A New Approach to Design Programmable Secure Network Interface Card

Darshana Hooda
System Analyst
DCRUST, Murthal

Parvinder Singh, PhD.
Associate Professor
Computer Science & Engg.
DCRUST, Murthal

ABSTRACT
In this paper, Secure Network Interface Card (SNIC) Architecture is proposed, to provide secure video communication without extra overhead on host processor of receiver. PROM based security model is developed & its integration with Network Interface is described. The approach adopted here to design SNIC, is based on remote reference passing. In this approach PROM is integrated to NIC to serve as security buffer where data values are to be placed at memory locations using some mathematical mapping which establishes relation between location reference and data. Sender generates respective location reference(at receiver's security buffer) corresponding to the each data byte of video stream. For reference creation, respective reverse mathematical mapping is used. In this, security is achieved at MAC layer at receivers end.

General Terms
Security

Keywords
SNIC, NIC, Encryption, Decryption, Memory, security module, PROM, Remote References.

1. INTRODUCTION
In present, the role of computers in society has undergone a dramatic shift from stand alone processing devices to networked systems. Further, recent advances in multimedia compression, communication technologies and abundant availability of low cost constrained display devices, have led to phenomenal growth of digital multimedia services and applications video chat, video conferencing, telemedicine & variety of entertainment services. Multimedia applications demands high performance network servers, to cope up with critical time bound processing; network interface cards (NIC) will have a significant impact on a system performance. Generally network interface cards perform simple tasks to allow the host processor to transfer data between the main memory and the network, typically Ethernet. As these tasks are fixed and well defined, so most NICs use an Application Specific Integrated Circuit (ASIC) controller to store and forward data between the host system memory and the network(Ethernet). Today networking is an integral part of modern computer systems. While the network interface has traditionally been a simple device that forwards raw data between the network and the operating system, but now its role is changing[9]. More sophisticated/specialized network interfaces are being developed every day that perform functions such as TCP offloading [1], iSCSI [2], encryption and firewalling [3], remote direct memory access [4], and so on. Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier and common than compromising physical or local security because of openness of network. Network security offers measures to protect network and related resources from unauthorized access, monitor and determine its effectiveness. In this work network security is introduce at physical layer significant to video transmission. An approach to design fast and secure network interface card has been introduced here. This secure network interface card is designed by introducing a new security module inbuilt with network interface card and the controller in the NIC must be able to extract the header and data. In security module MAR, MDR and ROM is introduce for security purpose. The architectures can be verified in real environment, and potential implementation bottlenecks can be identified. Thus, what is needed is a platform, which combines the performance and efficiency of special- purpose hardware with the versatility of a programmable device [5]. Architecturally, the platform must be processor-based and must be largely implemented using a configurable hardware. An FPGA with an embedded processor is a natural fit with this requirement [6].

Video security is one of the key issues that we have taken in to account in this paper. Providing a secure mechanism to real time communication in heterogeneous environment along with taking care of display/browsing devices with limited processing capability is very challenging. In network technologies security protocols like IPsec and transport layer protocol are introduced. But in this way adding the security, the packet size increased and, once the packet size is increased, the processing time increases adding additional delay during the transmission and this increased delay is highly undesirable in streaming of video. Keeping in the view, all above innovation in NIC is proposed to offer security at MAC layer without any additional packet payload. Hence proposed MAC layer security is better approach to offer confidentiality and authentication to the communication without introducing additional delay and payload to the packet.

2. VIDEO SECURITY
Now a days nearly all companies, gov. agencies, educational institutes and home users depend on computer system and communication system. Dependency on digitized information in recent time makes information more vulnerable for abuse , situation is even worse when information travels from one point to other point. If there are security problems in information and communication systems, user will fear that their sensitive information may be monitored, altered and can be stolen. For these reasons it is important to make information &n communication system more secure by protect data resources from malicious acts. Crypto Algorithms are the core of conventional security system however watermarking and finger printing techniques are evolving rapidly to address other security needs i.e. copy right

protection etc. of multimedia applications. Multimedia services can be broadly classified in to entertainment service & communication services. Both services have different security needs .Confidentiality is critically needed for communication services while copy right protection is vital for entertainment applications.

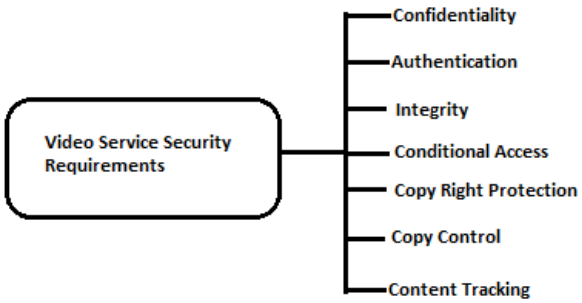

Figure 1:Basic Video Security Services

Multimedia encryption is a technology that applies to digital multimedia to protect confidentiality of the media content, prevent unauthorized access, and provide persistent access control and rights management of the content . It is a special application of general encryption that the representation of multimedia is encrypted such that the content cannot be rendered intelligibly or to an acceptable perceptual quality. And beyond that Real-time video streams have stringent requirements for end-to-end delay and loss during network transport. Multimedia encryption has a number of unique issues that are not seen in text encryption and plays a critical role in modern digital multimedia services and applications.

The most important are certainly the protection of information & authentication, achieved using digital signatures. Hash functions generally maps an input of arbitrary length to a string of fixed length, the hash code and if these mappings are widely used to check integrity of received information. Other cryptographic applications where hash functions are useful are the optimization of digital signature schemes, the protection of passphrases and the commitment to a string without revealing it. Hash functions evolved when it was realized that encryption is not sufficient to protect authenticity of transmitted information. The simplest example is the encryption with a block cipher in Electronic Code Book (ECB) mode, where every block is encrypted independently. It is clear that an active attacker can easily modify the order of the cipher text blocks and hence of the corresponding plaintext blocks. It will be shown that cryptographic hash functions allow for efficient constructions to protect authenticity with or without secrecy. Cryptographic hash functions are a useful tool in the protection of information integrity. Therefore the need exist for provably secure in terms of privacy and efficient constructions duly taking care of current challenges like heterogeneous networking environment, availability of enormous display devices with varying degree of processing capability & other resources. For the time being only a limited number of provably secure constructions exist, that is very inefficient.

In this paper we have proposed secure network interface architecture, targeting the stringent requirements of video transmission.

3. BACKGROUND :NETWORK INTERFACE CARD

Network interface card, usually referred as NIC, act as physical interface or connection between the computer and network cable. NICs facilitate the transmission and receipt of frames between the networks and host operating system.
Network interface cards faclitates the operating system to send and receive the packets to the network. The operating system stores and retrieves data from the main memory and communicates with the NIC over the local interconnect, known as peripheral component interconnect bus . Most NICs have a peripheral component interconnect bus hardware interface to the host server. NIC device driver facilitates host processor to communicate with the operating system and use local receive and transmit storage buffers. NICs hosts a direct memory access (DMA) engine to transfer data between host memory and the network interface memory. Further, NICs have a medium access control (MAC) unit, which implements the link level protocol for the underlying network such as Ethernet, and use a signal processing hardware to implement the physical (PHY) layer defined in the network [7].

Basic NIC Architecture & Operation:

As shown in the block diagram shown in fig.2, most NICs have a DMA interface unit, a medium access control unit, memory, and control logic. In the case of a programmable NIC, the control logic is one or more programmable processors that run compiled-code firmware. The DMA unit is directed by the on board control logic to read and write data between the local NIC memory and the host's memory. The medium access unit interacts with the control logic to receive frames into local buffer storage and to send frames from local buffer storage out onto the network. The memory is used for temporary storage of frames, buffer descriptors, and other control data [8].

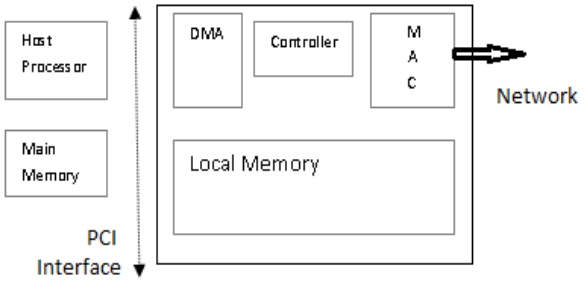

Figure 2:Network Interface Architecture

Transmission Mode:

- The host operating system is interrupted that a frame is in host memory and is ready to be sent. The OS prepares a buffer descriptor regarding this frame in host memory.
- The OS notifies the NIC about that a new buffer descriptor is in host memory and is ready to be fetched and processed. This is generally referred as a "mailbox" event.

- The NIC initiates a direct memory access (DMA) read of the pending buffer descriptor and processes it.
- Having determined the host address of the pending frame, the NIC initiates a DMA read of the frame contents.
- When the all segments of the frame (which may use several buffer descriptors and buffers) have arrived, the NIC transmits the frame out onto the Ethernet.
- Depending on how the OS has configured the NIC, the NIC may interrupt the host to indicate that the frame has completed.

Receiving Mode:

For this, OS creates buffer descriptors that point to free regions in host memory and that the NIC has read these buffer descriptors into local NIC memory via DMA [8].

- The NIC receives a frame from the network into its local receive buffer.
- Presuming there is enough host memory available for this received frame, the NIC initiates a DMA write of the frame contents into host memory. The NIC determines what the starting host address is by examining the next free buffer descriptor (which it has previously fetched).
- The NIC modifies the previously fetched buffer descriptor regarding the space that the new frame now occupies; the NIC fills in the frame length and possibly checksum information. After modifying this buffer descriptor, the NIC initiates a DMA write of it to the host.
- Depending on how the OS has configured the NIC, the NIC may interrupt the host to indicate that a frame has arrived.

As depicted in the transmission and receiving cases, NIC processing breaks up into several steps, some of which have very long latencies (e.g., waiting for DMAs to complete, waiting for frames to arrive, and so forth). To tolerate these latencies, NIC firmware uses an event model of computation. Events are typically associated with the completion of one of the NIC processing steps (as previously outlined) that require further processing. In the event model, the processors wait for events to arrive and then dispatch specific event handlers to process the newly-arrived events. These handlers may, for example, enqueue new long-latency I/O operations which will eventually trigger more events. After each event handling functions return, the processors resume waiting for other events. Hence, the processors can overlap processing of intermediate steps of a frame with latencies associated with another frame.

4. PROPOSED WORK

High performance networking technologies have made multimedia applications increasingly popular like Video on demand, Internet television, Video telephony and video conferencing. In open network, confidentiality and authentication is one of the main concerns for its users. A variety of video encryption algorithms have been proposed in order to fulfill the specific requirements raised by the peculiarities of video communication. However, the design of fast video encryption algorithm with a high security level remains, therefore there is still need to evolve a fast method to offer good level of security for video transmission [10]. Network is too vulnerable to security issues because during the designing of network architecture security has not taken in to consideration to counter the threats. But in today's scenario, it is mandatory to deploy security services to protect critical multimedia communication over network. The network interface card has traditionally been a simple device that fundamentally required for computer systems to simply forward raw data between the network and the operating system, but now its role is changing and there is need to evolve NIC to provide secure communication.

In this a fast and secure network interface card has been proposed to meet security requirements of video communication for confidentiality & authentication. In order to increase the security at MAC layer a new network interface card architecture is introduced, in which decryption of data achieved using dereferencing at receiver side. To achieve this a security module is integrated with network interface card. This secure NIC works on the concept of remote reference passing concept. Remote reference passing mechanism is based on client server architecture. Sender device is high end server while receiving device may be with limited computational capabilities. In remote reference creation approach, encryption at sender side takes place at application layer while as decryption at receiver side takes place at MAC layer. In this paper only decryption as dereferencing at MAC layer is discussed. SNIC is designed to decrypt the data by referring the memory location where intended data is stored, transmitted by the sender.

Under this work, security module as in fig 4 is proposed and integrated with NIC as in fig 3. NICs connected to host system via a local interaction such as PCI bus. A device driver running on the host system is responsible for communication with the NIC over this interconnection. Traditionally NIC itself has small amount of memory as a transmit(TX) and receive(RX) buffer known as local memory. These separate buffers are connected to MAC Controller which implements the link level protocol. The MAC is attached to a physical interface(PHY) which performs the actual signal processing necessary to send the signal on the copper, wireless, or optical network[Technical Report TREE0611]. Transmission of packet over network is as per generic NIC. The process employed by a generic NIC, to receive a packet from the network is only modified in proposed SNIC.

Medium Access Controller performs the frame parsing resulted in defragmentation and de-concatenation, as for generic NICs. In proposed SNIC architecture, after frame parsing, MAC forward intended header information directly to RX buffer after stripping off from received packet but data is forwarded towards the security module rather than to RX buffer. As in proposed method sender has transmitted the data as references to memory locations of PROM, where actual data is stored. Security module is consisting of MAR, Selector Circuite, MDR, so data is transferred from MAC to MAR and thereafter selector activates the memory location pointed by MAR data i.e. address stored in MAR, now data from activated memory is transferred to the MDR. From MDR data is shifted to receiver buffer.

The block diagram in fig 3 shows the proposed work:

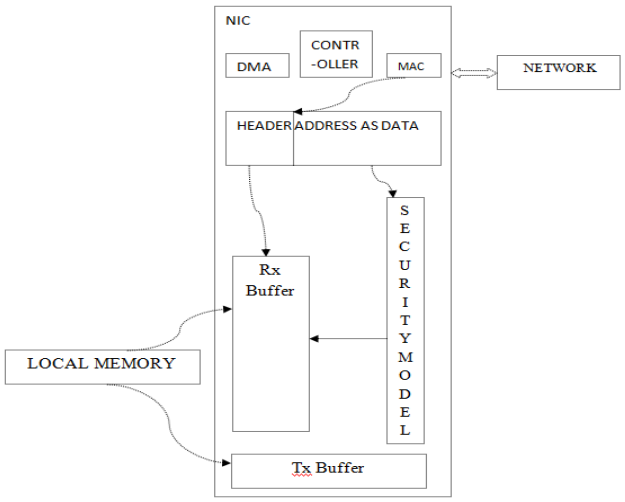

Figure 3: Proposed NIC with Security Module

In fig.3 a security module is introduced in NIC. This security module having some memory elements like Programmable Read Only Memory (PROM), Memory address register (MAR), Memory Data Register (MDR). The size of PROM is 256*8. MAR and MDR are used to store 8 bit address and data respectively. Each Memory location is containing the values, calculated by predetermined mathematical mapping which establishes relation between memory address and values to be stored at that location. The block diagram of security module for proposed NIC is shown in fig. 4.

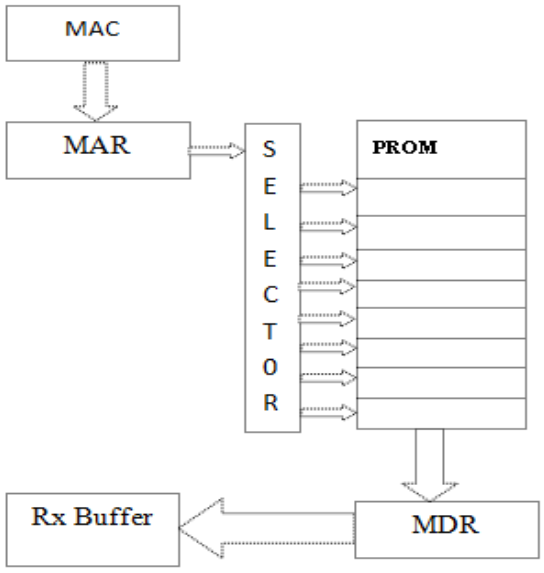

Figure 4: Block Diagram of Security Module

WORKING:

In proposed work only receiver function of NIC is modified. Transmission of packet takes place as generic NIC. At sender's end encryption takes place at application layer. Predetermined mathematical mapping are used to create PROM locations references from the intended video data bytes meant for transmission. When packet comes from the network to the MAC unit, MAC unit extract the header information and address of the data and send the header information in Receiver buffer while addresses to the security module. Security module is having Memory address register to hold the data incoming from MAC. Address comes from the MAC unit are stored in the 8 bit Memory Address Register and selector decode the address and activate the memory location pointed by the address in MAR. Data from activated memory location is transferred to the Memory Data Register, which is also a 8 bit register and finally from MDR data is transferred to the Receiver buffer(local memory at NIC) . After concatenating upper layer headers, already in receiver buffer and incoming decrypted data, generic data packet is formed and transferred to the host memory according to conventional

5. CONCLUSION

Proposed model offers fast secure communication for video streaming. It offers security without considering host processor capability and adding extra overhead for secure communication. Further, proposed architecture offer security without introducing any additional delay, one of most critically undesirable factor in video transmission. Varying level of security may be achieved by applying different mathematical mapping; therefore, it has potential to offer varied level of security as per security need of video services. Current software implementation of cryptography techniques is slower and hardware implementation restricts the flexibility in selection of algorithm as per security needs of applications. We have proposed a method which incorporates flexibility of software implementation and faster execution of hardware implementation. Proposed model has potential for commercial production to address security needs of the display devices with limited processing capability.

REFERENCES

[1] T-210-CX 10GbE Protocol engine with TCP offload.

[2] Adaptec iSCSI ASA-7211C gigabit Ethernet adapter.

[3] 3 Com secure copper NIC, 3CR 990B.

[4] D. Dalessandro and P. Wyck off. " A performance analysis of the ammasso RDMA enabled Ethernet adapter and its iWARP API. In proceedings of RAIT workshop, Sep 2005.

[5] D.L. Perry, "VHDL", Tata Mcgraw Hill Edition, 4th Edition, 2002.

[6] C. Maxfield, " The design warrior guide to FPGAs" Elsevier, 2004.

[7] H. Peter Hofstee " Power Efficient processor Architecture and the cell processor." In proceedings of the 11th International symposium on High Performance computer Architecture, 2005.

[8] Suchita Kamble, N. N. Mhala, " Controller For Network Interface Card on FPGA" In International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol.-2, Issue-3, July-2012

[9] Jeffrey Shafer and Scott Rixner, " A Reconfigurable and Programmable Gigabit Ethernet Network Interface Card." In Rice University-Technical Report TREE0611.

[10] Fuwen Liu, Hartmut Koenig, "A Survey of Video Encryption algorithms, Computers&Security 29(2010)