# An Overview of Network Architecture and security framework of Asynchronous Transfer Mode

**Niraj Nake**
Department of Electronics and Telecommunication, PRMCEAM, Badnera-Amravati

***Abstract-*** Asynchronous Transfer Mode (ATM) has emerged as most promising technology in supporting broadband multimedia communications. Congestion control plays important role in the effective and stable operation of ATM networks. The management of these networks creates new challenges for both private network operators and public telecommunications service provider communities due to the heterogeneous mix of ATM Switch equipment, and the need to establish, control and monitor end-to-end connections (virtual circuits) through a network. ATM is a standard for carriage of a complete range of user traffic, including voice, data, and video signals. It is designed to unify telecommunication and computer networks. It uses asynchronous time-division multiplexing and it encodes data into small, fixed-sized cells. ATM provides data link layer services that run over a wide range of OSI physical Layer links. ATM has functional similarity with both circuit switched networking and small packet switched networking. It was designed for a network that must handle both traditional high-throughput data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video.

***Index Terms***- ATM Networks, Congestion, VP, VC, VPI, VCI, OSI model

## I. Introduction

There are lot of high speed networking technologies used to transfer data between two or more devices. Asynchronous Transfer Mode is one of these technologies. ATM's speed, low latency and ability to handle all types of traffic over a single network make it ideal for a range of bandwidth-intensive applications, including multimedia, medical imaging and more.One difference between ATM and other networking technologies is the concept of "virtual circuits".Negotiating a virtual circuit with nominated bandwidth and quality of service parameters is a feature of ATM circuit provisioning.VP's in asynchronous transfer mode (ATM) networks provide substantial speedup during the connection establishment phase at the expense of bandwidth loss due to the end-to-end reservation of network resources. Thus, VP's can be used to tune the fundamental tradeoff between the network call throughput and the processing load on the signaling system. They can also be used to provide dedicated connection services to customers such as virtual networks (VN's).ATM operates as a channel-based transport layer, using virtual circuits (VCs).ATM became popular with telephone companies and many computer makers in the 1990s. ATM operates at the data link layer (Layer 2 in the OSI model) over either fiber or twisted-pair cable.Asynchronous Transfer Mode (ATM) is a technology that has the potential of revolutionizing data communications and telecommunications.

## II. Necessity

### 2.1 Frame Network

Before ATM, data communications at the data link layer had been based on frame switching and frame networks. Different protocols use frames of varying size and intricacy. As networks become more complex, the information that must be carried in the header becomes more extensive. The result is larger and larger headers relative to the size of the data unit. In response, some protocols have enlarged the size of the data unit to make header use more efficient (sending more data with the same size header). Unfortunately, large data fields create waste. If there is not much information to transmit, much of the field goes unused. To improve utilization, some protocols provide variable frame sizes to users.

### 2.2 Mixed Network Traffic

As we can imagine, the variety of frame sizes makes traffic unpredictable. Switches, multiplexers, and routers must elaborate software systems to manage the various sizes of frames. A great deal of header information must be read, and each bit counted and evaluated to ensure the integrity of every frame. Internetworking among the different frame networks is slow and expensive at best, and impossible at worst. Another problem is that of providing consistent data rate delivery when frame sizes are unpredictable and can vary so dramatically. To get the most out of broadband technology, traffic must be time-division multiplexed onto shared paths.

### 2.3 Cell Networks

Many of the problems associated with frame internetworking are solved by adopting a concept called cell networking. A cell is a small data unit of fixed size. In a **cell** network, which uses the **cell** as the basic unit of data exchange, all data are loaded into identical cells that can be transmitted with complete predictability and uniformity. As frames of different sizes and formats reach the cell network from a tributary network, they are split into multiple small data units of equal length and are loaded into cells. The cells are then multiplexed with other cells and routed through the cell network. Because each cell is the same size and all are small, the problems associated with multiplexing different-sized frames are avoided.

### 2.4 Asynchronous TDM

ATM uses asynchronous time-division multiplexing-that is why it is called Asynchronous Transfer Mode-to multiplex cells corning from different channels. It uses fixed-size slots (size of a cell). ATM multiplexers fill a slot with a cell from any input channel that has a cell; the slot is empty if none of the channels has a cell to send. When all the cells from all the channels are multiplexed, the output slots are empty.

## III. ARCHITECTURE

ATM network is switched network. It's architecture uses a logical model to describe the functionality it supports. ATM functionality corresponds to the physical layer and the data link layer of the OSI reference model.

The ATM reference model is composed of the following planes, which span all layers:

- *Control*-This plane is responsible for generating and managing signaling requests.
- *User*- This plane is responsible for managing the transfer of data.
- *Management*-This plane contains two components:
  -Layer management manages layer-specific functions, such as the detection of failures and protocol problems.
  -Plane management manages and coordinates functions related to the complete system.

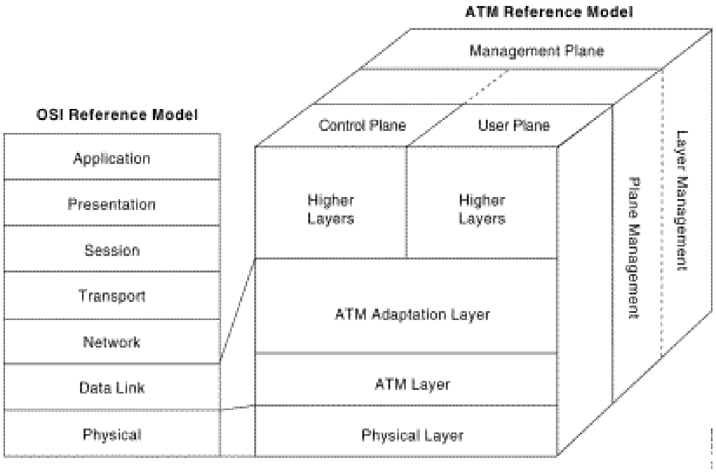

**Figure 1:Relating layers of OSI and ATM model.**

The ATM reference model as shown in figure 1,is composed of the following ATM layers:

- *Physical layer*-Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.
- *ATM layer*-Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for establishing connections and passing cells through the ATM network. To do this, it uses information in the header of each ATM cell.
- *ATM adaptation layer (AAL)*-Combined with the ATM layer, the AAL is roughly analogous to the data data-link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes.

### 3.1 The ATM Physical Layer

The ATM physical layer has four functions: bits are converted into cells, the transmission and receipt of bits on the physical medium are controlled, ATM cell boundaries are tracked, and cells are packaged into the appropriate types of frames for the physical medium. Examples of physical medium standards for ATM include Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH), DS-3/E3, 155 Mbps over multimode fiber (MMF) using the 8B/10B encoding scheme, and 155 Mbps 8B/10B over shielded twisted-pair (STP) cabling.

### 3.2 ATM Adaptation Layers: AAL1

AAL1, a connection-oriented service, is suitable for handling circuit-emulation applications, such as voice and video conferencing. Circuit-emulation service also accommodates the attachment of equipment currently using leased lines to an ATM backbone network. AAL1 requires timing synchronization between the source and destination. For this reason, AAL1 depends on a medium, such as SONET, that supports clocking. The AAL1 process prepares a cell for transmission in three steps. First, synchronous samples are inserted into the Payload field. Second, *Sequence Number* (SN) and *Sequence Number Protection* (SNP) fields are added to provide information that the receiving AAL1 uses to verify that it has received cells in the correct order. Third, the remainder of the Payload field is filled with enough single bytes to equal 48 bytes.

### 3.3 ATM Adaptation Layers: AAL2

Originally AAL2 was intended to support a variable-data-rate bit stream, but it has been redesigned. It is now used for low-bit-rate traffic and short-frame traffic such as audio (compressed or uncompressed), video, or fax. A good example ofAAL2 use is in mobile telephony. AAL2 allows the multiplexing of short frames into one cell. The CS layer overhead consists of five fields:

- Channel identifier (CID). The 8-bit CID field defines the channel (user) of the short packet.
- Length indicator (LI). The 6-bit LI field indicates how much of the final packet is data.
- Packet payload type (PPT). The PPT field defines the type of packet.
- User-to-user indicator (UUI). The UUI field can be used by end-to-end users.
- Header error control (HEC). The last 5 bits is used to correct errors in the header.

The only overhead at the SAR layer is the start field (SF) that defines the offset from the beginning of the packet.

### 3.4 ATM Adaptation Layers: AAL3/4

Initially, AAL3 was intended to support connection-oriented data services and AAL4 to support connectionless services. As they evolved, however, it became evident that the fundamental issues of the two protocols were the same. They have therefore been combined into a single format calledAAL3/4.AAL3/4 provides comprehensive sequencing and error control mechanisms.AAL3/4 prepares a cell for transmission in four steps. First, the *convergence sublayer* (CS) creates a *protocol data unit* (PDU) by prepending a beginning/end tag header to the frame and appending a length field as a trailer. Second, the *segmentation and reassembly* (SAR) sublayer fragments the PDU and prepends a header to it. Then, the SAR sublayer appends a CRC-10 trailer to each PDU fragment for error control. Finally, the completed SAR PDU becomes the Payload field of an ATM cell to which the ATM layer prepends the standard ATM header.

### 3.5 ATM Adaptation Layers: AAL5

AAL5 is the primary AAL for data and supports both connection-oriented and connectionless data. AAL5 also is known as the simple and efficient adaptation layer (SEAL) because the SAR sublayer simply accepts the CS-PDU and segments it into 48-octet SAR-PDUs without adding any additional fields. AAL5 prepares a cell for transmission in three steps. First, the CS sublayer appends a variable-length pad and an 8-byte trailer to a frame. The pad ensures that the resulting PDU falls on the 48-byte boundary of an ATMcell. The trailer includes the length of the frame and a 32-bit cyclic redundancy check (CRC) computed across the entire PDU. This allows the AAL5 receiving process to detect bit errors, lost cells, or cells that are out of sequence. Second, the SAR sublayer segments the CS-PDU into 48-byte blocks. A header and trailer are not added (as is in AAL3/4), so messages cannot be interleaved. Finally, the ATM layer places each block into the Payload field of an ATM cell. For all cells except the last, a bit in the *Payload Type* (PT) field is set to zero to indicate that the cell is not the last cell in a series that represents a single frame. For the last cell, the bit in the PT field is set to one.

## IV. THREATS

As other networks, ATM networks will suffer a lot of threats. Typical ones are eavesdropping, spoofing, service denial, VC stealing and traffic analysis etc. Notice that VC stealing and traffic analysis happen only in ATM networks.

### 4.1 Eavesdropping

Eavesdropping refers to the threat that the attacker connects or taps into the transmission media and gain unauthorized access to the data. It is one of the most common attacks to the network. Since most ATM networks are connected with optic cables, some people might get the wrong impression that is not so easy to tap a ATM network.

### 4.2 Spoofing

Spoofing attack means that an attacker tries to impersonate another user to the third part therefore can get access to resources belonging to the victim to take advantages or just destroy them. Spoofing might need special tools to manipulate the protocol data unit. And sometimes it might require the attacker has special access permission, say,must be the super user in UNIX environment. However, since a network will be connected to many untrusted networks via the Internet, it's impossible to prevent a hacker from getting this access permission or even trace the people with this particular access permission. ATM is being implemented in public domain. Therefore, it is subject to this kind of attack also.

### 4.3 Service Denial

ATM is a connection-oriented technique. A connection, which is called Virtual Circuit(VC) in ATM, is managed by a set of signals. VC is established by SETUP signals and can be disconnected by RELEASE or DROP PARTY signals. If an attacker sends RELEASE or DROP PARTY signal to any intermediate switch on the way of a VC,then the VC will be disconnected. By sending these signals frequently, the attacker can greatly disturb the communication between one user to another, therefore will disable the Quality of Service(QoS) in ATM. Combining this technique with other tricks like eavesdropping, the attacker can even completely block one user from another.

### 4.4 Stealing of VCs

If two switches in an ATM network compromise, the attacker can even steal a VC from another user. Say VC1 and VC2 are two virtual channels which will go through switch A and switch B. VC1 is owned by user U1 and VC2 is owned user U2. If A and B have compromised, then A can switch VC1's cells going from A to B through VC2 and B will switch back those cells to VC1. Since switches will forward cells based on the VCI(Virtual Channel Identifier) or VPI(Virtual Path Identifier) in the cell header, A and B can just alter these fields back and forth. Switches between A and B won't notice these changes and will switch the assumed VC2's cells just like the authentic VC2's cells. In public packet-switching network, U1 won't gain too much by this trick. However, in ATM network, if quality of service is guaranteed, then user 1 can gain a lot by stealing a higher quality channel which user 1 is not entitled to use according to the access control policy. User 1 can gain even more if every user has to pay for the communication. In both cases, user 2 will be hurt. Someone maybe argues that the possibility that the switches will compromise is pretty low. That will true if the ATM network is owned by one organization. when we consider ATM internetworking, in which case cells will travel through different ATM networks, it will be very easy for two switches to compromise.

### 4.5 Traffic Analysis

Traffic analysis refers to a threat that the hacker can get information by collecting and analyzing the information like the volume, timing and the communication parties of a VC. Volume and timing can reveal a lot of information to the hacker even though the data is encrypted, because encryption won't affect the volume and timing of information. And also the source and destination parties can be obtained from the cell header (normally is in clear text) and some knowledge about the routing table. Another related threat is called convert channels. In this technique, the attacker can encode the information in the timing and volume of data, VCI, or even session key to release information to another people without being monitored. Normally, these two attack won't happen. However,when ATM is used in a environment requiring stringent security, it might happen.

## V. SECURITY FRAMEWORK

People have practiced security for a long time. In the past, security services were considered only after the network service was totally designed. These ad hoc approaches turn out to be unsatisfactory.

ATM Forum tries to avoid such pitfalls by considering the security as one integrated part of ATM. Recently, ATM Forum Security Working Group proposes a draft of Security Framework for ATM to address the basic requirements for ATM security. Main security objectives for ATM security:

- Confidentiality
- Data Integrity
- Accountability
- Availability

Confidentiality and data integrity are obvious. Accountability means that all ATM network service invocations and network management activities should accountable. And any entity should be responsible for the actions it initiates.Accountability includes both authentication and non-repudiation. It is extremely important for operators to manage the system and bill the services. Availability means all legitimate entities should be able to access to ATM facilities correctly, no service denial should happen. That is important for QoS operation. According to these main objectives, the draft proposes the principal functions which a ATM security system should provide:

- **Verification of Identities:** Security system should be able to establish and verify the claimed identity of any actor in an ATM network.
- **Controlled Access and Authorization:** The actors should not be able to gain access to information or resources if they are not authorized to.
- **Protection of Confidentiality:** Stored and communicated data should be confidential.
- **Protection of Data Integrity:** The security system should guarantee the integrity of the stored and communicated data.
- **Strong Accountability:** An entity can not deny the responsibility of its performed actions as well as their effects.
- **Activities Logging:** The security system should support the capability to retrieve information about security activities in the Network Elements with the possibility of tracing this information to individuals or entities.
- **Alarm reporting:** The security system should be able to generate alarm notification about certain adjustable and selective security related events.
- **Audit:** When violations of security happen, the system should be able to analyze the logged data relevant to security.
- **Security Recovery:** The security system should be able recover from successful or attempted breaches of security.
- **Security Management:** The security system should be able to manage the security services derived from the above requirements.Among the ten requirements, the last two won't provide security services. However, they are necessary to support the maintenance of security services. If the security system can not be recovered from attacks and can not provide security services any more, then the system won't be secure after these attacks. On the other hand, security services and the information about security have to be managed securely. They are the foundations of the security system.

## VI. Conclusion

ATM technology perhaps is the most complex networking technology we ever have. To secure such a complex system will be even more difficult than design it. And now people just begin to discuss some issues of ATM security. It will take times for us to figure out how to completely achieve our security objectives. Because the goal of ATM is to provide a unified networking platform and communication infrastructure, ATM security , as a part of this infrastructure, has to be flexible and compatible with other technology. That will introduce more difficulties to ATM security. ATM Forum Security Working Group has come up with drafts for security specification and security framework. A lot of other security issues have been discussed in ATM Forum.ATM is capable of transporting multiple types of services simultaneously on the same network. All data is placed in cells of uniform size. The cell header contains information concerning cell routing using VCI's and VPI's. Cells from various applications with the same destination can be interleaved to share physical facilities. This allows network providers to transport different types of services using the same physical facilities. This is an advantage for network providers in that facilities can be fully utilized. It is an advantage for end users since they can connect their various networks and only pay for the data they are sending.

## References

[1] A Survey on ATM Security, http://www.cis.ohio-state.edu/~jain/cis788-97/atm_security/index.htm (4 of 14) [2/7/2000 10:51:41 AM].

[2] JAMES R. WEBSTER. Asynchronous Transfer Mode (ATM) Technology: An Overview, NRL/NR/8143--93-7337, June 4, 1993.

[3] M.Sreenivasulu, Dr. E.V. Prasad, Dr. G.S.S. Raju. Performance evaluation of rate based congestion control schemes for ATM networks, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.

[4] Nigel Cook, Robert Coote, David Horton, Geoff Thompson, And Hiroshi Suzuki1. An Openview Based Atm Network Management System, Citr Technical Journal Volume. OpenView Forum, Seattle, USA, June 1995.

[5] Nikolaos Anerousis, Aurel A. Lazar. Virtual Path Control for ATM Networks with Call Level Quality of Service Guarantees. IEEE/ACM Transactions On Networking, Vol. 6, No. 2, April 1998

## Authors

**First Author**-Niraj Babanrao Nake, Lecturer ,Department of Electronics and Telecommunication, Prof Ram Meghe college of engineering and management,Badnera-Amravati.

**Correspondence Author**-email Id: nirajnake24@gmail.com