The time efficient security for broadcast Networks

Santosh L Deshpande[1] sldeshpande@gmail.com
SDM College of Engg. and Technology
Dharwad Karnataka India.

N H Ayachit[1] nhayachit@gmail.com
BVB College of Engg. and Technology
Hubli Karnataka India.

Kamaksi Prasad V[2] kamakshiprasad@yahoo.com
JNT University Hyderabad A. P. India

Abstract

The audit ability and security of the broadcast network and security needs to be enhanced. This article is proposing the security solutions for such networks that are cost effective. The solution also takes care of the reduction of effective bandwidth-delay product. The improvement in terms of a cost effective comparator improves the efficiency and security of such networks. The threats like Eavesdropping, Interception and modification of transmitted data, Spoofing, Denial of service (DoS), Free–loading, and Accidental threats are some of the threats addressed in this article.

Keywords: Broadcast Networks. Hardware security, Bandwidth delay product. Parallel timing

1 Introduction:

The development or improvement in the broadcast networks is very valuable as these systems are cost effective. The fundamental drawback for the broadcast network is auditing of the system. LAN as broadcast network it never built up with the intension of security as auditing such a system is most difficult. The mechanism of this kind is totally missing in the LAN. The medium access control protocols are less efficient but in such networks cost effective.[1] Hence it is very difficult to find the golden lining between the efficiency (e.g. throughput) and the security (e.g. eavesdrop).

This article highlights the problem and tries to find the hard-wired solution to this. The hardware or the software need the same time in the LAN due to the problem of Bandwidth delay product leading to the major hurdle. The time required by LAN to transmit the information from a host to a destination is given by the equation number 1.Tprop=Time for the propagation in the medium.

Tproc=Time for processing the data.
Tframe=Time for the frame transfer.

The aim is to optimize on the Tproc, which is the dynamic factor and changes from one system to another. Total time required to transmit a frame is always

T= Tprop+ Tproc +Tframe………Equation 1

Of all these three times Tproc is the time that is totally dependent on the network program. The ability to execute this depends on the processor speed. This highly affects the normalized Bandwidth delay product, as maximum Tproc is taken in into the account. Further the efficiency ρ= Reff /R of the network is affected because Reff is inversely proportional to the normalized bandwidth delay product. Here Reff is the effective bit rate and R is the bit rate of the carrier.

Another important issue is all the packets travel till the network layer making it possible to grab other users' information. This raises issue of security of the information in the network. Unnecessary parallel processing of the other systems to deny the frame is reduced.

In this article an effort has been made to address the above-mentioned issues in the LAN by slightly changing the hardware design and checking of the packet at the rate of reception. All the LAN structures can be mapped to OSI models. The OSI Models mapped with different types of LANs is shown in the figure 1(a) and 1(b) respectively.

In the LAN the system that wants to communicate broadcasts the message in the media. The message remains in the media till the bandwidth delay product time. This information is processed by all the machines till the MAC sub layer, which is a software program. The effective total time of the system is null to the extent explained herewith. If a total of n systems are in the network, time lost in unnecessary computation is n-2 to other computers for which the packet needs to be dropped. That is the network as a whole will lose (n-2)* tproc.

As mentioned above the security threats for such network against are too many. [4] The wired and wireless less LANs use authentication techniques to use its recourses. Eavesdropping, Interception and modification of transmitted data, Spoofing, Denial of service (DoS), Free–loading, and Accidental threats are the common problems in terms of the security. Thus, data when under the peer process for processing it is under the threat. [4]

The method proposed in this article is not only dealing with saving of the time in broadcast network but also makes an attempt to give solution to such attacks.

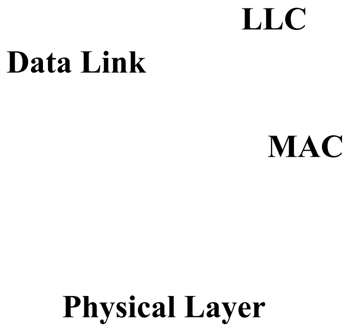

Fig 1(a). OSI Layer

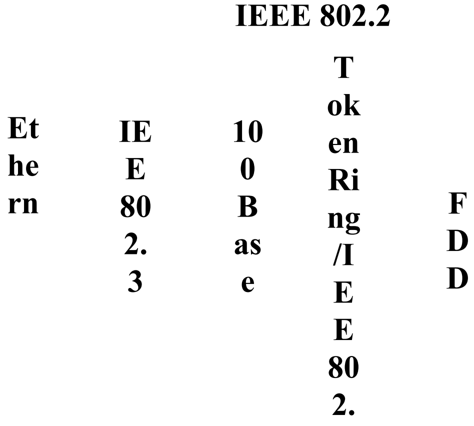

Fig 1(b). LAN **Specification**

2 The proposed system:

The hardware security blocks the data at the physical layer through MAC address. With the help of a comparator compares the MAC address with the help of a comparator preventing it to get in to the peer process such that the LLC layer cannot access it. This will prevent the nonlegitimate packets to enter in to system.

Use a comparator that uses selection sorting technique so that the system being faster than the software driven method.

The proposed will work as follows after the suggested change. All the comparators will sense the start of the frame. They will accept the start of and read the address in the frames. If the address is of the true owner then only LLC layer will be invoked and processor will be interrupted, else the packet will be dropped. Even the broadcast condition also can be checked in the same comparators. This will prevent any unauthenticated user to eavesdrop in the other user's data packet.

The Tproc will be reduced such that in turn will reduce the bandwidth delay product as bandwidth is usually a larger term and delay is smaller.

Manchester line coding is followed in Ethernet and it's a self-clocked code that can trigger the register of the comparator automatically. [5] Thus the implementation of this system is also expected to be cost effective in terms of keeping the system audited for security. All the registers have to be numbered and can be authenticated by the system administrator. The diagram 2 gives the schematic representation about the implementation of such a system.

1 Analysis of the system:

The above scheme is analyzed for different possible threats. Table 1 discusses the pitfalls, nature of the problem and proposed solution in the system. [2]

Figure 2. Proposed Schema

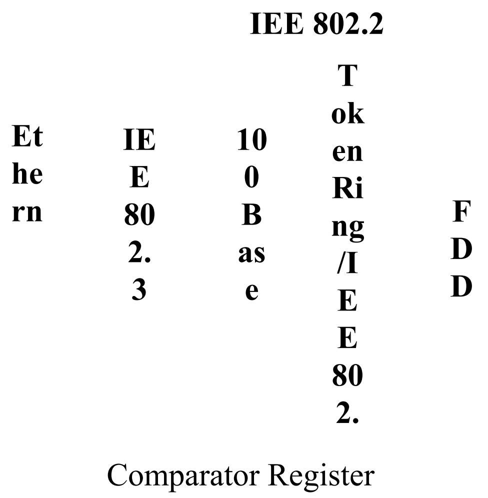

Table 1. The analysis of the system.

The pitfall	Nature of problem	Solution by the proposed system
Interception and modification of transmitted data	Attacker can gain access to the network, he or she can insert a rogue computer to intercept and modify network data communicated between two legitimate parties	The only legitimate users will have the access, as the register will not interrupt the computer processor.
Eavesdropping	Disclosure of confidential data, disclosure of unprotected user credentials, and the potential for identity theft. It also allows sophisticated intruders to collect information about your IT environment, which can be used to mount an attack on other systems or data that might not otherwise be	The registers in the comparators will let the data come into the system only if it is matched hence this possibility will be ruled out. The admin will not let the system that is not registered with its comparator will not be allowed to access.

	vulnerable.	
Spoofing	Ready access to an internal network allows an intruder to forge apparently legitimate data in ways that would not be possible from outside the network, for example, a spoofed e–mail message. People, including system administrators, tend to trust items that originate internally far more than something that originates outside the corporate network	Ready access does not exist in the present system.
Free–loading	An intruder may want nothing more sinister than to use your network as free point of access to the Internet. Though not as damaging as some of the other threats, this will, at the very least, not only lower the available level of service for your legitimate users but may also introduce viruses and other threats.	Intruder can not be identified by the proposed system

3 Conclusion:

The method proposed is proposed for a better performance of broadcasting network such that security and audit ability increases and at the same time performance of the system is efficient with respect to time. In spite of, all these system will be cost effective. The system blocks the data at the physical layer than the LLC.

4 References:

1. A. Escudero, B. Pehrson, E. Pelletta, J.O. Vatn, P. Wiatr, “Wireless access in the lyinglinux. NET infrastructure: Mobile IPv4 integration in a IEEE 802.11b”, 11th IEEE Workshop on Local and

2. Metropolitan Area Networks, LANMAN2001, Co,USA, March 2001.TDM local access published as a white paper by CISCO in 2005

3. Intel Building Blocks for Wireless LAN Security 2003

4. Detecting Wireless LAN MAC Address Spoofing Joshua Wright, GCIH, CCNA 2003

5. 2nd edition Lion Garcia and Indra Wadija Data Communication 2005