2010 Sixth International Conference on Networking and Services

FINLAN Packet Delivery Proposal in a Next Generation Internet

Fabíola Souza Fernandes Pereira*, Eduardo Souza Santos†, João Henrique de Souza Pereira‡,
Pedro Frosi Rosa* and Sérgio Takeo Kofuji‡

*Department of Computer Science
Federal University of Uberlândia, Uberlândia, MG, Brazil
Email: fabfernandes@comp.ufu.br, pedro@facom.ufu.br

†Department of Electrical Engineering
Federal University of Uberlândia, Uberlândia, MG, Brazil
Email: eduardo@mestrado.ufu.br

‡Department of Electrical Engineering
University of São Paulo, São Paulo, SP, Brazil
Email: joaohs@usp.br, kofuji@pad.lsi.usp.br

***Abstract*—There are several studies on the TCP/IP architecture evolution since the 80's, however, due to the great installed and used base there are difficulties in implementing improvements in large scale. In the last years, the number of researches that discuss the next generation Internet has grown, and this paper is a study collaboration in this area. This paper proposes the adding of a mechanism to guarantee the packet delivery in FINLAN, which is a protocol that enables the communication in networks with connectivity in layer 2 without the use of IP, TCP, and UDP protocols.**

***Keywords*-Computer Networks; Next Generation Internet; Post IP; TCP/IP Architecture**

I. Introduction

Most of the applications supported by TCP/IP architecture need to establish communication with little data loss and low end-to-end delay. However, even with this architecture efficiency, there are complexities in its protocol stack and the main specifications used nowadays in layers 3 and 4, as TCP, UDP and IP, were specified about 30 years ago [1], [2] and therefore do not take into account some recent needs, capacities and computer network proportions.

So, noticing the improvement possibilities of the current TCP/IP architecture, there is the FINLAN proposal (Fast Integration of Network Layers) to change the packet delivery in this architecture for some applications. The FINLAN is part of the studies in the post IP area and proposes the removal of network and transport layers aiming to meet today's application needs in a simple and optimized way.

The analysis of TCP/IP architecture complexity growth in the last years shows the need to re-think this architecture and the possibility to contribute to this evolution of next generation Internet, encourages the studies in this area, in the belief that an improvement in distributed communication systems will result in benefits to mankind.

The purpose of this paper is propose a mechanism to guarantee the data delivery in FINLAN, in such a way that the operational system will receive the information over the needs of the applications and guarantee the data delivery, when necessary, without the need to use distinct transport protocols, such as UDP or TCP.

This paper is organized as follows: Section 2 presents correlated studies over alternatives to TCP/IP use; Section 3 presents a proposal to incorporate a delivery guarantee mechanism to FINLAN; at last, Section 4 presents the next steps to be developed and the conclusions in this study area.

II. Correlate Works

To guarantee that the data transmission over the network be reliable is a complex requirement to be technically met. There are different technologies for loss detection and packet re-transmission up to architectures that do not worry about guaranteeing a reliable transmission.

Among the existing technologies it is possible to point out the old Frame Relay [3] as an example of protocol that works in the lower layers and does not worry about guaranteeing the data delivery. The idea is that the application be in charge of dealing with lost packets. The ATM networks [4] are also examples of technology that does not implement the delivery guarantee. In this technology, there is a great trust in the transmission medium.

The ATM architecture is different from the TCP/IP architecture, because in TCP [5] the delivery guarantee is given in non reliable transmission medium through packet confirmation. This occurs similarly in SCTP, which is also a transport protocol in TCP/IP architecture.

There is also the MPLS, which is a low layer protocol and with a large capacity of management and traffic and

978-0-7695-3969-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ICNS.2010.12

therefore, with more reliability, although it is not designed to secure that all data packets will get to the destination [6].

Even in the higher layers, it is possible to point out protocols which do not meet the delivery guarantee requirement, for example the UDP [7] of TCP/IP architecture. Such fact can be explained by the purpose of each protocol or architecture, that is, they transmit data that do not have a delivery packet guarantee as a necessary requirement.

On the other hand, it is also possible to find solutions that guarantee the data delivery, implemented in different layers. There are also the old networks X25 [8], which guarantee the delivery based on confirmation of each data packet received. In more recent technologies, as Myrinet and Infiniband [9], it is also possible to verify a structure which provides a reliable message transmission through the sending of messages of destination requiring the missed packets [10], [11].

There are still works in wireless and mobile networks that have solutions to guarantee data delivery due to the flexibility of a mobile host. In [12], for example, a protocol which uses ARQ and FEC mechanisms, aiming at low rate re-transmission, is proposed. In [13], there is the analysis of the problem of using variable paths aiming at low loss rate and the proposal for a load balancing algorithm as a solution.

A. FINLAN Structure

This work consists of incorporating a delivery guarantee mechanism to the FINLAN, a proposed structure for a next generation Internet studies [14]. Several works have been developed in this area with the purpose to propose new address solutions, joined with the search for mobility and safety, according to the works [15]–[17]. In [15], it is presented a new model of inter-connection among network elements through flat routing, and in [16], an architecture is proposed for address which meets challenges such as dynamicy, safety, and multi-homing.

The FINLAN is a post IP study for a structure which eliminates the use of network and transport layers in networks with connectivity in layer 2, differently from work [17], which proposes the creation of an intermediate identification layer in charge of a new address way. The purpose of FINLAN is simplify the way the information is addressed and transmitted, optimizing the network structure and reducing the neighbourhoods dependency. This can help for a horizontal addressing architecture, as proposed in the correlate works discussed in [18], [19].

Such proposal of a new layer structure takes into account the real needs of applications such as the VoIP communication, which beginning of development was around 15 years before the UDP, TCP and IP protocols came up, and therefore suffer impact due to the use of an architecture that was not designed with the requirement to support it.

Basically, the FINLAN structure consists of changes in the Ethernet header in a way that a hybrid communication is allowed, compatible with the network structure in use. For so, FINLAN and TCP/IP packets are distinguished through EtherType field. One aspect of this proposal is the communication through the establishment of information flows, which allows the addressing to take place without the need of ports or logical addresses. Figure 1 shows the header of an application with this structure. It can be noticed that hosts are identified through MAC address, and moreover, the fields in various sizes guarantee that the overhead caused by the header become of an adaptive size.

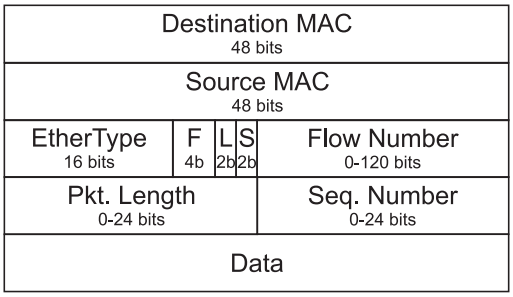

Figure 1. Ethernet header structure for FINLAN applications

In the Figure 1, the identification bits contain three fields, “F”, “L”, and “S”, which represent the number of bytes used in the fields “Flow Number”, “Packet Length”, and “Sequence Number”.

This work proposes a solution which incorporates a delivery guarantee mechanism to the FINLAN, which allows that such requirement be optional, according to usage needs. For real time application, such as voice and video transfer, the delivery guarantee can be withdrawal, according to usage preference; on the other hand, for a file transfer, for example, the guarantee that the data will arrive fully at its destination is a necessary requirement.

III. Delivery Guarantee with FINLAN

The proposal to realize the delivery guarantee in FINLAN is that this protocol recognizes the usage need, in such a way to identify whether or not the delivery guarantee is required. For so, the application informs its necessity through FINLAN library use.

It is important mentioning that with the improvement of a delivery guarantee mechanism, the Ethernet heading structure for FINLAN applications suffer some changes in relation to the one showed in Figure 1, as will be described in this section.

To minimize the complexity and network cost, the FINLAN only provides the delivery guarantee when required by the application. To make this flexible the flag “G” is used to inform the guarantee necessity. This flag has 1 bit, located after the EtherType, followed by the field F, which has 3 bits. In FINLAN previous version without delivery guarantee the field F had 4 bits.

When G=0, there is no delivery guarantee and FINLAN behavior is as described in section II. When G=1, the field "Packet Number" is enabled with 16 bits. This field is located after the "Sequence Number".

The delivery guarantee mechanism in FINLAN is done by periodical confirmation according to network behavior characteristic at each instant in time, according to RTT (Round Trip Time). In this confirmation, the network elements, in communication, inform mutually the next sequence number to receive the confirmation. This information can indicate the next packet to be confirmed or a packet loss.

This informative packet, similar to a keepalive, does not have data field and for this, it is designated by the field L=00. Note: The field L is used to inform the quantity of bytes of "Packet Length" field. Once L is equal to "00", the "Packet Length" is suppressed in FINLAN packet and the "Confirmations Quantity" (CQ) field is added, with 8 bits, after the "Packet Number" field.

Depending on the value of the field "Confirmations Quantity", the fields C1, C2, C3, ..., C255 are filled, to inform from 1 up to 255 "Packet Number" not received. Each "Cx" field has 16 bits, since this is the size of the field "Packet Number". For this kind of packet (L=00) the FINLAN structure has the format shown in Figure 2.

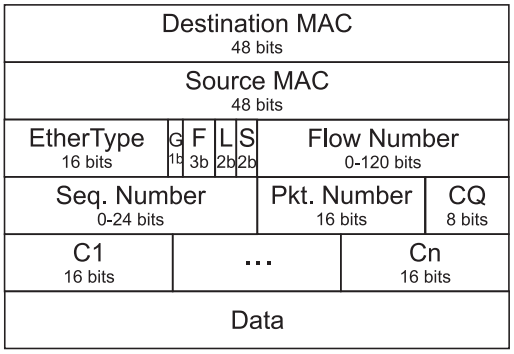

Figure 2. FINLAN confirmation packet

In case the network element sending the packets notices that the keepalive is missing, it will interrupt the data transmission and will only keep the periodical sending of its keepalive. This way, it is expected to optimize the use of network resources in case of communication interruption among the elements. For the definition of the timer which identifies the lack of communication it is proposed the use of Jacobson's studies for network re-transmission [20].

Thus, when one keepalive is sent, a timer is activated and if there is the receive confirmation, the timer is switched off. Otherwise, the keepalive is re-transmitted. This mechanism is similar to TCP, however the TCP does that for each of the transmitted packet [5]. In this work's proposal, the FINLAN does not confirm each of the packets, but simply informs on the missing packets.

To make the re-send, it is necessary to use a specific timeout interval and determining it is not simple, because the range of time of packets to send and receive can vary in different intervals, and a bad choice of the timeout can cause unnecessary re-transmissions in the network or the delay of re-sending a packet.

Therefore, the solution to this problem is use an algorithm that will dynamically calculate the timeout based on continuous evaluation of network performance.

It is suggested the use of the algorithm created by Jacobson [21], where for each communication flow keeps a variable RTT, which consists of the best estimate (for that moment) for the send and receive time up to packets destination. So, for each keepalive sent, a timer is activated. In case the confirmation is received before the end of the timer, FINLAN calculates the M necessary time and updates RTT according to Equation (1) where the value α is a smoothing factor which determines the weight given to the old value [20].

$$RTT = \alpha RTT + (1 - \alpha)M \quad (1)$$

However, even with an appropriate RTT value, it is still not easy to determine the timeout. Typically, TCP implementations the timeout value is set equal to βRTT, but determine this value is very hard. According to Jacobson's studies, it is proposed to keep β proportional to the standard deviation of the probability density function of arrival confirmation time. It is also proposed to keep the deviation forecast through median deviation (D), which is given by Equation (2) and calculated at each keepalive confirmation.

$$D = \alpha D + (1 - \alpha)|RTT - M| \quad (2)$$

With the D variable value, there is, in most of TCP implementations, the timeout value given by Equation 3. It is noticed that the constant 4 is an arbitrary value, but suits the processing and network needs, since multiplying by 4 consists of a sole dislocation of 2 bits and less than 1% of packets arrive with a delay over four times the standard deviation [20].

$$Timeout = RTT + 4D \quad (3)$$

So, it is suggested that the FINLAN use this mechanism for keepalive control and identify the necessity, or not, of interrupting the communication flow, and also calculate the time to indicate the lack of one or more packets.

IV. Conclusion and Future Works

Since the Internet architecture design, there are studies for its evolution, however the developments do not have approached the principal protocols of intermediate layers such as IP, TCP, and UDP. Recently, there has been a raise

in interest by researchers in this area with discussions over post IP technologies for next generation Internet.

In this area, this work contributes with a proposal to guarantee the delivery in FINLAN. By this, the applications do not need to use different transport protocols to have or not data delivery guarantee. In this proposal, the applications only need to inform the operational system their need about data delivery guarantee by using FINLAN library.

In turn, the FINLAN enables the network overhead reduction by reducing the redundancy and changing the packet confirmation way done by the in use protocols.

So, this proposal is just a first step to improve FINLAN with a variety of QoS guarantees, a required feature for technologies for next generation Internet [14]. The idea is append new basic requirements like security and isolation in FINLAN in future works.

For the continuity of this work, this proposal will be implemented for performance evaluation and comparison to TCP/IP architecture, in networks with low and high rate of packet loss. In this comparison, the network cost, processor and memory use will be evaluated.

After the performance evaluation, a study will be conducted to FINLAN be used, in a hybrid way with the TCP/IP architecture in the worldwide network, without the use of IP, TCP, UDP, SCTP or any other protocol from layers 3 and 4 of the current architecture.

REFERENCES

[1] J. Postel, "RFC 760: DoD Standard Internet Protocol," *Information Sciences Institute of the University of Southern California*, 1980.

[2] ——, "RFC 761: DoD Standard Transmission Control Protocol," *Information Sciences Institute of the University of Southern California*, 1980.

[3] T. Bradley, C. Brown, and A. Malis, "Multiprotocol interconnect over frame relay," *Internet Engineering Task Force Document IETF RFC 1490*, pp. 1–25, 1993.

[4] A. E. Joel, *Asynchronous Transfer Mode Switching*. Institute of Electrical & Electronics Enginee, 1993.

[5] J. Postel, "RFC: 793: DoD Standard Transmission Control Protocol," *Information Sciences Institute of the University of Southern California*, 1980.

[6] E. Rosen, A. Viswanathan, and R. Callon, *Multiprotocol Label Switching Architecture*. RFC Editor, 2001.

[7] J. Postel, "RFC 768: DoD Standard User Datagram Protocol," *Information Sciences Institute of the University of Southern California*, 1980.

[8] "Draft Recommendation X-25," *CCITT Study Group VII*, 1976.

[9] Top500.org, "Interconect family share over time," retrived 2009-10-02. [Online]. Available: http://www.top500.org/overtime

[10] I. T. Assoc., "Infiniband architecture specification, volume 1, release 1.2," 2004, retrived 2009-10-02. [Online]. Available: http://www.infinibandta.org

[11] I. Myricom, "Myricom," retrived 2009-10-02. [Online]. Available: http://www.myri.com

[12] A. Boukerche, D. Ning, and R. B. Araujo, "UARTP - A Unicast-based self-Adaptive Reliable Transmission Protocol for Wireless and Mobile Ad-hoc Networks," *2nd ACM international workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks - WASUN '05, Canada*, pp. 255–257, 2005.

[13] P. Djukic and S. Valaee, "Reliable packet transmissions in multipath routed wireless networks," *IEEE Transactions on Mobile Computing*, 2005.

[14] R. Jain, "Internet 3.0: Ten problems with current internet architecture and solutions for the next generation," *Miliray Communications Conference, 2006, MILCOM 2006*, pp. 1–9, 2006.

[15] R. Pasquini, F. L. Verdi, and M. F. Magalhães, "Towards a landmark-based flat routing," *27th Brazilian Symposium on Computer Networks and Distributed Systems - SBRC 2009, Recife - PE, Brazil*, 2009.

[16] R. Pasquini, L. Paula, F. Verdi, and M. Magalhães, "Domain identifiers in a next generation internet architecture," *IEEE Wireless Communications & Networking Conference - WCNC 2009, Budapeste*, 2009.

[17] W. Wong, R. Villaca, L. Paula, R. Pasquini, F. L. Verdi, and M. F. Magalhães, "An architecture for mobility support in a next generation internet," *22nd IEEE International Conference on Advanced Information, Networking and Applications - AINA 2008. Okinawa, Japan*, 2008.

[18] J. H. S. Pereira, S. T. Kofuji, and P. F. Rosa, "Distributed systems ontology," *IEEE New Technologies, Mobility and Security Conference - NTMS, Cairo*, 2009.

[19] ——, "Horizontal address ontology in internet architecture," *IEEE New Technologies, Mobility and Security Conference - NTMS, Cairo*, 2009.

[20] A. S. Tanenbaum, *Computer Networks (4th Edition)*. Prentice Hall, 2002.

[21] V. Jacobson, "Congestion avoidance and control," *SIGCOMM '88: Symposium proceedings on Communications architectures and protocols, USA*, pp. 314–329, 1988.