SECURITY ISSUES IN EMERGING HIGH SPEED NETWORKS

Vijay Varadharajan[*], Panos Katsavos[†]

July 4, 1996

Abstract

There is a growing interest in the development of broadband services and networks for commercial use in both local area and wide area networks. In particular, connectionless Switched Multilmegabit Data Service (SMDS) and connection-oriented Frame Relay based broadband services are beginning to be offered by a number of major operators in the US and Europe. This paper considers the issues that need to be addressed in the design of security services for such high speed networks. First the relevant characteristics of broadband network interfaces are discussed, some of the existing security protocols for TCP/IP and OSI networks are reviewed, and their suitability for providing security in broadband networks assessed. Then the developed arguments are applied to design security services for the connection-oriented Frame Relay networks. An earlier paper [3] considered the development of security services for the connectionless SMDS.

1. Introduction

There is a growing interest in the development of broadband services and networks for commercial use in both local area and wide area networks. The initial stimulus some ten years ago was the development of Asynchronous Transfer Mode (ATM) for use on broadband networks, under the banner of Broadband ISDN (B-ISDN). Recently there is a real pragmatic drive for broadband services, to meet the demand for increased bandwidth for remote sites inter-connection, and for image and high speed data transfer. Broadband activity now has commercial services under a variety of titles, and most of these fall under the umbrella of Fast Packet Switching (FPS). This is a generic term that refers to the switching process being done at a layer which corresponds to layer 2 in the OSI Reference Model. Some of these networking technologies use ATM techniques such as Switched Multimegabit Data Service (SMDS) [2] (can be offered using ATM) and Dual Queued Data Bus (DQDB) [4], and others not such as Frame Relay.

Although it is possible to appreciate the differences between these technologies in terms of the network infrastructure, it is not very clear what each of them has to offer in terms of supporting applications. In particular, with the development of new applications such as networked multi-media, desktop video-conferencing and entertainment services, the need for such broadband services is constantly growing. Also the interconnection of Local Area Networks (LANs) providing high speed information transfer is becoming a strategic necessity for many enterprises to support their growing number of workgroup-based and backbone-type LANs.

There is also a significant change in the nature of network traffic. It is more and more of the form of bursty traffic characterized by an unpredictable demand for bandwidth of several megabytes. The new generation of networking technologies enable interconnection at high-speeds in the range of Mbit/s or even Gbit/s over very wide areas, which effectively moves the bottleneck from networks to end systems. Furthermore, the user is able to access bandwidth on demand and the user is only charged for the bandwidth actually used. As more and more information (audio, image and data) are transferred over

[*] Prof. Vijay Varadharajan, University of W.Sydney, Australia. Email:vijay@st.nepean.uws.edu.au. Previously, he headed the Distributed Systems Security Group at Hewlett-Packard Labs.UK.

[†] HP sponsored student,UK.

but also by the level of trust that can be placed on its performance, security and availability.

This paper considers the issues in the design of security services for high speed networks. Section 2 briefly outlines the characteristics of the various broadband networking interfaces that are relevant to this paper. Section 3 first considers the security threats in this environment and the services required; then it describes the background work done and being carried out in the TCP/IP and OSI arena. Section 4 assesses the adequacy of the earlier work in the broadband context, and then considers the placement of security layer within the broadband protocol profiles, and discusses the rationale behind the different choices. Section 5 applies these arguments in the context of connection-oriented Frame Relay networks.

2. Broadband Network Interfaces

A number of options exist for the provision of wide area broadband communication services: leased lines, N-ISDN (Narrowband ISDN), SDH (Synchronous Digital Hierarchy) cross-connect, Frame Relay, FDDI (fibre Digital Data Interface), DQDB, SMDS, B-ISDN. ATM, and SONET (Synchronous Optical Network). These technologies in effect merge the Public Data Networks world and the Voice Circuit-based Networks world together. In doing so, they lead to a new way of modelling communication over the networks in comparison to the OSI model. For instance, the support of circuit-type traffic such as voice, CD quality audio and video traffic is explicitly taken into account in the design of the broadband protocol reference model. Also traditional protocol reference models such as the DoD TCP/IP suite and the OSI model do not have a separate out-of-band signalling path. All network control is carried out by either management entities at the application level with access to the internals of the layers below, or as in-band peer-layer management protocols.

Figure 1 shows some of the protocol profiles of the network interfaces used in broadband communications and their comparison to the OSI model. Although these broadband systems have different models based on multi-protocol stacks, they offer a standard set of services to users : connectionless (CLS), connection-oriented (CO), and isochronous (ISO) services. Note that the functionality of these network interfaces resembles that of the layers 1 and 2 of the OSI model. For instance, SMDS offers connectionless service, and Frame Relay offers connection-oriented service. In fact, in the LAN to LAN market, at present SMDS and Frame Relay are the best known ways of accessing these multi-megabit backbones. FDDI(II) supports both connectionless and isochronous services, but not a connection-oriented one, while DQDB supports the full range. B-ISDN goes further by assigning two different protocol stacks to the isochronous service, namely one for transfer with strict periodicity and another for transfer with guaranteed delivery latency. SDH/SONET interface is equally capable of carrying all different types of traffic. N-ISDN combines circuit-switching with higher special purpose protocol stacks to make provisions for a relatively wide service spectrum including OSI layer 7 teleservices. In this case, there is only a limited support of the connectionless service over the D-channel.

Each of these technologies is claimed to be suitable for a range of applications, and often an application can be equally supported by more than one technology. For instance, both SMDS (CLS) and Frame Relay (CO) can claim to be suitable for interconnection of LANs. The connectionless service supports interactive applications producing bursts of data, with no special timing constraints, to optimize the utilization of network resources. On the other hand, isochronous service addresses circuit-type traffic with strict timing dependencies. The connection-oriented service supports traffic of either data or circuit-type, offering more efficient management of traffic than the connectionless service by allocating resources within the network. In practice, it is not possible to identify all the uses of a multiservice network. However it is clear that such technologies can support not only classic data applications but also applications with real-time transport requirements. Applications make use of these network interfaces by employing an appropriate protocol stack. The synthesis of these protocol stacks is dependent on the nature of the application to be supported; in general, it will be either in the form of a OSI type (or some similar model such as the DoD TCP/IP) or a single adaptation layer.

protocol. However implementations of transport protocols such as DoD's TCP, and ISO's TP4 can have performance limitations. Naturally therefore a great deal of research is currently being focussed on this layer; several pieces of work are currently in progress that are considering extensions and modifications to the existing transport protocols to adapt them to high speed environments (e.g. [7]). In our view, it is likely that future communication scenarios will not have full OSI style stack on top of a broadband network interface; some form of adaptation layers will assume the functonality of the traditional transport and network layers.

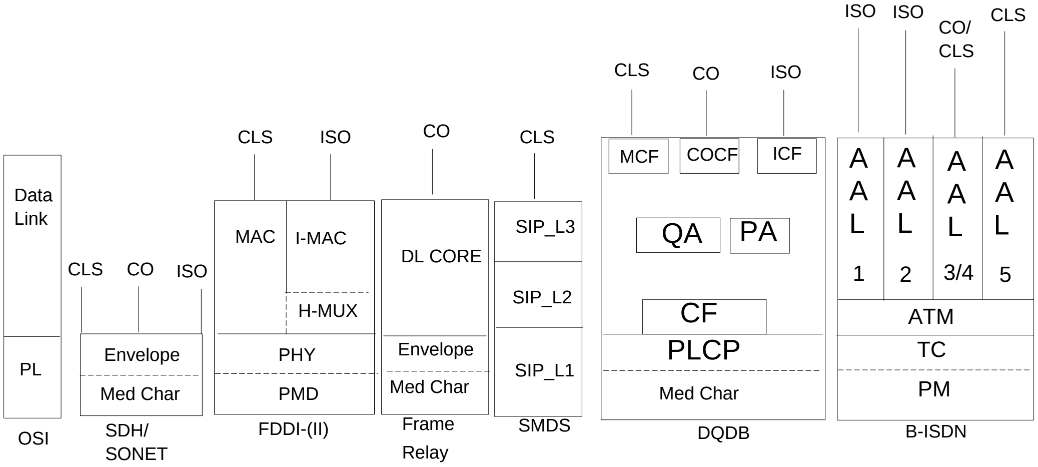

Fig. 1: Protocol Profiles of Broadband Network Interfaces

In the near term, it is clear that most major operators are and will be offering either SMDS or Frame Relay based services. Therefore, it is important at the first instance to address security for these broadband services. Security services for SMDS have been considered in [3]. Before describing the security services for Frame Relay, let us first assess the use of the existing security protocols in traditional networking models to protect broadband information and services efficiently.

3. Security Issues

The fundamental questions that we need to consider when addressing security in high speed Metropolitan Area and Wide Area Networks (MAN/WAN) are :

- What are the security threats in the network environment?
- What are the required security services and mechanisms?
- Where should these services and mechanisms be provided in the protocol stack?
- How are they to be managed?

When dealing with security for public networks, the provision of security services need to be considered from different organizations' points of views. There are several options for security services providers within a MAN/WAN environment.

There is the option of the security services and features provided by the *user* to protect his information being carried across public networks. Then there is the provision of security services by the MAN/WAN operator to the end user on a service contract basis. This may not be an attractive option for the end users because of the lack of trust on the network operator. However with the increase in the trend of outsourcing and the options for legislative recourse, there may be opportunities for such a service in the future. In addition to the above, there are security services that are required (and managed) by the network operator to protect his own network resources and information. Finally, there are the services provided by third parties[1] to the end users which may be in the form of supplementary and/or support security services. For instance, notary services come under this category. A common situation is when there is a need to deal with a number of external organizations involving sensitive issues, e.g. contract negotiations. A third party can be of assistance in setting up a secure negotiation between different users through notary and directory dervices.

From the public network point of view, the positioning of facilities and resources to provide secure traffic needs to be carefully evaluated to ensure that the impact of security features on reliability and overall availability of the services is minimized.

3.2 Security Threats and Services

Let us begin by enumerating briefly the types of security threats that can arise in such a network environment.

Unauthorized disclosure of information via eavesdropping and wiretapping is perhaps the most common threat that comes to one's mind when one thinks about network security attacks. This attack can be carried out by an eavesdropper located anywhere along the communication path. If the target of the eavesdropper is not the user to network interface, subscription to a connectionless service (such as the SMDS, ATM AAL5 or MAC service based on MAN based DQDB) can make the customer traffic less susceptible to this attack compared to the use of a connection-oriented service such as Frame Relay or ATM AAL1/2, where the same route is always followed. A more interesting situation is where the eavesdropper is a legitimate user sharing the network access interface with (or is attached on the same ring as) the source and destination system of the information in transit. This could occur for instance in a multi-CPE (Customer Premise Equipment) access arrangement in an SMDS network.

In addition to this, the information may be altered in an unauthorized manner. The threat of *unauthorized modification* of information and resources causes integrity violation. Such an attack may involve unauthorized insertion and deletion of information transferred over the network. This attack often occurs in conjunction with other attacks such as replay whereby a message or part of a message is repeated intentionally to produce an unauthorized effect. Network parts including digital exchanges, MAN nodes and communication links, as well as bridges, routers and hosts are vulnerable to this form of attack.

In a *masquerading attack* one entity pretends to be another and attempts to gain privileges and access to information and resources to which it is not authorized. For instance, a customer of a MAN can transmit information at a higher rate than the one allowed by the "Access Class" it has negotiated earlier with the network, having at the same time another customer (with whom it shares the user to network interface) to be charged for the bandwidth it uses, as long as the packets it sends carry the other user's source network address (e.g. MAC address in E.164 format).

A noticeable weakness in the general MAN architecture has been that a user connected to a MAN node has access to all the information passing through the node. This raises a fundamental security problem. It imposes limitations on how users can be connected to the network. For instance, when the DQDB

[1] Network operators might themselves provide some of these services.

or be provided with specific security facilities.

Another common attack is the *unauthorized access* to network resources and services. Having successfully masqueraded as another entity, an entity can gain access to resources which are otherwise denied to it. Resources could be network components such as printers or network resources such as operating systems, databases and applications.

Unauthorized denial of service attack by an entity involves the denial of a service to another entity even though the latter is authorized to access that service. That is, an entity prevents other entities from carrying out their legitimate functions. In a network, this form of attack may involve blocking the access to the network by continuous deletion or generation of messages so that the target is either depleted or saturated with meaningless messages. Network failures and errors resulting from equipment reliability also need to be accounted for. For example, an ATM switch may suffer from an accidental breakdown or malfunction resulting in disruption of its customers communications. Denial of a service can be regarded as an extreme case of information modification in which the information transfer is either blocked or drastically delayed.

Repudiation of actions is another form of attack that can occur in a networked system. It occurs when a sender (or a receiver) of a message denies having sent (or received) the information.

3.3 Background

There has been a number of efforts in the development of security protocols for the TCP/IP suite and the OSI over the last years.

3.3.1 TCP/IP Security

Originally, with respect to security, the *options* field in the header of the IP datagrams supported two security options for labelling of sensitive information. The options are referred to as the Basic Security Option (BSO) and the Extended Security Option (ESO). Security labels consist of the classification level at which the datagram is to be protected (such as top secret and secret), the authorities whose protection rules apply to each datagram, and some extra security information (only for the ESO). There are also new labelling standards, the NIST Standard for Secure Labelling (SSL) and the DoD Standard for Common Security Label (CSL). A Commercial Security Option (CIPSO) has been proposed by the Trusted Systems Interoperability Group (TSIG) to meet commercial instead of military requirements.

However recently, there has been considerable work within IETF to develop security mechanisms for IP, as part of the IP Security Protocol Working Group (IPSEC). A security protocol in the network layer supporting authentication, integrity, confidentiality and access control is being developed. There are two specific headers that are used to provide security services in IPv4 and IPv6. These headers are IP Authentication (AH) (RFC 1826) and the IP Encapsulating Security Payload (ESP) (RFC 1827). The IP AH is designed to provide integrity and authentication without confidentiality to IP datagrams. The IP ESP is designed to provide integrity, authentication and confidentiality to IP datagrams. A key management protocol called the Internet Key Management Protocol (IKMP) is also being defined at the application layer.

The Secure Data Network System (SDNS) protocols have been dveloped within the framework of the OSI to support secure interaction between applications. They are also intended to provide secure communications to DoD and commercial data networks with a preference for the TCP/IP stack. The SDNS protocols essentially encapsulate the protocol data units in a “security envelope” with some protected header in front. The protected header may have security labels, sequence numbers along with addresses and headers of the specific protocol. An Integrity Check Value is appended to the PDU. SDNS defines two categories of protocols, namely the SP3 family [12] which resides in the network layer, and the SP4 family [10] which resides in the transport layer. There are four variants of SP3 and two variants of SP4.

its termination at intermediate points. This is achieved by encapsulating routing information in the protected header of the SP3 Protocol Data Units (PDUs). Depending on the format of the protected portion of its header, the SP3 protocol can operate in different addressing modes, namely SP3N, SP3A, SP3I and SP3D. SP3A is at the top of the network layer and it includes the source and destination NSAP addresses in the protected header. SP3I lies below the CLNP network sublayer and includes the CLNP header in the protected header. SP3D is similar to SP3I except that it lies below the DoD IP protocol. SP3N is identical to SP4E and is used only in the end systems.

The integration of SP4 within the transport protocol, allows access to all of the Transport Protocol control information. Thus the SP4 protocols permit the use of crypotgraphic techniques to provide data protection for transport connections or for connectionless-mode TPDU transmission. SP4C is closely integrated with the OSI connection-oriented services (ISO 8073), and SP4E provides support for connectionless-mode transport service (ISO 8602) and DoD TCP. That is, SP4C can be seen as a sublayer near the bottom of the transport layer. Hence a separate security association with a separate key is formed for each transport association, even when the transport connections are between the same transport entities. SP4E resides between the transport and the network layers. Hence it is dependent on the services of the transport layer for connection integrity.

In addition to these secure communication protocols, the SDNS project also defined a Key Management Protocol (KMP).

3.3.2 OSI Security

In terms of security, the work that directly addresses the security issues in the OSI Architecture is the Security Architecture document (ISO 7498-2) [9]. It is worth emphasizing that it only defines a skeleton for the provision of security, and does not provide any details as to how the security services be provided. It deals with security at an abstract level, defining a number of security services and mechanisms to support them, and does not describe specific security protocols. The Network Layer Security Protocol (NLSP) and Transport Layer Security Protocol (TLSP) are upgarded versions of the SDNS SP3 and SP4, standardised by the ISO for use with the OSI compliant network and transport layers. With respect to connectionless service, NLSP (ISO 11577) provides the same services as SP3, plus traffic flow confidentiality. In addition, NLSP addresses the protection of the connection-mode network service defined in CCITT X.213. This is not the case with SP3 which only deals with the connectionless aspect of the network service in terms of the ISO CLNP and DoD IP. Furthermore, NLSP supports in the connection mode in-band key distribution during connection establishment or within an on-going connection. TLSP (ISO 10736) is almost identical to SDNS SP4. In the application layer, there are several OSI standards that address security aspects such as messaging (X.400) and file transfer (FTAM). Some are at initial stages of development whereas others such as X.400 (1988 Recommendations) have specified a comprehensive set of security services and profiles.

4. Security for Broadband Networks

Recall that the broadband MAN/WAN technologies support both data networks as well as circuit-based networks such as voice and video traffic. These applications have real-time characteristics which affect the way they are set up and managed. The protocol stacks for broadband networks are somewhat different, and hence first it is necessary to look at suitable ways of incorporating security services within these protocol profiles. Furthermore, these networks have a separate out-of-band signalling path. Hence from security point of view, there is a facility to integrate the security management protocols such as the key management as part of the signalling phase in the Control Plane (C Plane) rather than in the User Plane (U Plane).

With these in mind, let us consider the issues relating to provision of security in such broadband networks. The first question that arises is where in the protocol stack should the security services be provided. There

Application-embodied Security

In this option, the functionality of each individual application has to be enriched in order to support security services. This approach may be useful when specialized application-oriented security is required. This will offer protection at the highest possible level in the stack.

Security at the Stack-level

In the OSI stack, end-to-end security could only be achieved above the network layer. This is because the information required for routing occurs at the network level and this information needs to be in plaintext form. Subsequently, security protocols designed for this type of networks such as the TLSP, the NLSP and the SDNS' SP3 and SP4, operate in and between the transport and the network layers. End-to-end security avoids the need to place any trust on the resources such as routers and intermediary devices which are not owned by the sender and receiver (organizations).

The applicability of these security protocols appears to be limited in the context of broadband networks. First, the routing in such broadband networks is done based on values provided within the data link layer instead of the network layer. For instance, with a Frame Relay network, the routing is based on the DLCI values provided within the data link layer. Therefore it is now possible to provide end-to-end security at a lower level. Second, as mentioned earlier, transport protocols such as the TCP and the OSI's TP0-4 can become bottlenecks in high speed environments. Given this, it is likely that they will be modified in the near future by some light weight protocols. These will present an interface that will differ from the current ones for which the security protocols have been originally designed for.

Security at the Interface-level

There are three driving forces behind the provision of security at the interface level. Firstly, the layers comprising the access interface are always present independently of the supported traffic. Hence all the applications can use the security services offered by a security sublayer operating at this level. Secondly, both the user and the network operator must be given the choice to protect the traffic. The network operator has much fewer options by being restricted to provide security services within the boundaries of his domain. Thirdly, an internetworking device can act as a security service provider. It can effectively act as a “frontdoor-lock”. Not all end systems may have or indeed need to have built-in security mechanisms. Furthermore, such secure internetworking devices can be used to translate and interpret different security policies between networks, e.g. between public and private networks.

Considering the network access interfaces shown in Figure 1, we have several options for the placement of security services within these interfaces. Let us now consider each of these options.

- First consider the placement of security at the physical layer. The physical layer strictly deals with the medium and the characteristics of the transmitted signals. Protection at this layer can only take place in the form of scrambling of signals, using an encryption device at each link. Such a solution is very limited and inflexible. To decouple security mechanisms such as encryption from the medium (e.g. coaxial cable, twisted pair) and the encoding scheme (e.g. 4B/5B, HDB3), it is necessary to perform encryption just before translation to the characteristics of the medium occurs, and immediately after line coding has been carried out. Otherwise, each network interface will require a distinct type of encryption device upon adoption of a different physical layer medium dependent sublayer. Such a technique is useful for protection against traffic flow confidentiality, for instance, in an exposed link between the customer premises and the network switch (e.g. the User-to-Network Interface (UNI) in the N-ISDN and B-ISDN).

- Another option is to integrate security into one of the network access interfaces. For instance, in the case of Frame Relay, security can be integrated within the DL-CORE sublayer. However such an approach often impacts the functionality of that interface. Even when a clear interface it is preferable to avoid such an approach.

- Another option is to place the security functions on top of the access interface. In this way, it is possible to support a wide range of security services at this level. For instance, in the case of Frame Relay, we can place security on top of the DL-CORE sublayer. In the case of a LAN, the IEEE 802.10 standard placed the security layer on top of the MAC layer. Such an approach is attractive for incorporating security in devices such as remote bridges and routers. In fact, in our view, this option of providing security at the top of the access interface represents the most effective way of providing secure LAN-to-LAN interconnections, which is one of the main drivers of public broadband services.

5. Security for Connection-Oriented Service

The rest of this paper is concerned with the demonstration of providing security services on top of the access interface by considering the connection-oriented Frame Relay networks. The connectionless SMDS service has been considered in [3].

In general, for data traffic, the connection-oriented service offers more efficient management of traffic than the connectionless service, by allocating resources within the network. Another advantage occurs when the data is to be transferred over long periods; in this case, the duration of the call set-up phase can be justified by subsequent savings in time.

Moreover, circuit-type traffic with low service requirements can also be users of the connection-oriented service. For example, poor quality voice and low scan video could make use of connection-oriented Frame Relay. However circuit-type traffic with stringent timing constraints could suffer severe degradation of service. It may be possible to use under certain circumstances, for instance, providing access to an ATM-based core network (with no congestion and the end systems supporting appropriate traffic shaping mechanisms). In general, they are better handled using fixed cells than using variable length frames.

5.1 Frame Relay

Frame Relay can be thought of as a lightweight descendant of X.25. Here, much of the sophisticated control functionality and facilities found in X.25 [1] are sacrificed for the sake of high speed data transmission. Moreover, identification of the virtual channel now takes place at the data link layer instead of the network layer as in the case of X.25. As a result, Frame Relay gives an order of magnitude improvement in network throughput over X.25.

There are two types of Frame Relay connections : *permanent virtual connections* (PVCs), and *switched virtual connections* (SVCs). The establishment, maintenance, and release of PVCs are subject to local management operations. On the other hand, signalling is required to manage SVCs. Dynamically allocated SVCs are more attractive than the PVCs which function as dedicated private lines. At present, the Frame Relay implementations are primarily PVC-based. This is due to both the complexity of the required signalling and its unavailability on the local loop [5]. There is a growing demand for products supporting SVCs. However, PVCs provide a good immediate solution for LAN to LAN interconnectivity applications.

The Frame Relay interface is based on the core functions of the LAP-F protocol. This protocol is defined in the CCITT Rec.Q.922, and it is also sometimes referred to as Rec.I441* (* stands for extended). LAP-F allows the existence of multiple instantaneous logical sessions (statistical multiplexing) within a single physical channel. The transferred service data units appear in the form of frames. An attached logical identifier (DLCI) with local significance is used to identify the virtual circuit this frame belongs to.

addressing of frames, detection of errors (but not with recovery of frames in error), and supports some basic congestion control. The second sublayer is called DL-CONTROL, and it implements the actual control functionality of LAP-F. It is strictly concerned with information included within the control field of the LAP-F frame. This sublayer offers reliable transfer of information enabling the acknowledgement of frames and the recovery of lost frames. The Frame Relay interface implements only the functionality of the DL-CORE sublayer.

In principle, the connection-oriented service offered by Frame Relay addresses either data or circuit type traffic. Simultaneous support of both types of traffic may also take place. For example, packetized voice and data can be transferred over the same virtual connection offered by the Frame Relay interface during a LAN to LAN interconnection.

In a Frame Relay network, DLCI values at the DL-CORE level are used to identify the communication path. Given this, all the routing information in a Frame Relay network is provided within the interface, that is, at a lower level than the network level. Consequently, the network layer may become redundant during the data transfer phase. The main tasks of the adaptation layer are to segment the resulting bitstream into small information units that the underlying technology can handle, and to preserve the required synchronization. In some technologies such as DQDB and B-ISDN, the adaptation layer forms part of their interfaces. This is not the case with Frame Relay, where it has to be provided on top of its interface.

5.2 Secure Frame Relay Connections (SFRC) Layer

The placement of security within the Frame Relay interface can logically occur at the physical layer, or can be integrated into the DL-Core sublayer, or can be at the top of the DL-CORE layer. Following the discussions in Section 4, it is proposed that the Secure Frame Relay Connections (SFRC) layer operates on top of the DL-CORE sublayer (See Figure 2).

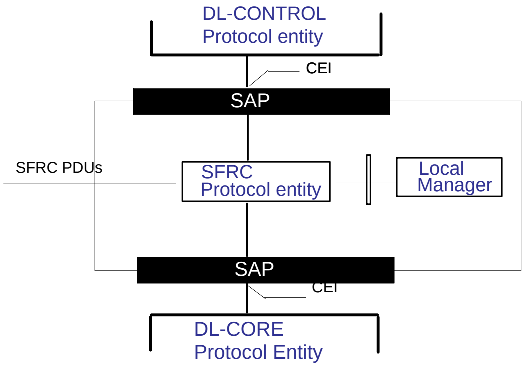

Fig. 2: Secure Frame Relay Connections (SFRC) Layer

Note that SFRC is different to the IEEE 802.10 SDE layer in that it should be able to cope with situations where there is no MAC sublayer. Consider for instance an user equipment accessing the Frame Relay interface either directly or by being connected to it via an ISDN interface. Here the MAC sublayer is absent and a data link protocol (e.g. LAPF) is used to pass the traffic over a multidrop line shared by several terminals. Another example may be a video-conferencing application between two studios over an ATM-based core network, where an internetworking device implementing a Frame Relay interface is providing access to the ATM network. An adaptation layer can be used to handle the bit streams from

Hence the need for SFRC layer to protect the different types of Frame Relay traffic. The SFRC should be able to support the security services required during both the call control phase and the data transfer phase of the Frame Relay.

The SFRC sublayer comprises one or more entities, each providing security services to an individual frame relay virtual connection. Communication between SFRC entities located in remote systems is achieved in terms of the SFRC protocol. The message units related to a connection are exchanged between the SFRC and its adjacent (sub) layers via points identified by the endpoint identifiers (CEIs).

The services offered by the SFRC are specified by describing the information flow to the layer immediately above (SFRC-user) and to the layer below (DL-CORE) in terms of service primitives. By having the SFRC sublayer operate on top of the Frame Relay interface in a transparent way, the primitives used across the service interface of the SFRC sublayer and the higher sublayer are identical to those supported by the DL-CORE sublayer. Parameters associated with the SFRC-DATA primitives are identical to those found in the corresponding DL-CORE primitives. The SFRC sublayer only processes the DL-CORE-User data field of a primitive; all other parameters are transferred transparently. These parameters are defined in Annex C of CCITT Rec.I.233.

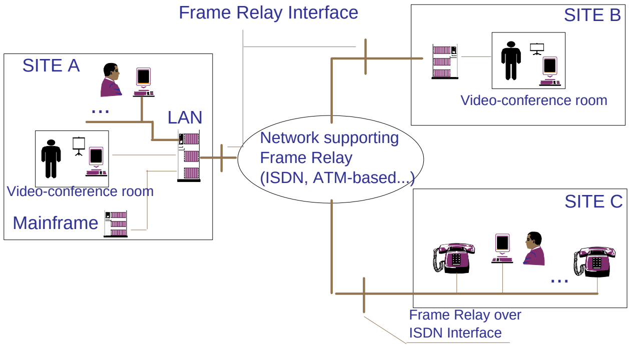

Fig. 3: Topology restricting the use of SDE

5.3 SFRC Layer Security Services

The SFRC layer supports the following security services : data origin authentication, access control, connection confidentiality and connection integrity without recovery. In addition to these, associated with the call setup phase of the SVCs, support is provided for peer authentication, establishment of a secret dialogue key, and release of a connection in an authorized manner. Furthermore, the protocols between the SFRC layer managers support secure negotiation of a session between their local SFRC entities, dynamic activation and deactivation of the negotiated security mechanisms during the data transfer phase, and renegotiation of the secure connection while the connection is still in place.

The structure of a SFRC protocol data unit is shown in Figure 4. It consists of four parts: a clear header, a protected header, user information field, and a trailer. Each of these PDU parts is further subdivided into a number of fields.

The Secure Connection Identifier (SC-ID) value associates the SFRC PDU with a secure frame relay connection at the destination frame relay interface. We recommend the use of the DLCI values as SC-IDs. Connection confidentiality is provided by encrypting the User Info. Connection integrity without protected for both confidentiality and integrity. Data origin authentication is provided by guaranteeing the association of frames with the virtual path over which the frames are transferred. This is done by having a unique shared key between the SFRC entities at the end points of a Frame Relay connection. A fuller description of the security services can be found in [14]. The access control mechanism determines which SFRC entities can communicate with each other, which in turn determines which entities can establish a secure conversation key. We discuss the secure call setup in Section 5.

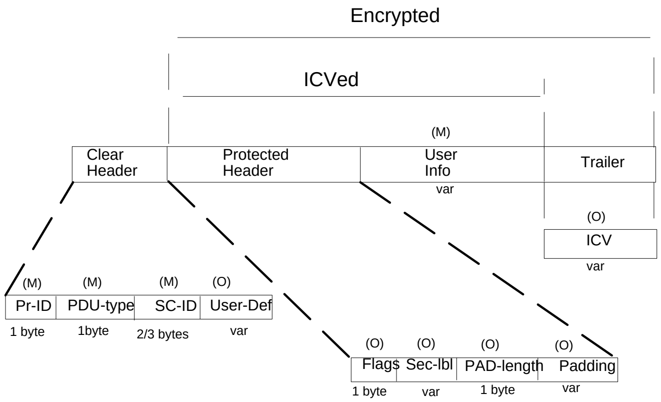

Fig. 4: SFRC Protocol Data Unit

Just a brief explanation for not including the connection integrity with recovery and traffic flow confidentiality security services.

Connection integrity with recovery service : In contrast to SP4 [11] and TLSP [12] which can access the sequence numbers of the transport layer, the SFRC has no access to such infomation in the DL-CORE sublayer. It is for this reason the ISO 7498-2 considers the provision of the connection integrity with recovery service at the transport layer and not at the network layer. Hence deletion of a protected SFRC PDU will only be detected by a higher sublayer (e.g. DL-CONTROL or transport layer), and retransmission will be requested. But in this case, the SFRC sublayer has no knowledge of this event. However, inclusion of an invalid PDU will be detected by the SFRC even when the attacker has knowledge of the current sequence number. This is because the attacker does not have access to the integrity and/or encryption key(s) used by the SFRC.

Traffic flow confidentiality service : Two security mechanisms can be used to support this service : routing control and traffic padding. The first case allows the routing