Real-Time Networks and Protocols for Industrial Automation

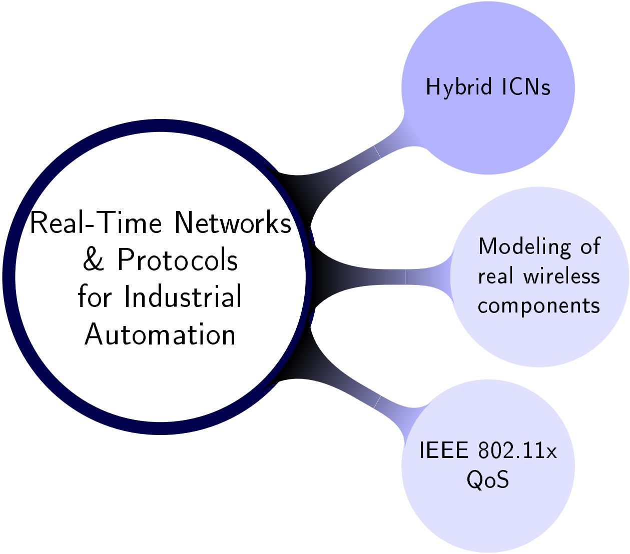
Lucia Seno

Italian National Council of Research, CNR - IEIIT
Department of Information Engineering
University of Padova, Italy

April 18th, 2011

DEPARTMENT OF INFORMATION ENGINEERING
UNIVERSITY OF PADOVA

Summary of Ph.D. research topics



Industrial Communication Networks

Nowadays Industrial Communication Networks (ICNs) are employed at all levels of factory automation systems

Industrial Communication Networks

Nowadays Industrial Communication Networks (ICNs) are employed at all levels of factory automation systems

ICNs are especially employed for device level communication

- *fast data exchange between controller and sensors/actuators*

Industrial Communication Networks

Nowadays Industrial Communication Networks (ICNs) are employed at all levels of factory automation systems

ICNs are especially employed for device level communication

- *fast data exchange between controller and sensors/actuators*

Precision of device level data exchange strongly influences the performance of a factory automation system

Industrial Communication Networks

Nowadays Industrial Communication Networks (ICNs) are employed at all levels of factory automation systems

ICNs are especially employed for device level communication

- *fast data exchange between controller and sensors/actuators*

Precision of device level data exchange strongly influences the performance of a factory automation system $\rightarrow$
ICNs, differently from general purpose networks, have to satisfy tight reliability and timing requirements

Networks/technologies for IC

Networks/technologies available for IC:

- Fieldbuses: ICNs implementing deterministic protocols (*Token Bus*, *Token Ring*, etc.)

Networks/technologies for IC

Networks/technologies available for IC:

- Fieldbuses: ICNs implementing deterministic protocols (*Token Bus*, *Token Ring*, etc.)
- Real Time Ethernet (RTE) networks: ICNs based on standard Ethernet IEEE 802.3 and using different techniques in order to improve determinism

Networks/technologies for IC

Networks/technologies available for IC:

- Fieldbuses: ICNs implementing deterministic protocols (*Token Bus*, *Token Ring*, etc.)
- Real Time Ethernet (RTE) networks: ICNs based on standard Ethernet IEEE 802.3 and using different techniques in order to improve determinism
- Wireless networks?

Wired ICNs

1. Fieldbuses
   - Transmission rates up to 10 Mb/s
   - Several products available (Profibus, P-Net, WorldFIP, Interbus, CAN, AS-interface, SERCOS I and II, Modbus, LonWorks, ControlNet, DeviceNet, etc.)
   - International Standard IEC 61158
   - Hundreds of millions nodes installed!
2. RTE networks
   - High transmission rates (up to 100 Mb/s)
   - Several products available (EtherNet/IP, Profinet, Ethernet Powerlink, EtherCAT, Modbus on TCP, SERCOS III, etc.)
   - International Standards IEC 61158 and IEC 61784
   - Increasing deployment

Wireless networks

1 Wireless networks

- Differently from wired networks, there are no wireless networks specifically developed for IC $\rightarrow$ research activity to evaluate/adapt existing wireless networks (IEEE 802.11 WLAN *WiFi*, IEEE 802.15.4 WPAN, IEEE 802.15.1 *Bluetooth*, etc.) according to IC requirements
- Transmission rates varying in a wide range (IEEE 802.15.4 250 Kb/s $\rightarrow$ IEEE 802.11 54 Mb/s)
- Wide deployment in several different fields

Wireless technology for IC: Pros and Cons

Pros:

- Cabling avoidance $\rightarrow$
  - Connection of devices that can not be reached by a cable (mobile components, etc.)
  - Decreased costs for cabling, installation and maintenance
  - Decreased risk of cables and connectors failures

Wireless technology for IC: Pros and Cons

Pros:

- Cabling avoidance →
  - Connection of devices that can not be reached by a cable (mobile components, etc.)
  - Decreased costs for cabling, installation and maintenance
  - Decreased risk of cables and connectors failures

Cons:

- Wireless channel is error prone →
  - High bit error rates (BER $\sim [10^{-3}, 10^{-2}]$)
  - Transmission errors caused by different phenomena (path loss, fast and slow fading, noise and interference) exacerbated in industrial environments
  - Non-stationary wireless channel error characteristic

Hybrid networks

Cons $\rightarrow$ *it seems unrealistic that wireless networks will totally replace wired ICNs (at least in the short-mid term)!*

Hybrid networks

Cons → *it seems unrealistic that wireless networks will totally replace wired ICNs (at least in the short-mid term)!*

Immediate employment of wireless technology for IC is for wireless extension of already deployed wired communication systems → hybrid (wired/wireless) networks

Hybrid networks

Cons → *it seems unrealistic that wireless networks will totally replace wired ICNs (at least in the short-mid term)!*

Immediate employment of wireless technology for IC is for wireless extension of already deployed wired communication systems → hybrid (wired/wireless) networks

Why hybrid networks?

Effective solution to the problem of connecting to an already deployed wired industrial communication system few nodes that can not be reached (easily/reliably) by means of a cable!

Problems in hybrid networks deployment (1 on 2)

1. Wireless networks are less performing than wired ICNs (lower tx rates, larger protocol overheads, half-duplex tx, rate adaptation mechanism for IEEE 802.11, etc.) → low throughput

Problems in hybrid networks deployment (1 on 2)

1. Wireless networks are less performing than wired ICNs (lower tx rates, larger protocol overheads, half-duplex tx, rate adaptation mechanism for IEEE 802.11, etc.) → low throughput

   Solutions:

   - Controller on the wired segment
   - Optimization of the wireless segment (reducing number of nodes and traffic)
   - Increasing throughput (IEEE 802.11n)

Problems in hybrid networks deployment (2 on 2)

2. Wireless networks employ medium access techniques based on randomness (IEEE 802.11 CSMA/CA, etc.) $\rightarrow$ unpredictable delays, jitter, missing deadlines in data delivery

Problems in hybrid networks deployment (2 on 2)

2. Wireless networks employ medium access techniques based on randomness (IEEE 802.11 CSMA/CA, etc.) $\rightarrow$ unpredictable delays, jitter, missing deadlines in data delivery

   Solutions:

   - TDMA (IEEE 802.15.4 beacon mode, PCF, iPCF)
   - Frame prioritization (IEEE 802.11e)

Problems in hybrid networks deployment (2 on 2)

2. Wireless networks employ medium access techniques based on randomness (IEEE 802.11 CSMA/CA, etc.) $\rightarrow$ unpredictable delays, jitter, missing deadlines in data delivery

   Solutions:
   - TDMA (IEEE 802.15.4 beacon mode, PCF, iPCF)
   - Frame prioritization (IEEE 802.11e)

3. Wireless networks present high bit error rates $\rightarrow$ re-transmissions, unpredictable delays, jitter and missing deadlines in data delivery

Problems in hybrid networks deployment (2 on 2)

2. Wireless networks employ medium access techniques based on randomness (IEEE 802.11 CSMA/CA, etc.) → unpredictable delays, jitter, missing deadlines in data delivery

   Solutions:
   - TDMA (IEEE 802.15.4 beacon mode, PCF, iPCF)
   - Frame prioritization (IEEE 802.11e)

3. Wireless networks present high bit error rates → re-transmissions, unpredictable delays, jitter and missing deadlines in data delivery

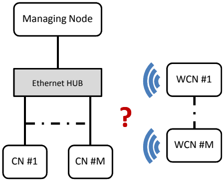
   Solutions:
   - Proper antennas placement
   - 5 GHz band (IEEE 802.11a)

Hybrid ICNs: a case study

Wireless extension of Ethernet Powerlink, by means of the IEEE 802.11g WLAN

Hybrid ICNs: a case study

Wireless extension of Ethernet Powerlink, by means of the IEEE 802.11g WLAN



- Already deployed Ethernet Powerlink system with one controller and M passive stations
- Necessity of connecting L new wireless passive stations

- Need to satisfy the same reliability and timing requirements satisfied by the pre-existing system
- Solutions?

Remarks

GOALs:
give insights on hybrid networks implementation,
highlight problems and possible solutions
concerning the interaction of the two networks,
evaluate performance.

Remarks

GOALs:
give insights on hybrid networks implementation,
highlight problems and possible solutions
concerning the interaction of the two networks,
evaluate performance.

Organization of research activity:

Remarks

GOALs:
give insights on hybrid networks implementation,
highlight problems and possible solutions
concerning the interaction of the two networks,
evaluate performance.

Organization of research activity:

- theoretical analysis (networks and devices specifications, scientific literature)

Remarks

GOALs:
give insights on hybrid networks implementation,
highlight problems and possible solutions
concerning the interaction of the two networks,
evaluate performance.

Organization of research activity:

- theoretical analysis (networks and devices specifications, scientific literature)
- simulative analysis (Opnet network simulator)

Remarks

GOALs:
give insights on hybrid networks implementation,
highlight problems and possible solutions
concerning the interaction of the two networks,
evaluate performance.

Organization of research activity:

- theoretical analysis (networks and devices specifications, scientific literature)
- simulative analysis (Opnet network simulator)
- experimental analysis

Ethernet Powerlink

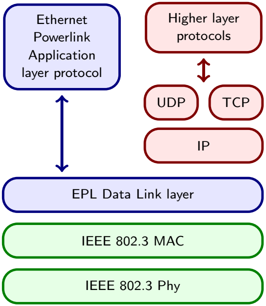
Ethernet Powerlink (EPL) is a popular RTE network defined by

1. EPL Standardization Group specifications (www.ethernet-powerlink.org)
2. International Standard IEC61784-2 (CPF#13, CP#1)

Ethernet Powerlink

Ethernet Powerlink (EPL) is a popular RTE network defined by

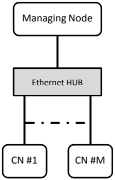
1. EPL Standardization Group specifications (www.ethernet-powerlink.org)
2. International Standard IEC61784-2 (CPF#13, CP#1)



EPL network architecture

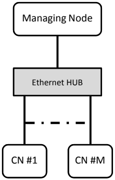
- Data Link layer protocol placed on top of standard Ethernet IEEE 802.3 Phy and MAC
- EPL frames are transmitted in standard Ethernet frames

EPL Data Link Layer



- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})

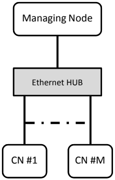
EPL Data Link Layer



- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})

EPL cycle

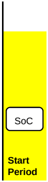
EPL Data Link Layer



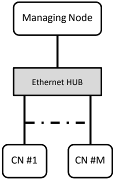
- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})

EPL cycle

1. Start Period



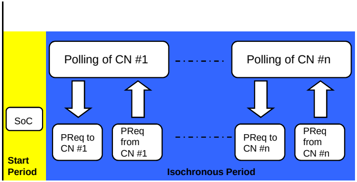
EPL Data Link Layer



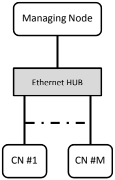
EPL cycle

1. Start Period
2. Isochronous Period

- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})



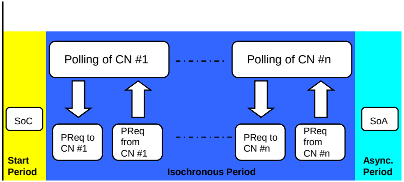
EPL Data Link Layer



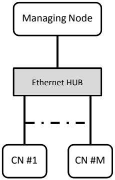
- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})

EPL cycle

1. Start Period
2. Isochronous Period
3. Asynchronous Period



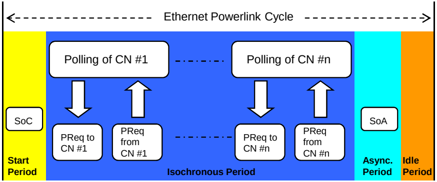
EPL Data Link Layer



- EPL Data Link layer protocol specifies a medium access technique based on TDMA
- The Managing Node (MN) polls the Controlled Nodes (CNs) during a cycle of fixed duration (t_{EPL})

EPL cycle

1. Start Period
2. Isochronous Period
3. Asynchronous Period
4. Idle Period



Implementation of the wireless extension

ISO/OSI model specifies that the interconnection between different communication systems has to be achieved by means of Intermediate Systems (ISs)

Types of ISs:

- Phy layer: repeaters
- Data Link layer: bridges
- Higher layers: gateways

Implementation of the wireless extension

ISO/OSI model specifies that the interconnection between different communication systems has to be achieved by means of Intermediate Systems (ISs)

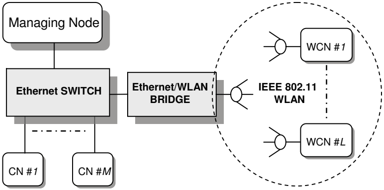
Types of ISs:

- Phy layer: repeaters
- Data Link layer: bridges
- Higher layers: gateways

We offered two different wireless extensions: one realized at the Data Link layer and the other realized at the Application layer.

Extension at the Data Link layer

Bridge-based wireless extension:

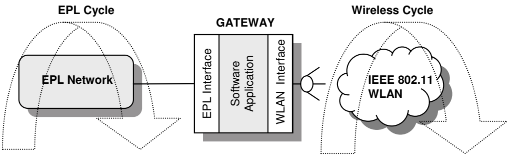


WCNs are directly included in the EPL cycle!

WCNs are directly included in the EPL cycle as CNs and the PReq and PRes frames flow across the bridge transparently to the EPL protocol.

Extension at the Application layer

Gateway-based wireless extension:



WCNs are polled by an application running on the gateway!

WCNs are polled by a specific application running on the gateway, implemented on one of the EPL network CNs.
Two different asynchronous cycles are running on the hybrid network: the EPL cycle which involves only CNs and the WCNs cycle realized by the gateway.

Performance Indicators

Hybrid networks performance evaluation

Performance Indicators

Hybrid networks performance evaluation→ need to define a set of Performance Indicators (PIs)

- to describe hybrid networks behavior
- to highlight how the choice of system parameters influences the system behavior

Performance Indicators

Hybrid networks performance evaluation$\rightarrow$ need to define a set of Performance Indicators (PIs)

- to describe hybrid networks behavior
- to highlight how the choice of system parameters influences the system behavior

Examples of considered PIs:

1. Polling Time (T_p)
2. Minimum Cycle Time (MCT)
3. Delivery Time (DT)
4. Real Time Throughput (RTT)

Polling Time

Polling Time T_p = time necessary to successfully poll a WCN

$$T_p = t_{det} + T_{rand}$$

Polling Time

Polling Time T_p = time necessary to successfully poll a WCN

$$T_p = t_{det} + T_{rand}$$

$$t_{det} = t_{data} + t_{ack} + t_{int}$$

$$\begin{aligned} t_{data} &= \text{transmissions of data frames} \\ t_{ack} &= \text{transmissions of ack frames} \\ t_{int} &= \text{interframe times} \end{aligned}$$

$$T_{rand} = T_{backoff} + T_{re-tx} + T_{devices}$$

$$\begin{aligned} t_{backoff} &= \text{backoff times} \\ t_{re-tx} &= \text{retransmissions} \\ t_{devices} &= \text{delays introduced by devices (buffer queues, operating} \end{aligned}$$

Minimum Cycle Time

Cycle time t_{EPL} of an EPL network is defined by the user in the off-line configuration phase and represent the sampling time of the system

Minimum Cycle Time MCT = lower bound of t_{EPL}

$$MCT = \sum_{i=1}^{L} \max\left(T_p^i\right)$$

L = number of WCNs

Delivery Time

Delivery Time DT = *"the time needed to convey an APDU containing data (message payload) that has to be delivered in real-time from one node (source) to another node (destination)"*

$$DT = T_{wait} + T_p$$

T_{wait} = time the data have to wait in the node before the polling starts, depends on T_{EPL} and on the data generation process

Real Time Throughput

Real Time Throughput RTT = *"number of octets per second transmitted on a specific link (i) exclusively relevant to real-time traffic"*

$$RTT^i = \frac{b^i}{t_{EPL}}$$

- inversely proportional to t_{EPL}, if b^i is constant, higher bound: $\frac{b^i}{MCT}$
- decreasing t_{EPL} down to MCT increases failed polling and, consequently, decreases b^i $\rightarrow$ tradeoff

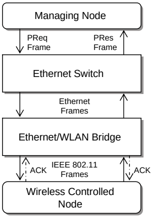
Theoretical analysis

Hypotesis

1. Ideal wireless channel
2. Semi-ideal interconnection components (introducing only queue delays)
3. Semi-ideal EPL devices (introducing only fixed, EPL standard-specified delays)

Example of PIs computation for the bridge-based extension

$$
\begin{aligned}
T_p &= t_{txP\,Req} + t_{txPRes} + \\
&\quad + t_{wtxP\,Req} + t_{wtxPRes} + \\
&\quad + 2t_{Ack} + 2t_{SIFS} + t_{DIFS} + \\
&\quad + D_{CN} + B = \\
&= 287.72\mu s + [0 \div 15] \cdot 9\mu s
\end{aligned}
$$



$$MCT = L \cdot t_{const} + (2L - 1) \cdot B$$

$B = CW_{min} \cdot t_{slot}$ = one backoff time (the first time the bridge does not execute backoff)

Simulation

Hypotesis

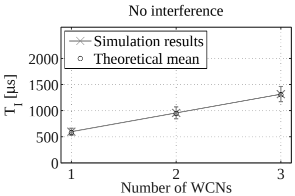
1. Non-ideal wireless channel
   - Interference: caused by other communication systems transmitting on the same band
   - Fast fading: caused by the addition/removal of obstacles to signal propagation (e.g. movement of people/machines)
2. Semi-ideal interconnection components (introducing only queue delays)
3. Semi-ideal EPL devices (introducing only fixed, EPL standard-specified delays)

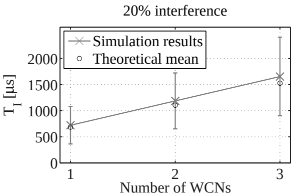
Wireless channel modeling

1. Interference
   - Effects: increased traffic on the wireless channel → incorrect/delayed/missed frame receptions
   - Modeling: other wireless stations using a certain percentage of the band
   - Effects of fading may be reduced using prioritized frames (IEEE 802.11e)!
2. Fast fading
   - Effects: temporal signal degradation → incorrect/delayed/missed frames receptions
   - Modeling: Gilbert-Elliott model

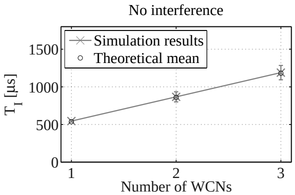
Example of simulation results

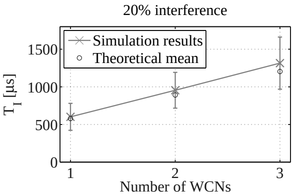
Non-prioritized frame (IEEE 802.11g):





Prioritized frame (IEEE 802.11e):

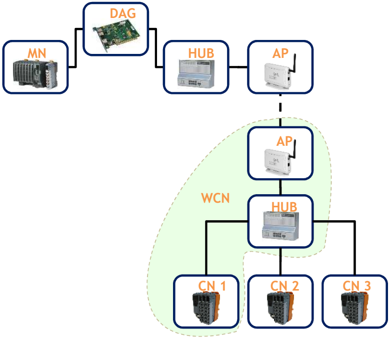




Experimental scenario

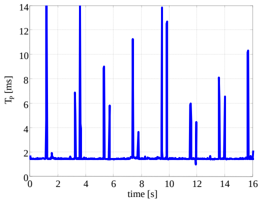
Hypotesis

1. Semi-ideal wireless channel (no interference, verified with a spectrum analyzer)
2. Real interconnection devices:
   - Linksys WAP54G Access Points
   - 3Com Office Connect Access Points
3. Real EPL devices
4. DAG board timestamping (60 ns resolution)

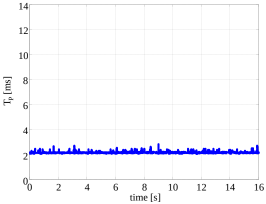


Example of experimental measurements (1 on 2)

T_p measured with Linksys APs:



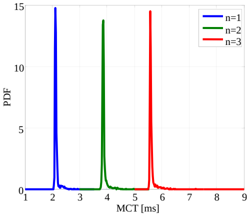
T_p measured with 3Com APs:



- Linksys APs cause periodic peaks in T_p (Idle state of the AP? Problem of AP parameters inaccessibility!)
- T_p values are considerably higher than those obtained from theoretical and simulative analysis (APs introduces consistent delays)

Example of experimental measurements (2 on 2)

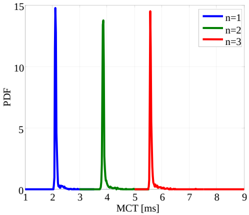
MCT empirical pdf with 3Com APs:



- Very asymmetric pdfs (presence of high value samples)!
- Delays introduced by the AP are non-negligible and non-predictable!

Example of experimental measurements (2 on 2)

MCT empirical pdf with 3Com APs:



- Very asymmetric pdfs (presence of high value samples)!
- Delays introduced by the AP are non-negligible and non-predictable!

Need to introduce models of real wireless components in the theoretical and simulative analysis!

Conclusion and Future Work

1. We analyzed a possible wireless extensions of Ethernet Powerlink by means of the IEEE 802.11 WLAN
2. We defined and computed, theoretically, via simulations and experimentally, a set of PIs suitable for polling-based networks
3. We shown how the presence of wireless channel non-idealities can negatively affect the system behavior
4. We proposed possible solutions
5. We experienced significant differences between theoretical analysis and experimental results
6. We experienced that IEEE 802.11 devices in some case present undesirable, not-modifiable behaviors
7. Future work will concern modeling of real wireless devices and strategies to limit the negative effects their behavior introduces in wireless network reliability

Publications

- L. Seno, S. Vitturi, C. Zunino, *"Analysis of Ethernet Powerlink Wireless Extensions Based on the IEEE 802.11 WLAN"*. IEEE Transactions on Industrial Informatics, vol. 5, n. 2, pp. 86-98, May 2009
- L. Seno, S. Vitturi, *"Wireless extension of Ethernet Powerlink networks based on the IEEE 802.11 Wireless LAN"*. Proceedings of the 7th IEEE International Workshop on Factory Communication Systems (WFCS 2008)
- G. Gamba, L. Seno, S. Vitturi, *"Performance indicators for wireless industrial communication networks"*. Proceedings of the 8th IEEE International Workshop on Factory Communication Systems (WFCS 2010)
- G. Gamba, L. Seno, S. Vitturi, *"Theoretical and experimental evaluation of polling times for wireless industrial networks using commercially available components"*. Proceedings of the 15th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2010)

Thank you!