of) complexity. Such a service provides "authentication by implication" which is sufficient at MAC level.

R.e. issue 6.8 (re-)association is medium access function, not a systems function. Therefore, there is no link between (re-)association and "authentication" or "access control". However, the results of authentication operations performed at, say, the application layer, can be used in the MAC layer to provide implicit authentication (if I have the right key than obviously I have been authenticated). Implicit authentication works within a logical group: changing groups may require re-authenticating to the new group.

B - Device Authentication

The discussion in March circled around the question whether this is really needed at the MAC level. The position taken by NCR is that the implicit authentication which occurs if a device has the appropriate key is sufficient - in case there are concerns about device authentication.

The device authentication problem may be clarified by looking at it from the following perspective. The situation we have in 802.11 is that we have to cater for mobile devices that move between access points. Note that only the MAC entities are aware of such changes; higher layers don't know about these changes.

If device authentication were implemented at MAC level, every change in access point would involve re-authentication to the access point. If it is assumed that the access points can distribute the authentication data between them such that a device needs to authenticate to some access point once and all further authentication is implicit, then that is the same as saying that authentication can be decoupled from the (MAC level) access point function. If that is true than it is also true that device authentication - to any level of sophistication - can be done outside the MAC.

And that is where it belongs. Leaving authentication out of the Wireless MAC standard leaves systems integrators the freedom to choose whatever they like or need and saves 802.11 work.

A final note: one could describe standards development as the art of selecting the minimum necessary to realise common implementations. Options in a standard tend to negate its primary purpose - common implementations. Therefore NCR is not in favour of making device authentication optional in the MAC protocol.

To summarize in terms of the issues:

R.e. Issue 6.4 No specification of authentication or registration at MAC level (feeds back to 6.1). The reason is that implicit authentication as provided by a MAC level confidentiality service is sufficient.

R.e. issue 6.7 Saame as 6.8: (re-)association is medium access function, not a systems function. Therefore, there is no link between (re-)association and "authentication" or "access control". However, the results of authentication operations performed at, say, the application layer, can be used in the MAC layer to provide implicit authentication (if I have the right key than obviously I have been authenticated). Implicit authentication works within a logical group: changing groups may require re-authenticating to the new group.