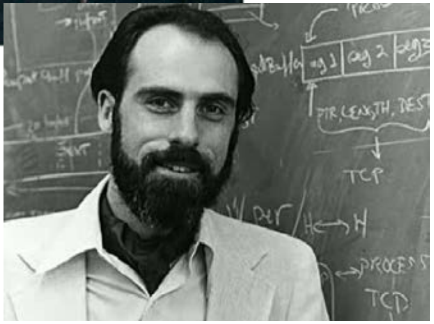
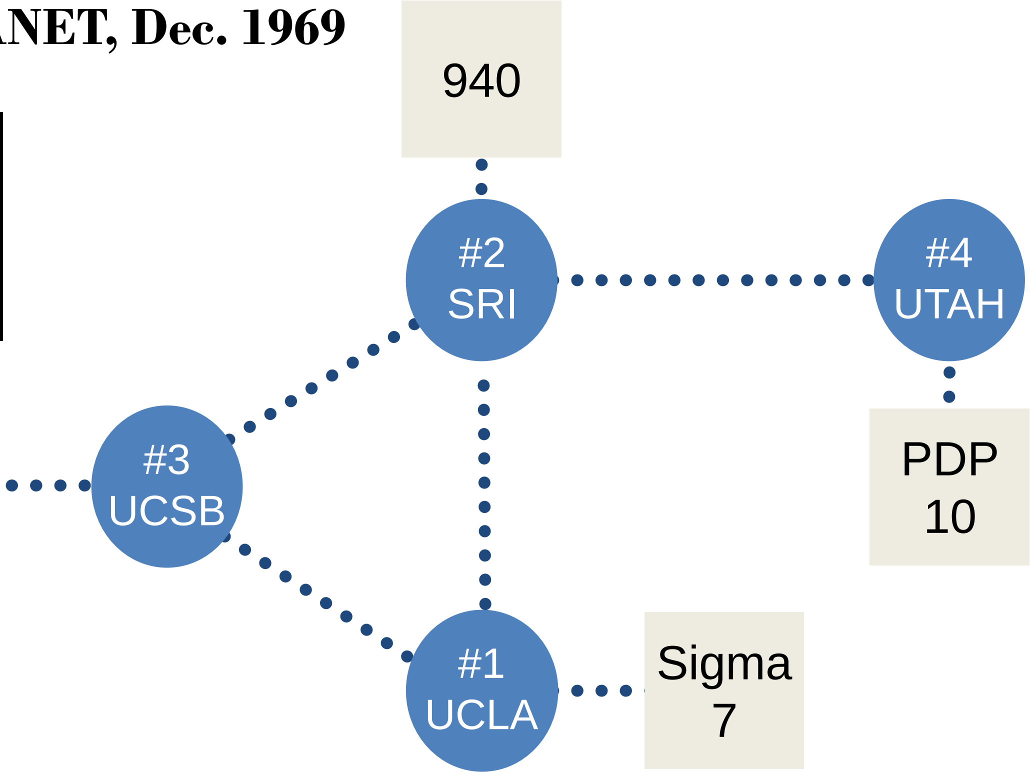
The Original ARPANET, Dec. 1969





940

#2
SRI

#4
UTAH

360

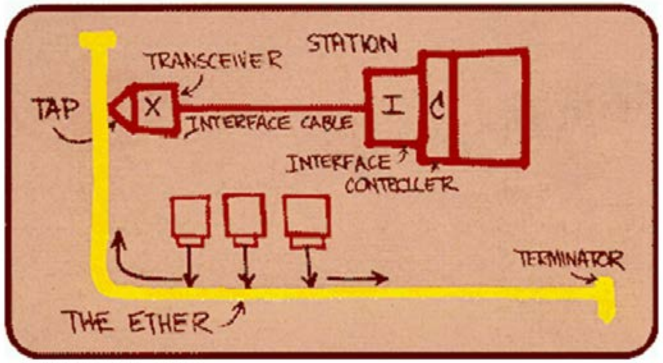
#3
UCSB

PDP
10

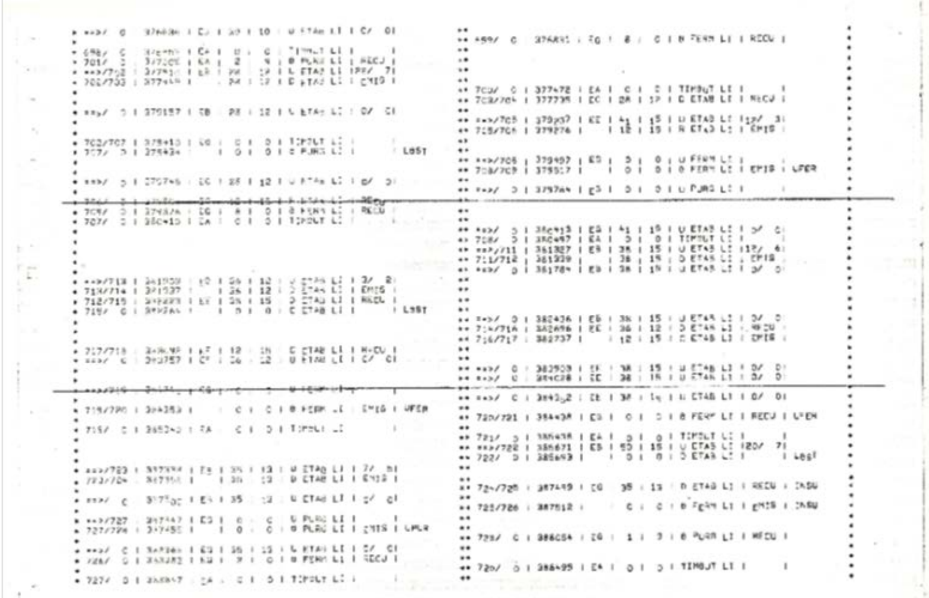
#1
UCLA

Sigma
7

A drawing of the first Ethernet system by Bob Metcalfe



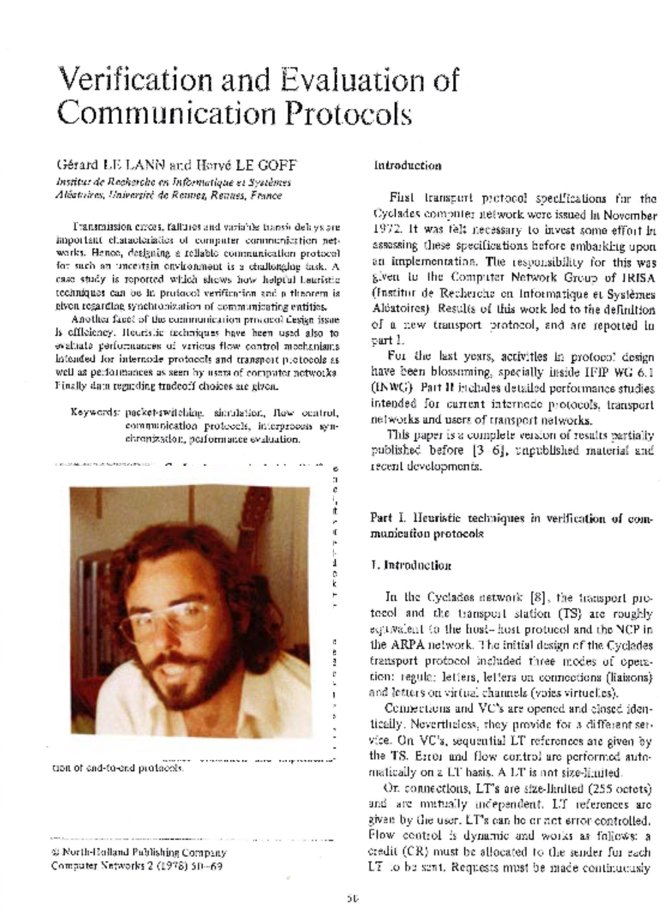
(1972-73) Simulation of Arpanet NCP and Cyclades Protocols in Simula-67



Sequences of events in virtual time

➔ **causal relationships**

➔ **causes of desynchronization**



Verification and Evaluation of Communication Protocols

Gérard LE LANN and Hervé LE GOFF

Institut de Recherche en Informatique et Systèmes Aléatoires, Université de Rennes, Rennes, France

Transmission errors, failures and variable transit delays are important characteristics of computer communication networks. Hence, designing a reliable communication protocol for such an uncertain environment is a challenging task. A case study is reported which shows how helpful heuristic techniques can be in protocol verification and a theorem is given regarding synchronization of communicating entities.

Another facet of the communication protocol design issue is efficiency. Heuristic techniques have been used also to evaluate performances of various flow control mechanisms intended for internode protocols and transport protocols as well as performances as seen by users of computer networks. Finally data regarding tradeoff choices are given.

Keywords: packet-switching, simulation, flow control, communication protocols, interprocess synchronization, performance evaluation.

tion of end-to-end protocols.

© North-Holland Publishing Company
Computer Networks 2 (1978) 50–69

Introduction

First transport protocol specifications for the Cyclades computer network were issued in November 1972. It was felt necessary to invest some effort in assessing these specifications before embarking upon an implementation. The responsibility for this was given to the Computer Network Group of IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires). Results of this work led to the definition of a new transport protocol, and are reported in part I.

For the last years, activities in protocol design have been blossoming, specially inside IFIP WG 6.1 (INWG). Part II includes detailed performance studies intended for current internode protocols, transport networks and users of transport networks.

This paper is a complete version of results partially published before [3–6], unpublished material and recent developments.

Part I. Heuristic techniques in verification of communication protocols

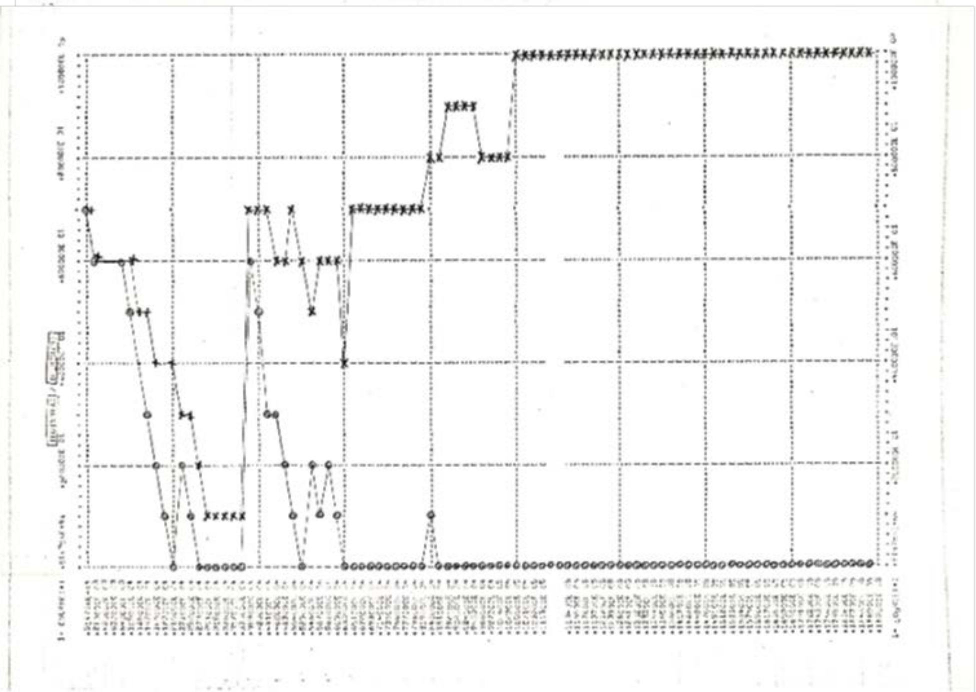
1. Introduction

In the Cyclades network [8], the transport protocol and the transport station (TS) are roughly equivalent to the host–host protocol and the NCP in the ARPA network. The initial design of the Cyclades transport protocol included three modes of operation: regular letters, letters on connections (liaisons) and letters on virtual channels (voies virtuelles).

Connections and VC's are opened and closed identically. Nevertheless, they provide for a different service. On VC's, sequential LT references are given by the TS. Error and flow control are performed automatically on a LT basis. A LT is not size-limited.

On connections, LT's are size-limited (255 octets) and are mutually independent. LT references are given by the user. LT's can be or not error controlled. Flow control is dynamic and works as follows: a credit (CR) must be allocated to the sender for each LT to be sent. Requests must be made continuously

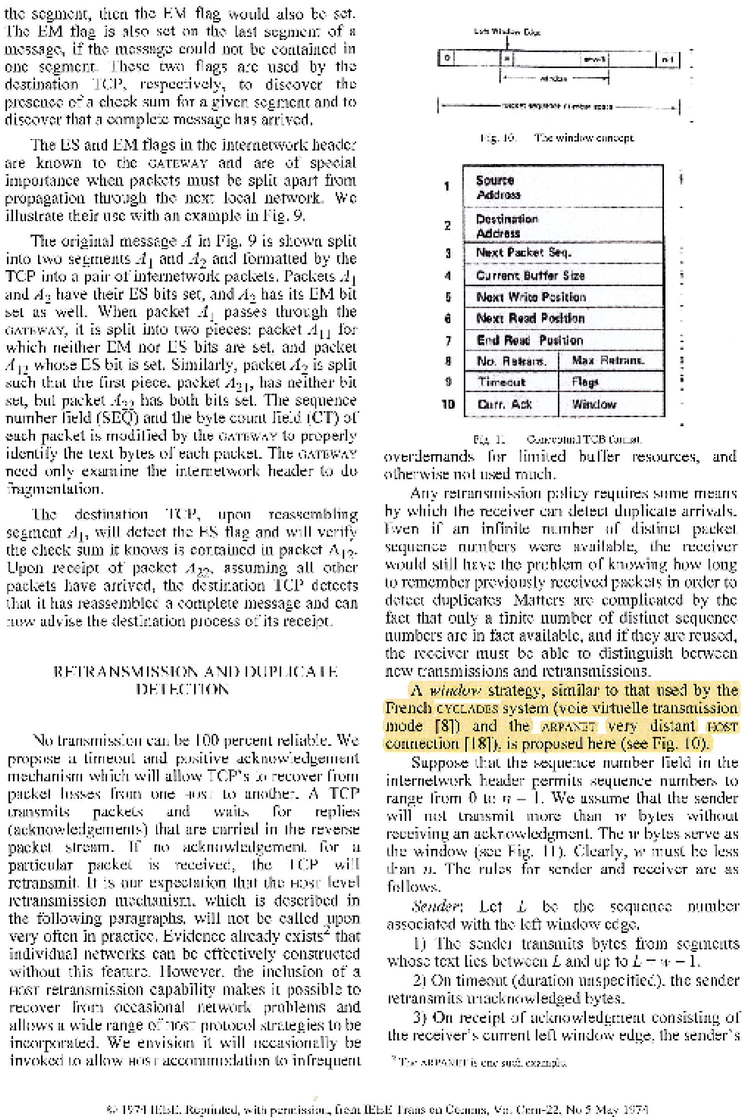
50



End port buffers occupancy

➔ **results of desynchronization**

V. Cerf, R. Kahn, 1974
Original publication on TCP



the segment, then the EM flag would also be set. The EM flag is also set on the last segment of a message, if the message could not be contained in one segment. These two flags are used by the destination TCP, respectively, to discover the presence of a check sum for a given segment and to discover that a complete message has arrived.

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

The original message A in Fig. 9 is shown split into two segments A_1 and A_2 and formatted by the TCP into a pair of internetwork packets. Packets A_1 and A_2 have their ES bits set, and A_2 has its EM bit set as well. When packet A_1 passes through the GATEWAY, it is split into two pieces: packet A_{11} for which neither EM nor ES bits are set, and packet A_{12} whose ES bit is set. Similarly, packet A_2 is split such that the first piece, packet A_{21}, has neither bit set, but packet A_{22} has both bits set. The sequence number field (SEQ) and the byte count field (CT) of each packet is modified by the GATEWAY to properly identify the text bytes of each packet. The GATEWAY need only examine the internetwork header to do fragmentation.

The destination TCP, upon reassembling segment A_1, will detect the ES flag and will verify the check sum it knows is contained in packet A_{12}. Upon receipt of packet A_{22}, assuming all other packets have arrived, the destination TCP detects that it has reassembled a complete message and can now advise the destination process of its receipt.

RETRANSMISSION AND DUPLICATE DETECTION

No transmission can be 100 percent reliable. We propose a timeout and positive acknowledgement mechanism which will allow TCP's to recover from packet losses from one HOST to another. A TCP transmits packets and waits for replies (acknowledgements) that are carried in the reverse packet stream. If no acknowledgement for a particular packet is received, the TCP will retransmit. It is our expectation that the HOST level retransmission mechanism, which is described in the following paragraphs, will not be called upon very often in practice. Evidence already exists[2] that individual networks can be effectively constructed without this feature. However, the inclusion of a HOST retransmission capability makes it possible to recover from occasional network problems and allows a wide range of HOST protocol strategies to be incorporated. We envision it will occasionally be invoked to allow HOST accommodation to infrequent overdemands for limited buffer resources, and otherwise not used much.

Fig. 10. The window concept.

1	Source Address	
2	Destination Address	
3	Next Packet Seq.	
4	Current Buffer Size	
5	Next Write Position	
6	Next Read Position	
7	End Read Position	
8	No. Retrans.	Max Retrans.
9	Timeout	Flags
10	Curr. Ack	Window

Fig. 11. Conceptual TCB format.

Any retransmission policy requires some means by which the receiver can detect duplicate arrivals. 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 packets in order to detect duplicates. Matters are complicated by the fact that only a finite number of distinct sequence numbers are in fact available, and if they are reused, the receiver must be able to distinguish between new transmissions and retransmissions.

A *window* strategy, similar to that used by the French CYCLADES system (voie virtuelle transmission mode [8]) and the ARPANET very distant HOST connection [18]), is proposed here (see Fig. 10).

Suppose that the sequence number field in the internetwork header permits sequence numbers to range from 0 to $n - 1$. We assume that the sender will not transmit more than w bytes without receiving an acknowledgment. The w bytes serve as the window (see Fig. 11). Clearly, w must be less than n. The rules for sender and receiver are as follows.

Sender: Let L be the sequence number associated with the left window edge.

1) The sender transmits bytes from segments whose text lies between L and up to $L + w - 1$.

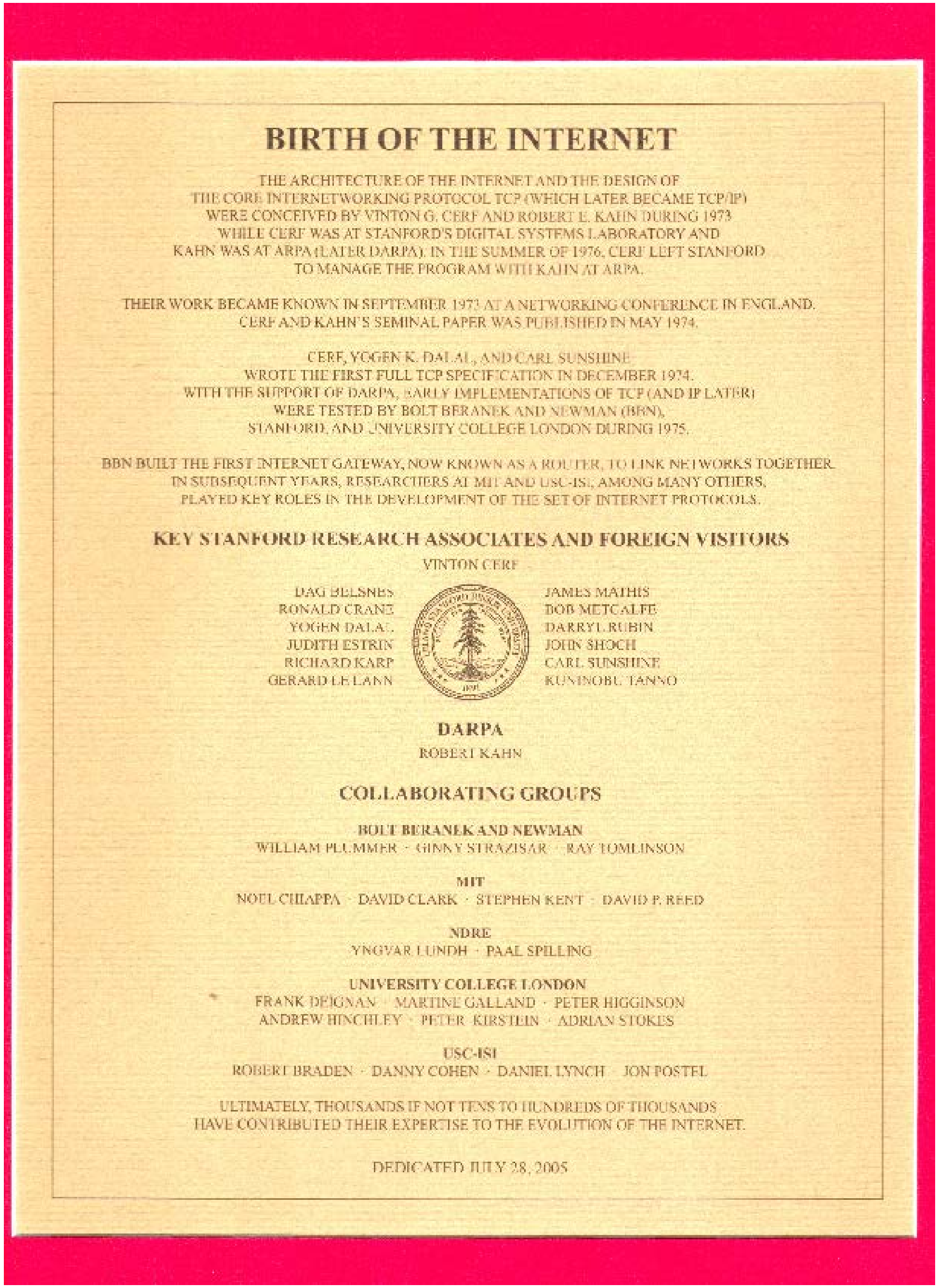
2) On timeout (duration unspecified), the sender retransmits unacknowledged bytes.

3) On receipt of acknowledgment consisting of the receiver's current left window edge, the sender's

---

[2] The ARPANET is one such example.

© 1974 IEEE. Reprinted, with permission, from IEEE Trans on Comms, Vol. Com-22, No 5 May 1974



BIRTH OF THE INTERNET

THE ARCHITECTURE OF THE INTERNET AND THE DESIGN OF
THE CORE INTERNETWORKING PROTOCOL TCP (WHICH LATER BECAME TCP/IP)
WERE CONCEIVED BY VINTON G. CERF AND ROBERT E. KAHN DURING 1973
WHILE CERF WAS AT STANFORD'S DIGITAL SYSTEMS LABORATORY AND
KAHN WAS AT ARPA (LATER DARPA). IN THE SUMMER OF 1976, CERF LEFT STANFORD
TO MANAGE THE PROGRAM WITH KAHN AT ARPA.

THEIR WORK BECAME KNOWN IN SEPTEMBER 1973 AT A NETWORKING CONFERENCE IN ENGLAND.
CERF AND KAHN'S SEMINAL PAPER WAS PUBLISHED IN MAY 1974.

CERF, YOGEN K. DALAL, AND CARL SUNSHINE
WROTE THE FIRST FULL TCP SPECIFICATION IN DECEMBER 1974.
WITH THE SUPPORT OF DARPA, EARLY IMPLEMENTATIONS OF TCP (AND IP LATER)
WERE TESTED BY BOLT BERANEK AND NEWMAN (BBN),
STANFORD, AND UNIVERSITY COLLEGE LONDON DURING 1975.

BBN BUILT THE FIRST INTERNET GATEWAY, NOW KNOWN AS A ROUTER, TO LINK NETWORKS TOGETHER.
IN SUBSEQUENT YEARS, RESEARCHERS AT MIT AND USC-ISI, AMONG MANY OTHERS,
PLAYED KEY ROLES IN THE DEVELOPMENT OF THE SET OF INTERNET PROTOCOLS.

KEY STANFORD RESEARCH ASSOCIATES AND FOREIGN VISITORS

VINTON CERF

DAG BELSNES
RONALD CRANE
YOGEN DALAL
JUDITH ESTRIN
RICHARD KARP
GERARD LE LANN

JAMES MATHIS
BOB METCALFE
DARRYL RUBIN
JOHN SHOCH
CARL SUNSHINE
KUNINOBU TANNO

DARPA

ROBERT KAHN

COLLABORATING GROUPS

BOLT BERANEK AND NEWMAN
WILLIAM PLUMMER · GINNY STRAZISAR · RAY TOMLINSON

MIT
NOEL CHIAPPA · DAVID CLARK · STEPHEN KENT · DAVID P. REED

NDRE
YNGVAR LUNDH · PAAL SPILLING

UNIVERSITY COLLEGE LONDON
FRANK DEIGNAN · MARTINE GALLAND · PETER HIGGINSON
ANDREW HINCHLEY · PETER KIRSTEIN · ADRIAN STOKES

USC-ISI
ROBERT BRADEN · DANNY COHEN · DANIEL LYNCH · JON POSTEL

ULTIMATELY, THOUSANDS IF NOT TENS TO HUNDREDS OF THOUSANDS
HAVE CONTRIBUTED THEIR EXPERTISE TO THE EVOLUTION OF THE INTERNET.

DEDICATED JULY 28, 2005

“ 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.”

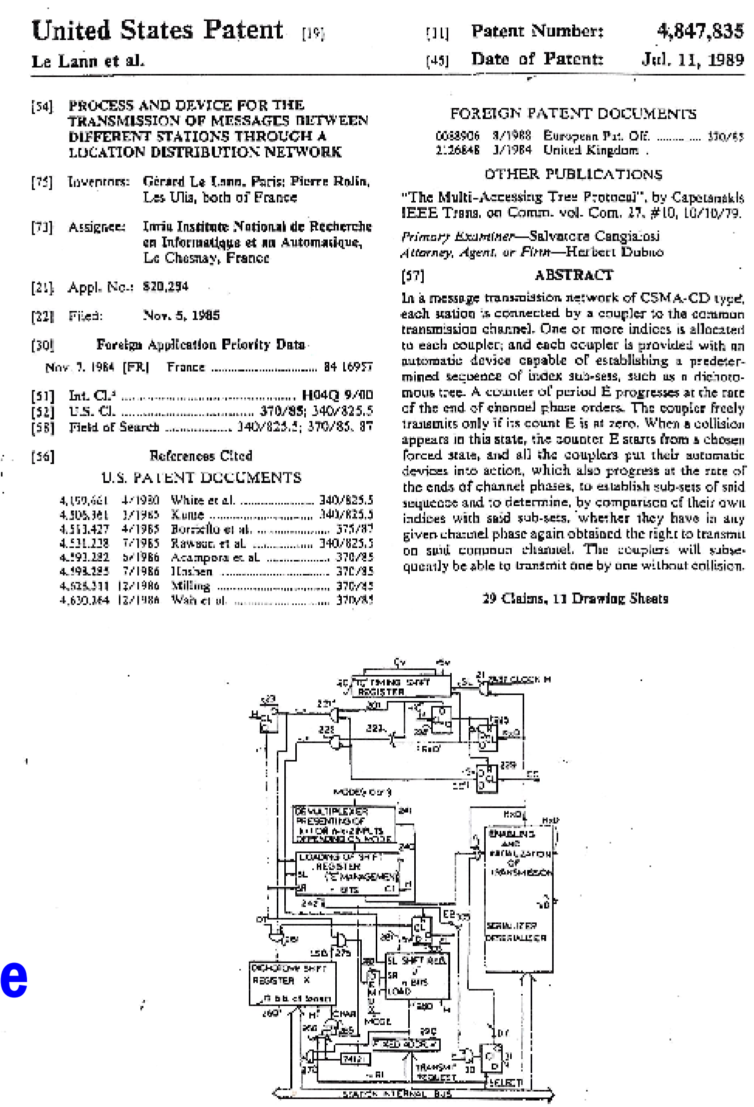
Leonard Kleinrock

1970s: AlohaNet (Hawaï), packet-radio, Ethernet (Xerox Parc)

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

In the1980s, 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.)



United States Patent [19]
Le Lann et al.

[11] **Patent Number:** **4,847,835**
[45] **Date of Patent:** **Jul. 11, 1989**

[54] **PROCESS AND DEVICE FOR THE TRANSMISSION OF MESSAGES BETWEEN DIFFERENT STATIONS THROUGH A LOCATION DISTRIBUTION NETWORK**

[75] Inventors: **Gérard Le Lann, Paris; Pierre Rolin, Les Ulis, both of France**

[73] Assignee: **Inria Institute National de Recherche en Informatique et en Automatique, Le Chesnay, France**

[21] Appl. No.: **820,294**

[22] Filed: **Nov. 5, 1985**

[30] **Foreign Application Priority Data**

Nov. 7, 1984 [FR] France 84 16957

[51] Int. Cl.⁴ **H04Q 9/00**
[52] U.S. Cl. **370/85; 340/825.5**
[58] Field of Search 340/825.5; 370/85, 87

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,199,661	4/1980	White et al.	340/825.5
4,506,361	3/1985	Kume	340/825.5
4,513,427	4/1985	Borriello et al.	375/87
4,531,238	7/1985	Rawson et al.	340/825.5
4,593,282	6/1986	Acampora et al.	370/85
4,598,285	7/1986	Hoshen	370/85
4,628,311	12/1986	Milling	370/85
4,630,264	12/1986	Wah et al.	370/85

FOREIGN PATENT DOCUMENTS

0038906	3/1988	European Pat. Off.	370/85
2126848	3/1984	United Kingdom	

OTHER PUBLICATIONS

"The Multi-Accessing Tree Protocol", by Capetanakis IEEE Trans. on Comm. vol. Com. 27, #10, 10/10/79.

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Herbert Dubno

[57] **ABSTRACT**

In a message transmission network of CSMA-CD type, each station is connected by a coupler to the common transmission channel. One or more indices is allocated to each coupler; and each coupler is provided with an automatic device capable of establishing a predetermined sequence of index sub-sets, such as a dichotomous tree. A counter of period E progresses at the rate of the end of channel phase orders. The coupler freely transmits only if its count E is at zero. When a collision appears in this state, the counter E starts from a chosen forced state, and all the couplers put their automatic devices into action, which also progress at the rate of the ends of channel phases, to establish sub-sets of said sequence and to determine, by comparison of their own indices with said sub-sets, whether they have in any given channel phase again obtained the right to transmit on said common channel. The couplers will subsequently be able to transmit one by one without collision.

29 Claims, 11 Drawing Sheets

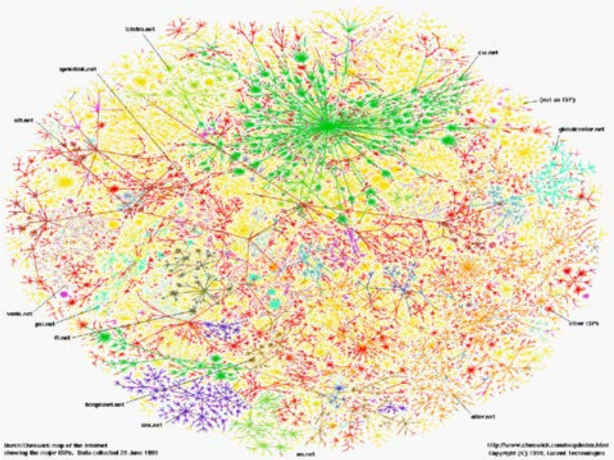
Post 1983 (replace or enrich?)

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.



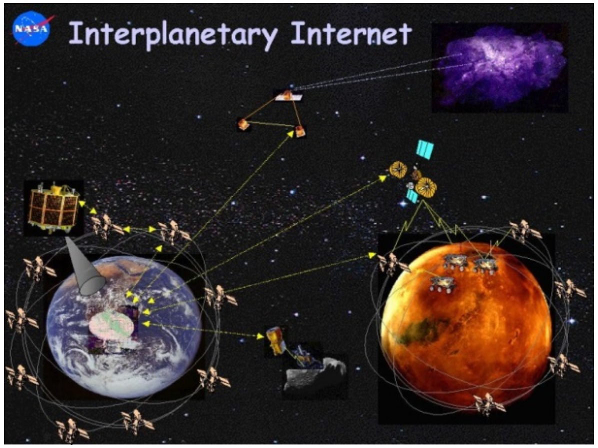
◀ **Internet**
Map in 1999

Anonymity Online

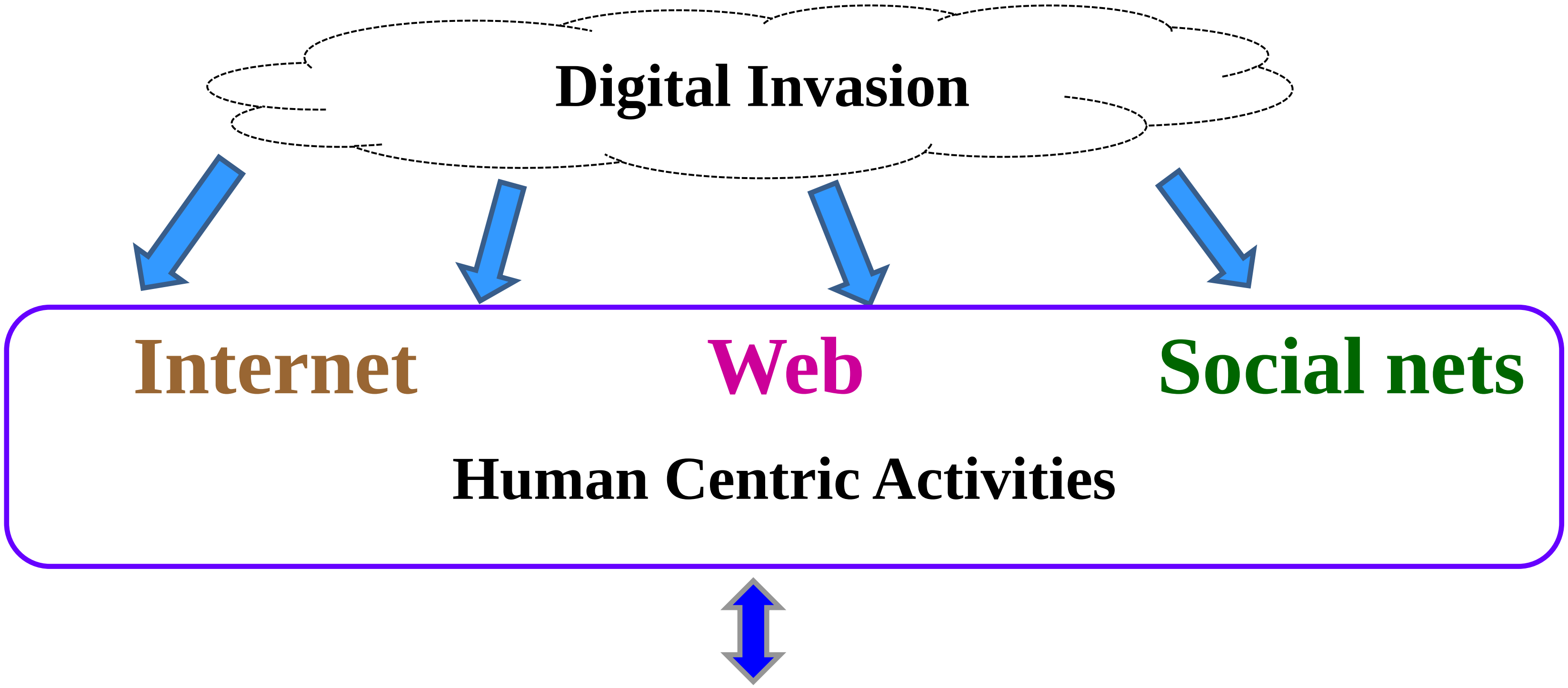
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

TOR atop Internet

▲ Prédictions françaises en 2008



◀ **Internet**
in Planet Earth neighborhood



Digital Invasion

Internet **Web** **Social nets**

Human Centric Activities

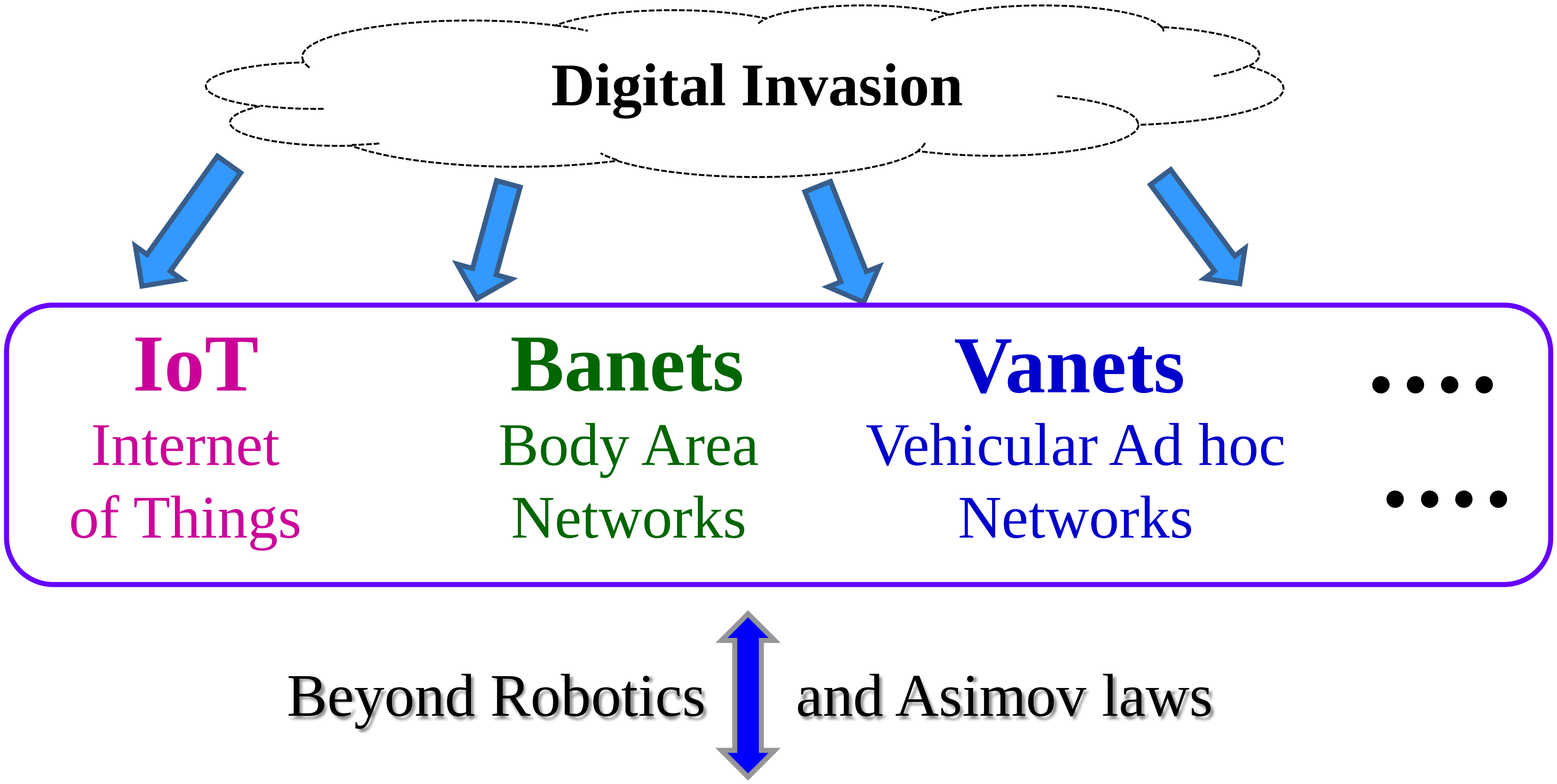
Cyber networks

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?)



Digital Invasion

IoT
Internet
of Things

Banets
Body Area
Networks

Vanets
Vehicular Ad hoc
Networks

….

….

Beyond Robotics and Asimov laws

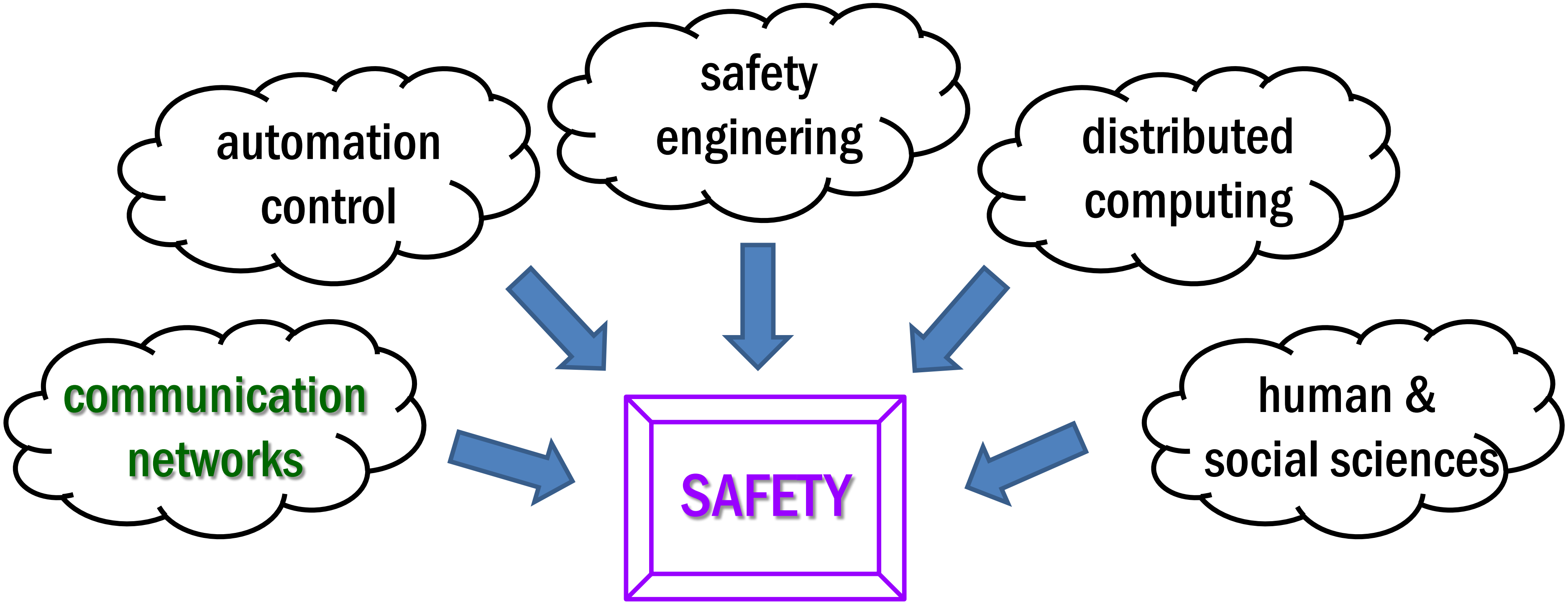
Humans surrounded by digital devices
Humans wear digital prostheses
Humans within digital prostheses (automated vehicles)

Cyberphysics

→ Augmented Human Capabilities

Réseaux spontanés de véhicules automatisés

Domaine applicatif ≈ tous les humains ➢enjeux sociétaux majeurs



automation control

safety enginering

distributed computing

communication networks

human & social sciences

SAFETY

≈ 0 fatalities ≈ 0 severe injuries

Lessons learned from Internet & Ethernet % wireless nets

Réseaux spontanés de véhicules automatisés

- ***Safety?*** So far: **4 fatalities**, dozens of severely injured passengers in hospitals.

Robotics +
WiFi broadcast ≈ 300 m

CAV (vehicules autonomes connectés)

- ***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).

Big **browser** is watching you

- ***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

[The Illegal $5 WiFi Jammer for iPhone & Android]()

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

Safety or/and mobility compromised by <u>remote unknown</u> cyberattackers

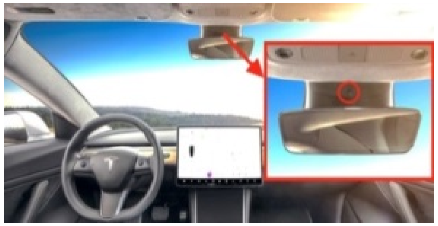
Privacy Threats with CAVs/V2X

In addition to:

❖ ❖ ❖ ❖ ❖❖ **EXTERNAL** EAVESDROPPING ❖ ❖ ❖ ❖ ❖ ❖

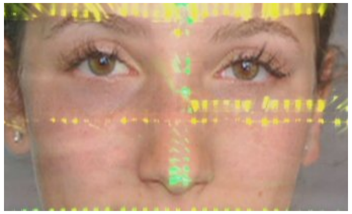
INTERNAL CYBER-ESPIONNAGE WITH **V2X**

Janusian justification: for assisted driving (ADAS)



Facial recognition

Continuous cybersurveillance



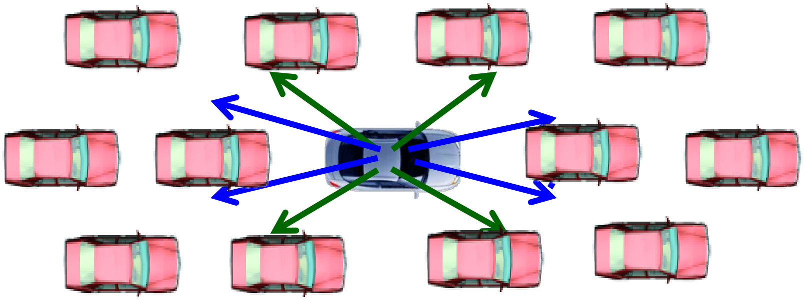
Who collects, stores, processes, mines, resells, personal data?

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) ?

7



Optique + radio cellulaire très courte portée (≈ 10-80 m), directionnelle

Algorithmes 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~~

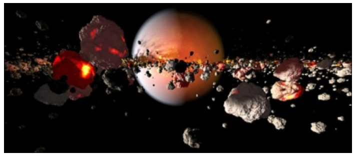
- 0 interventions humaines
- Innocuité absolue théorique
  (≈ 0 morts, ≈ 0 blessés graves)
- 0 atteinte à la vie privée
- 0 cyberattaque distante
- Cyberattaque locale: irrationnelle

Cyberphysical Constructs and Concepts
for Fully Automated Networked
Vehicles

Gérard Le Lann

RESEARCH REPORT
N° 9297
16/10/2019
RITS

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

les tâches physiques ou cognitives consomment du temps humain

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

Teilhard de Chardin :
La place de l'homme
dans la nature
Le groupe zoologique humain

10 18

Internet = innovation majeure dans l'aventure humaine