The Original ARPANET, Dec. 1969

A drawing of the first Ethernet system by Bob Metcalfe
Simulation of Arpanet NCP and Cyclades Protocols in Simula-67

Sequences of events in virtual time
→ causal relationships
→ causes of desynchronization

Verification and Evaluation of Communication Protocols

Gérard Le Lann and Yves Le Goff
Centre d'Études de l'Informatique, Université de Clermont-Ferrand, France

Introduction

First transport protocol specifications for the Cyclades network were issued in November 1972. It was felt necessary to ensure more effectively a correct implementation of these specifications before embarking upon their implementation. The responsibility for this lay given to the Computer Network Group of INRIA (Institut National de Recherche en Informatique et en Automatique). This group was formed to work and to define the design of a new transport protocol, and was expected to partake in the verification and evaluation of communication protocols.

Part 1: Dynamic techniques in verification of communication protocols

1. Introduction

In the Cyclades network [9], the transport protocol and the transport station (TS) are roughly equivalent in the transport protocol and the NCP in the Arpanet network. This initial version of the Cyclades transport protocol included these features: sequential transfer, transmission of messages, and sending and receiving messages at the same time.

In practice, TSs are connected to one another through a network of interconnected messages and sending and receiving messages at the same time. These messages are exchanged in a cyclic manner, and the messages are transmitted through a network of interconnected messages and sending and receiving messages at the same time.
V. Cerf, R. Kahn, 1974

Original publication on TCP

The segment, then, the IP flag would also be set. The LMK flag is also set if the last segment of a message, if the message were to be continued by one segment. How can flag, as used by the destination TCP, respectively, to discover the presence of a checksum for a given segment and to ensure that a completed message has arrived.

The LMK and LMK flags in the internetwork header are known to the destination and are of special importance when packets must be split apart from propagation through the next hop network. We illustrate their use with an example in Fig. 9.

The original message of Fig. 9 is shown split into two segments, A and B, and transmitted by the TCP into a pair of internetwork packets. Packets A and B have their LS bits set, and D has its LM bit set as well. When packet A passes through the gateway, it is set into two pieces: packet A1 for which neither LMK nor LMK bits are set, and packet A2 whose LS bit is set. Similarly, packet B is split such that the first piece, packet B1, has neither bit set, but packet B2 has both bit set. The sequence number field (SN) and the byte count field (CT) of each packet is modified by the gateway to properly identify the byte offsets of each packet. The overall need only ensure that the internetwork header is not fragmented.

The destination TCP, upon recognizing segment A, will detect the LM flag and will verify that this flag is contained in packet A1. Upon receipt of packet A2, assuming all other packets have arrived, the destination TCP verifies that it has received a complete message and can now advise the destination process of its receipt.

TRANSMISSION AND DUPLICATE DETECTION

We propose a simple and reliable acknowledge mechanism which will allow TCP to recover from packet losses from time to time. A TCP transmits packets and waits for receipt (acknowledgment) that are carried in the reverse packet stream. If no acknowledgment is received for a particular packet in succession, the TCP will retransmit. It is not our intention that the new level acknowledgment mechanism, which is described in the following paragraphs, will not be called upon very often in practice. Evidence already exists that occasional acknowledgments can be efficiently carried out without loss of time. However, the inclusion of a new acknowledgment mechanism makes it possible to recover from occasional network problems and allows a wide range of TCP protocol strategies to be implemented. We envision it will occasionally be used to allow accommodation of transport protocols with robustness demands for limited buffer resources, and other network needs.

Any retransmission policy requires some means by which the receiver can detect duplicate packets. Even if an infinite number of distinct packet sequence numbers were available, the receiver would still have the problem of knowing how long to remember previously received block in order to avoid duplicates. More, we are interested by the fact that only a finite number of distinct sequence numbers are in fact associated, and that if they are retransmitted, the receiver must be able to distinguish between new transmissions and retransmissions.

A window strategy, similar to that used by the DECnet transport system, which introduced a virtual transmission mode [3] and the concept very distant user connection [18], is proposed here (see Fig. 10).

Suppose that the sequence number limit in the internetwork header permits sequence numbers to range from 0 to r - 1. We assume that the sender will not transmit more than r bytes without receiving an acknowledgment. The window serves as the window (see Fig. 11). Clearly, the data is less than r bytes, the rate for sender and receiver are as follows:

Sender: Let A be the sequence number associated with the last window edge. Then:
1) The sender transmits byte from segment whose first byte lies between A and up to A + r - 1.
2) On receipt (or detection) of acknowledgment, the sender transmits (or sends) the last window edge bytes.
3) On receipt of acknowledgment consisting of the receiver's current window edge, the sender's

BIRTH OF THE INTERNET


THEIR WORK BECAME KNOWN IN SEPTEMBER 1974 AT A NETWORK CONFERENCE IN ENGLAND, WHERE KAHN'S PAPER WAS PUBLISHED IN MAY 1974.


VINTON CERF

RAJDESIGN

ROBERT DARPA

JAMES MATHIS

FOR METALLIC

DANIEL KLEIN

RICHARD ALLEN

GERHARD LANN

DARPA

COLLABORATING GROUPS

BOB BERANIK AND NEUMAN

WILLIAM PLUMMER AND CHASEY

RAY TOMLINSON

NOEL CHAPPLE - DAVID CLARK - STEPHEN KENT - DAVID F. REED

NOE

YUKI HIRANO - PAUL ELLING

UNIVERSITY COLLEGE LONDON

FRANK DEERHOFF - MARCO-CARL - PETER HEIDEN - ANDREW STORIES

UNCAS

ROBERT BRADEN - DANNY COHEN - DANNY LEE - DANNY JOST

ULTIMATELY, THOUSANDS OF THINKING MACHINES HAVE CONTRIBUTED TO THE EXPLOSION OF THE INTERNET.

DEDICATED JULY 08, 2005

Gérard Le Lann, INRIA

Les 50 ans d’Internet, CNAM, Paris, 29 octobre 2019
“The Internet would have emerged even if none of those folks had ever been born! It was “in the air” and awaiting the technology to catch up with the vision.”

Leonard Kleinrock
May 1973, Bob Metcalfe wrote a memo describing the *Ethernet* (IEEE 802.3 standard in 1983)

In the 1980s, deterministic version of Ethernet patented by INRIA (requested by the French Navy)

→ In late 1980s and 1990s, numerous deployments (submarines, surface vessels, Ariane launchpad in French Guiana, etc.)
Post 1983 (replace or enrich?)

Ethernet

Assertions by Big Auto (GM, etc.), the MAP initiative ≈ 1980s:
Ethernet not for real-time, token bus is perfect.

Nowadays:
Ethernet all over the world
Real-time (deterministic)
Ethernets everywhere:
Offices, factories, homes, cars (CAN), plants, etc.

Internet Map in 1999

TOR atop Internet

Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Interplanetary Internet

TOR PROJECT

Download Tor

NASA

Prédictions françaises en 2008

Internet in Planet Earth neighborhood
Digital Invasion

Internet

Web

Social nets

Human Centric Activities

Cyber networks

utilisés par les *humains*, situés *à l’extérieur* de ces réseaux

Cyberphysical networks

les *humains* graduellement intégrés *à l’intérieur* des réseaux

(digital « black hole » or expanding digital universe?)
Humans surrounded by digital devices
Humans wear digital prostheses
Humans within digital prostheses (automated vehicles)

Cyberphysics

Augmented Human Capabilities
Réseaux spontanés de véhicules automatisés

Domaine applicatif ≈ tous les humains ≥ enjeux sociétaux majeurs

- automation control
- safety engineering
- distributed computing
- communication networks
- human & social sciences

≈ 0 fatalities  ≈ 0 severe injuries

Lessons learned from Internet & Ethernet % wireless nets
• **Safety?** So far: 4 fatalities, dozens of severely injured passengers in hospitals.

Robotics + WiFi broadcast ≈ 300 m

• **Privacy?** (passive adversaries): No personal data can be inferred or extracted from cyber-centric information (wireless communications), from physical-centric information (paths and routes followed by vehicles).

• **Cybersecurity?** (active adversaries): Mobility, safety, not compromised by internal/external cyberattacks (masquerading, Sybil attacks, man-in-the-middle attacks, message falsification, injection of bogus data, intrusions, replay attacks, DoS).

**This is what Big Auto has in store for us: V2X standards**
Cyber Attacks with CAVs/V2X

assistance

congestion

terrorist attacks

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Safety or/and mobility compromised by remote unknown cyberattackers

The Illegal $5 WiFi Jammer for iPhone & Android
Privacy Threats with CAVs/V2X

In addition to:

- **EXTERNAL** EAVESDROPPING

**INTERNAL** CYBER-ESPIIONNAGE WITH **V2X**

Janusian justification: for assisted driving (ADAS)

Facial recognition

Continuous cybersurveillance

Who collects, stores, processes, mines, resells, **personal data**?

Reasons? For how long? Responsibilities in case of hacking?
This is what Research has in store for us: **CMX functionalities**

Réseaux véhiculaires ad hoc ≈ formations spontanées d’oiseaux (flocks/swarms) ?

Optique + radio cellulaire très courte portée ($\approx 10-80$ m), directionnelle

Algorithme de coordination distribuée quasi-instantanée
This is what Research has in store for us: **CMX functionalities**

Next-Gen Vehicles ↔ Robotics + CMX (mobile edge computing)

- Major vulnerabilities with CAVs eliminated

- **0 interventions humaines**

- **Innocuité absolue théorique**
  (≈ 0 morts, ≈ 0 blessés graves)

- **0 atteinte à la vie privée**

- **0 cyberattaque distante**

- **Cyberattaque locale: irrationnelle**
Mise en perspective

Géosphère (≈ 4,5 M.années)

Biosphère (Bactéries ≈ 3,8 m.années / Homo rudolfensis ≈ 2,9 m.années / Homo habilis ≈ 2,5 m.années)

Humano-biosphère (Homo sapiens ≈ 200.000 ans / Sumériens ≈ 9.500 ans) : les humains transforment la biosphère

Noosphère : les humains se transforment eux-mêmes et externalisent leurs capacités cognitives

les tâches physiques ou cognitives consomment du temps humain

Internet = innovation majeure dans l’aventure humaine