Document:	**IEEE P802.11-94/....**
Author:	**ETSI PT-41**
Date:	**14 December, 1993**

Version: 1.0

Radio Equipment and Systems (RES);
HIgh PErformance Radio Local Area Network (HIPERLAN)
Security Information (input for STAG)

Distributed to members of IEEE P802.11 for its internal use
with the written approval of the chair of ETSI STC RES10

Internal document of

European Telecommunications Standards Institute sub-technical committee RES10

Contents

Blank page

1. Introduction

RES10 believes that the specification of the security services of HIPERLAN would benefit from the guidance of the ETSI Security Techniques Advisory Group (STAG). This document aims to identify the form of this guidance and provide, or reference, information relating to HIPERLAN security which will allow STAG to contribute towards further development of HIPERLAN's security architecture.

This document contains a description of HIPERLAN's security requirements, an outline of the currently proposed security solution and an indication of the input requested from STAG.

For background information on HIPERLAN, the reader is referred to the Services and Facilities document [1] and the Draft System Architecture Document [2].

This document is based largely on the contributions of RES10 members.

2. Security requirements

Users have varying security concerns that are related to their business or to their role in society. These requirements range from the need for simple confidentiality of internal communications to complex transaction security schemes that provide protection against fraud and repudiation. In the military world access control to information and systems resources is of overriding importance.

2.1. Confidentiality

HIPERLAN is a radio based communications subsystem that will be provided to users as part of a larger systems offering. The minimum that users expect from a radio based system that carries their (business) data, is that "the competitor next door can't see my data on his screen". In other words, simple confidentiality protection is the minimum that is needed. The HIPERLAN Services and facilities document [1] states that: "HIPERLAN can at least protect its users from *casual* eavesdropping and data injection in order to provide a level of security comparable to that of a wired LAN."

As wireless communications become more ubiquitous, the need for confidentiality will only increase. Note that the competitor next door may include the department next door. In many corporations, LANs are interconnected, but filters in bridges between LAN segments limit traffic flows. Private networks (of a sort) are thus created. From this point of view, there is a need to provide confidentiality at the private virtual network level in HIPERLAN.

2.2. Authentication

Wireless systems typically provide authentication of devices and, in some cases, users. GSM and DECT are examples. There are two significant differences between such systems and HIPERLAN: the former are public services and they are complete systems. The owners/operators of such systems are concerned that they will be able to collect revenues for the services they provide, hence their demand for authentication functions in the systems they operate. These allow them to prove that X called Y at Z time. HIPERLAN is intended for private use and is a subsystem. The private nature of HIPERLAN strongly reduces the need for device authentication. The subsystem aspect implies the presence of a higher level system which can take care of user authentication. A typical network operating system performs user authentication. Authentication, therefore, is not needed in the HIPERLAN standard.

2.3. Extent of security service

The Services and Facilities document states that: "protection should be contiguous over multiple radio networks that together cover a given area under one administration." This statement requires clarification. The term "radio networks" refers to HIPERLANs and the statement is referring to the level of protection provided for communications (over the HIPERLAN air interface) between co-operating HIPERLANs. The statement then implies that protection can be applied individually to the part of the connection between the source node and inter-HIPERLAN forwarding node and that between the inter-HIPERLAN forwarding node and the destination node. End-to-end protection need not be provided.

When two HIPERLANs communicate using a fixed network, protection is only provided for the parts of the connection between the HIPERLAN nodes and the HIPERLAN nodes providing interworking with the fixed network. Only the HIPERLAN parts of the connection are protected. This is consistent with the requirement to provide protection equivalent to that of a wired LAN.

2.4. Forwarding

To avoid the need for data to be decrypted and re-encrypted at all forwarding nodes[1], MAC addresses within the header of the MPDU should be un-encrypted. This is non-secure in that traffic flow information is disclosed, but traffic flow confidentiality is not required for HIPERLAN.

2.5. Interworking

Any security service provided by HIPERLAN must operate in situations where the HIPERLAN is interworking with existing fixed networks. The HIPERLAN security service must therefore be defined such that no additional functionality within existing fixed network nodes is required for HIPERLAN interworking. This implies that any security service must be restricted to HIPERLAN radio links.

2.6. HIPERLAN co-location

Data flowing within one HIPERLAN must be confidential from another, possibly co-located, HIPERLAN[2].

2.7. Double Encryption

In some of the regulatory environments targeted by HIPERLAN, a HIPERLAN sub-system implementation which results in a system which transfers data which has been subject to double encryption will be resisted. Double encryption can also reduce the system's efficiency. The HIPERLAN sub-system should therefore provide some means of preventing encryption when the HIPERLAN sub-system is integrated with other system components which also provide a data encryption service. A mechanism allowing the HIPERLAN encryption service to be disabled is therefore desirable.

2.8. Summary of security requirements

The following points summarise the security requirements:

- Protection from *casual* eavesdropping and data injection;
- Provision of a level of security comparable with that of wired LANs;
- Protection contiguous over multiple radio networks that together cover a given area under one administration;
- User is able to make use of security services defined by other Open Systems standards for information security;

[1] Decryption and re-encryption is not required for intra-HIPERLAN forwarding if the same encryption key is used throughout a single HIPERLAN. It is not clear whether it will be required for inter-HIPERLAN forwarding.

[2] A possible exception to this is when a bilateral agreement exists between the Hiperlans which allows data to be passed from a node of one Hiperlan to a node of another using a single key. In this case, the inter-HIPERLAN forwarding node is not required to decrypt (using the source node key) and re-encrypt (using the destination node key). The destination node of the destination HIPERLAN must be supplied with a key of the source HIPERLAN or the source node must be supplied with the key of the destination HIPERLAN.

- Provision of security services shall be achieved with low power consumption and low cost.;

- The security service shall be capable of operating in an environment in which HIPERLAN is interconnected with existing unmodified fixed networks;

- Data flowing within one HIPERLAN shall be confidential from another HIPERLAN. A possible exception to this is the case where a bilateral agreement exists between the HIPERLANs which allows encrypted data to be passed from a node of one HIPERLAN to a node of another without intermediate decryption and re-encryption;

- Source and destination MAC addresses shall remain un-encrypted;

- Traffic flow confidentiality is not required;

- Authentication (if any) is provided by higher layers;

- Provision of an encryption service should be a configuration option so it can be disabled when not required.

3. Existing security standards

This clause considers whether existing security standards can be used in conjunction with HIPERLAN in order to meet the security requirements of the HIPERLAN user. ISO 7498 Part 2 [3] and IEEE 802.10 [4] are considered.

3.1. OSI security architecture

The OSI model identifies a number of threats and it defines security services and mechanisms to deal with them. These mechanisms include data confidentiality, data integrity, authentication of systems and applications, data origin authentication, access control and traffic flow confidentiality. See Figure 1.

	Human user authentication, access control, transaction security
Application services	Application authentication, Access control, enc/dec, sealing
Presentation services	Data encryption/decryption
Session services	
Transport services	System access control Enc/dec, sealing
Network services	Network access control Enc/dec, sealing
Link services	Data encryption/decryption
Physical services	Data encryption/decryption

Figure 1: OSI security architecture - ISO 7498 part 2.

Data confidentiality is provided for in almost all layers; the other services only appear at the Network Layer and higher.

The main problem with ISO 7498 is that it was developed before the advent of the LAN, and the Link layer security services are not what *could* be provided at that layer.

3.2. Secure Data Exchange (SDE)

IEEE 802.10 thought it necessary to duplicate OSI's Network layer security services, within the LLC/MAC layer. This recognises the fact that there are many proprietary LLC and Network layer implementations that are impossible to retrofit with security functionality. The Secure Data Exchange service of 802.10 provides confidentiality, integrity, data origin authentication and access control functions without the need to change higher layer implementations. See Figure 2.

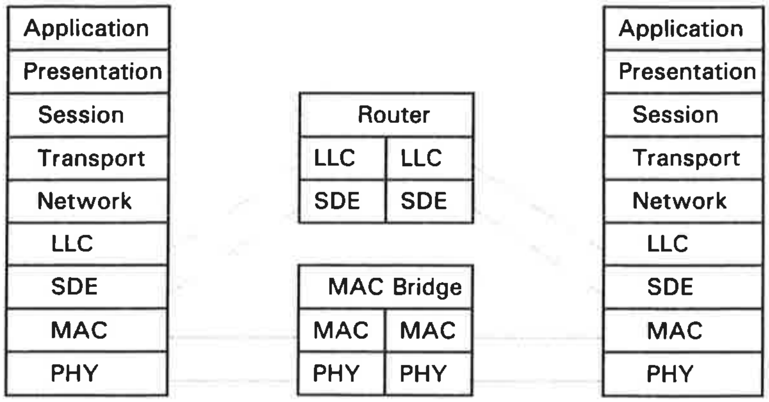

Figure 2: MAC sub-layer bridging and routing with SDE.

Note that SDE provides a limited form of end-to-end security; traffic going through a MAC bridge need not be decrypted and re-encrypted. (The MAC addresses remain in the clear).

SDE is unsuited to the requirements of HIPERLAN because the use of SDE with the HIPERLAN standard would require any node of a fixed network with which the HIPERLAN is interworking to include SDE functionality. The SDE standard has yet to be adopted by ISO and because of the cost of retrofitting SDE onto existing LAN network operating systems, as well as the complexity of SDE services and their management, the installed base of SDE is limited to a small proportion of the total of LAN systems.

The cost and complexity of SDE also make it undesirable for use with HIPERLAN.

3.3. Satisfying customer requirements

HIPERLAN customers include the end-users as well as systems integrators. As indicated earlier, users expect simple confidentiality of the contents of their air traffic as a minimum. That capability should provide interoperability. Systems integrators shall provide this. Using 802.10 SDE or the OSI network layer is both costly and an overkill. In many cases it may not even be possible (consider adding a crypto capability to a palmtop, only to secure its air traffic). Therefore, it makes good sense to provide simple confidentiality as part of the HIPERLAN standard, assuring a minimum level of performance and interoperability with low cost. Systems integrators are able to provide security features within the higher layers if they so desire, but the HIPERLAN standard should provide at least a confidentiality service. Thus the systems integrator is not *compelled* to use a complex and costly solution, such as SDE or ISO 7498, in order merely to achieve confidentiality.

4. HIPERLAN security services

From the preceding clause is was concluded that existing security standards cannot be relied upon to meet the security needs of HIPERLAN and that a simple confidentiality service is required within the HIPERLAN standard. This clause considers the provision of such a service within HIPERLAN.

4.1. MAC or PHY level confidentiality service

Confidentiality can be provided at PHY and MAC layers. In either case, encryption is the default mechanism. PHY encryption was one of the first security standards: ISO 9160 which covers crypto-modems was approved in 1986. These devices are intended to secure point to point leased lines; not portable computers with radio modems.

PHY level confidentiality in a LAN environment suffers the drawback that all stations must share the same key or other vector that controls the key used for encryption and decryption. Key sharing is the nightmare of every security officer and therefore a single key is not an option except for rather small, closed networks that do not service guests. PHY level encryption would also encrypt MAC addresses. Since the PHY does not know about the MAC message structure, all MAC data in all messages are encrypted. PHY layer encryption is therefore unsuitable for HIPERLAN.

MAC level encryption avoids the problem of encrypted MAC addresses - the MAC protocol machine knows about its messages and when to encrypt a message or part thereof. Also, the MAC knows about HIPERLAN IDentifiers (HIDs) - this allows separate virtual sub-networks to have different keys so as to provide isolation between networks in the same organisation (security domain). The placement of encryption services in the MAC, relative to its other functions, determines both the complexity of the implementation and the implications for the overall HIPERLAN system design. Performing the encryption service at the bottom of the MAC does not require encryption of MAC addresses but leaves the option to do that where required. When MAC addresses are not encrypted, intra-HIPERLAN forwarding can be performed on encrypted messages[3]. See Figure 3.

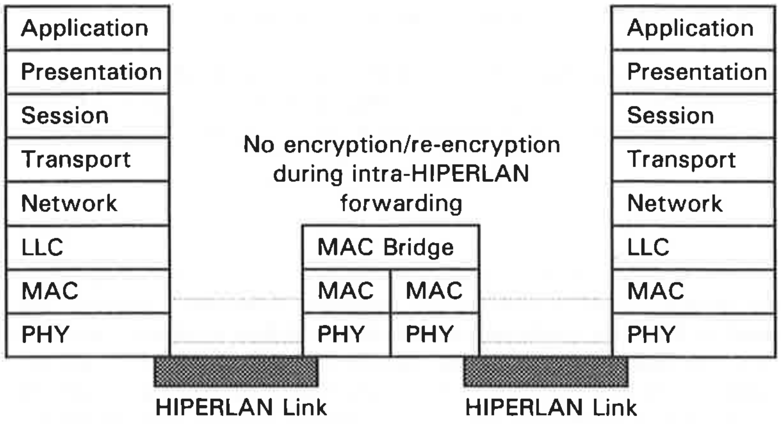

Figure 3: HIPERLAN forwarding of encrypted messages.

MAC based encryption will support both asynchronous and time bounded data services; there is no need to put an encryption function in the HIPERLAN LLC.

However, it may be that encryption has implications for the MAC frame size. Longer frame sizes make recovery more costly in terms of time[4].

[3] It is not clear whether inter-HIPERLAN forwarding will require decryption/encryption. It depends on whether keys of one HIPERLAN can be provided to another for the purposes of an inter-HIPERLAN communication, or whether distribution of a HIPERLAN keys is strictly limited to individual HIPERLANs.

[4] This is a subject for further work.

It should be noted that time bounded services impose stringent requirements on delay and delay variance. Encryption can add to both of these. In particular, loss of crypto synchronisation, which requires protocol overhead in order to be re-established, is likely to have a disasterous effect on delay. Thus, a simple encryption scheme is needed that is tolerant of transmission errors[5].

MAC based encryption need not be more expensive in terms of production cost than PHY based encryption. In both cases the encryption function can be embedded in hardware.

Placing HIPERLAN security in the MAC avoids the limitations of PHY based security without paying the price of the increased cost of SDE or OSI Network layer security.

4.2. Key management

Key management is an integral part of all applications of encryption where these do not rely on a secret algorithm.

In its simplest form, key management in HIPERLAN follows the pattern of the HIPERLAN structure, with each HIPERLAN having its own key or set of keys. Simple procedures allow keys to be changed or synchronised at any time. One possibility is for selection of the key to be used in a given HIPERLAN to be done during a "HIPERLAN Create" or "HIPERLAN Join" operation.

Key distribution to users happens outside the protected HIPERLANs. Before a node joins a HIPERLAN, it could access a sign-on application on a clear un-encrypted HIPERLAN. The sign-on procedure should include authentication of the user and the transfer of one of more keys for protected HIPERLANs. The keys so distributed would be provided to the MAC through the MAC Layer Management Entity interface. However, this application level functionality lies outside the scope of the HIPERLAN standard.

Key distribution to HIPERLAN users need not happen in real time but could be done off line, e.g. by means of smart cards as in DECT and GSM. Since HIPERLAN is not a complete system standard, functions such as off-line key distribution can be omitted from the standard and left to competitive advantage. The standard shall however define how key selection in the MAC Tx and Rx functions is related to HIPERLAN addresses and how key synchronisation is assured[6].

The distribution and other management aspects of cryptographic keys do not differ in principle from the distribution and management of other systems management information. Therefore, if a decision is made to provide for on-line key management functions, they should be treated in the same way as other management functions.

4.3. 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 depends on the number of keys used in a given logical sub-network. 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 sub-network - 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[7].

[5] The question of the delay caused by encryption and any other impact that encryption will have on time bounded services requires further work.

[6] These are subjects for further work.

[7] This is an example of a possible means of key synchronisation. The example requires MAC layer management protocol support. Alternative methods, that do not involve a MAC layer management protocol would be preferable and should be investigated.

It should be noted that there need not be any requirement for key synchronisation functions in the HIPERLAN LLC for time bounded services. MAC level encryption should not be visible at LLC level.

4.4. Support for authentication

Device authentication can be performed by higher layers when creating or joining a HIPERLAN. A key is then provided which enables the MAC sub-layer to perform encryption and decryption. No further authentication of the node or user is done during the time the node remains in contact with the HIPERLAN. However, if the node moves out of range of the HIPERLAN for a period of time, and if the key is changed during this time, the node will have to be authenticated again if it wishes to remain a member of the HIPERLAN.

A node wishing to join a HIPERLAN must be able to request membership without possession of a key on an un-encrypted channel. This channel is arranged by MAC management entities which can bypass the encryption stage within the MAC.

4.5. Intra- and inter-HIPERLAN forwarding

The provision of security for data transfers within and between HIPERLANs, and its impact on the forwarding mechanism and on time-bounded services, is an important aspect of the security service provided by HIPERLAN. A number of options are available including the following:

1. A single key or multiple keys is/are used throughout a given HIPERLAN;

2. For communications between a node of one HIPERLAN and a node of another, either the same key (belonging to one HIPERLAN) can be used for all hops, or, multiple keys can be used.

Given the requirement to provide protection similar to that of a wired LAN, the provision of a single key per HIPERLAN would appear to be adequate, since the situation with respect to access of data would then be equivalent to that of a wired LAN[8].

To some extent, the choice of key(s) for inter-HIPERLAN traffic depends on the time taken for a node to perform encryption and decryption. If this is significant, then it is undesirable for nodes to have to decrypt and re-encrypt messages simply to perform forwarding, be it intra-HIPERLAN or inter-HIPERLAN. This is particularly so in view of the delay and delay variance requirements for time-bounded data,.

Assuming a single key is used throughout a given HIPERLAN, then intra-HIPERLAN forwarding will not require encryption/re-encryption. For Inter-HIPERLAN communications there are at least three choices.

1. The inter-HIPERLAN forwarding node performs decryption/re-encryption and must hold the key to both HIPERLANs;

2. The destination node is supplied with the key for the HIPERLAN containing the source node. The key has end-to-end significance, so the inter-HIPERLAN forwarder need not perform decryption/re-encryption;

3. The source node is supplied with the key for the HIPERLAN containing the destination node. The key has end-to-end significance, so the inter-HIPERLAN forwarder need not perform decryption/re-encryption.

The consequences in terms of delay need to be considered for the first case. The consequences for the security of the individual HIPERLANs need to be considered for the last two cases.

[8] The wider implications of using one key per HIPERLAN need to be considered.

4.6. Solution summary

The following points summarise the more important points of the solution expected to meet HIPERLAN's security requirements:

1. A confidentiality service is provided by MAC sub-layer encryption of the MSDU (this could be similar to the SDE confidentiality service). The MAC addresses within the MAC frame are not encrypted;

2. Key distribution is handled by higher layers;

3. Key synchronisation is handled by the MAC sub-layer using a two key roll-over scheme. Information within the MAC frame indicates when a key is changed;

4. Any required authentication is performed by the higher layers. A mechanism allowing provision of clear unencrypted channels for operation of sign on procedures will be included in the MAC sub-layer;

5. Each HIPERLAN has a single key. Intra-HIPERLAN forwarding does not involve decryption and re-encryption. Inter-HIPERLAN forwarding may involve decryption and re-encryption and depends on the access nodes have to keys of other HIPERLANs;

6. A MAC layer management facility will be provided to allow encryption to be enabled or disabled. This will prevent double encryption of data.

5. STAG contribution

The contribution from STAG to the work on the HIPERLAN architecture is requested to take the following form:

- a review of HIPERLAN's security requirements and SAG's proposed approach to security within HIPERLAN;

- an indication of the implications, in terms of cost, size, power consumption, complexity, processing time and effectiveness of the proposed approach;

- recommendations for changes;

- an investigation of suitable algorithms for HIPERLAN's confidentiality service.

6. References

[1] ETSI TC-RES: "Radio Equipment and Systems (RES); HIPERLAN Services and facilities", V1.0, ETSI, ETR069, February 1993.

[2] ETSI TC-RES STC-RES10: "Radio Equipment and Systems (RES); HIPERLAN Systems Architecture", Draft issue V0.8, ETSI internal document, September 1993.

[3] ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part2: Security Architecture".

[4] IEEE Std 802.10: Interoperable Local Area Network Security, *Currently contains* Secure Data Exchange (SDE).

IEEE P802.11
Wireless LANs

HIPERLAN Security Information
Version: 1.0

Radio Equipment and Systems (RES);
HIgh PErformance Radio Local Area Network (HIPERLAN)
Security Information (input for STAG)

Subject document was distributed to members only. This document is not available on the subsciption and order service due to copyright clauses.