A Bayesian Packet Sharing Approach for Noisy IoT Scenarios

A.M. Vegni\textsuperscript{1}, V. Loscrì\textsuperscript{2}, A. Neri\textsuperscript{1}, and M. Leo\textsuperscript{3}

\textsuperscript{1} COMLAB Telecommunication Laboratory
Roma Tre University, Department of Engineering, Rome, Italy

\textsuperscript{2} Inria Lille – Nord Europe, Lille, France

\textsuperscript{3} RadioLabs – Rome, Italy
Outline

• Introduction:
  – Smart City & Internet of Things

• Related projects:
  – DAHMS (Distributed Architecture Home Modular Multifunctional Systems) & LogON (Logistics Open Network)

• Open issue:
  – To reduce the huge amount of data generated by sensing devices. This can affect energy consumption and cause network congestion.

• Our solution:
  – An IoT Bayesian approach with cloud architecture
  – Data sharing based on Pearl’s Belief Propagation (BP) with the twofold objective of (i) recovering missing data, and (ii) reconstructing incomplete or corrupted messages

• Conclusions
From Smart Cities to Internet of Things

• Smart City is a paradigm shift combining:
  – Sensors,
  – Devices,
  – Internet of Things (IoT),
  – Machine-to-Machine (M2M).

• The IoT is an emerging global Internet-based information architecture, with the aim of
  – facilitating the exchanges of “things” in a secure and reliable manner.
DAHMS project (1/3)

- DAHMS is a project founded by the Italian Minister of Economic Development in the framework “New Technologies for the Made in Italy”.
- **Goal**: to improve the quality of life of disabled persons through the integration of home automation and remote healthcare functionalities.
DAHMS project (2/3)
- Architecture -

• Fixed and mobile devices based on Raspberry and Arduino, able to notify events, send/receive data and commands from a set of local and remote control interfaces.

• Each device is equipped with MQTT. The information sent follows a publish-subscribe framework able to forward MQTT messages.

• Secure Mediation GateWay (SMGW) represents the conjunction element among the devices within the Control Room and on-board devices.
DAHMS project (3/3)
- Overview -

Control Room

Remote Sensors Log

RFID Access Log

REST

MQTT

Pub/Sub

Internet

VEHICULAR

LTE/HSDPA

SMGW

SOAP – WS Security

MySQL
LogON project
- Overview -

• LogON is a project funded by the Italian Minister of Economic Development in the framework of “Bando Industria 2015”.

• It deals with the study, development and test of a novel platform of services and devices for the logistics in urban environment.
IoT Network Model (1/2)

- Following DAHMS architecture, and due to the heterogeneity of the IoT devices, we assume a *cloud-based multi-network scenario* with a plethora of interconnected devices.

- Each device performs sensing and processing activities. Gateways collect data and forward to the cloud.

- GWs and IoT nodes implement publish-subscribe message passing mechanisms.
IoT Network Model (2/2)

• An IoT node can act in two states:
  – *Idle state*: it is disconnected
  – *Active state*: it can perform sensing activities, and can send and receive messages

• Errors in the connectivity links among IoT devices can affect communication reliability, and also cause packet losses.
  – Error concealing strategy based on BP message passing algorithm with a twofold objective *i.e.*, (i) to recover missing data, and (ii) to reconstruct “incomplete” or “corrupted” messages.
IoT as a Bayesian network

• Our assumptions:
  – Each node is initiated in active mode and transmits messages to its neighbors,
  – A message is related to local data measurements, sampled at fixed time step,
  – The global information is related to a given sub-network and is obtained from the contributions coming from each IoT device within the sub-network.

• Our aim is to estimate the state $\mathbf{X}$ of the sensed environment starting from the sets $\{\mathbf{D}_i\}$ of data collected by the individual nodes related to non-overlapping regions $\{\mathbf{R}_i\}$. 
MRFs and Factor Graphs

• To derive the distributed state estimation model, we resort to the unified representation for both Bayesian Networks and MRFs, constituted by the Factor Graphs (FGs).

• $\mathbf{X}$ is modeled as a Markov Random Field, so that we have

$$P_X(\mathbf{X}) = \frac{1}{Z} \exp\{-U(\mathbf{X})\} = \frac{1}{Z} \exp\left\{- \sum_{\text{clique } c} V_c(\mathbf{X})\right\}$$

Energy function \hspace{1cm} Potential of clique $c$

• FGs use factor nodes to describe the factorization property of the joint distribution, as the one by Hammersley-Clifford Theorem.

$$P_X(\mathbf{X}) = \prod_i \phi_i(\mathbf{x}_i) \prod_{(i,j) \in E} \phi_{ij}(\mathbf{x}_i, \mathbf{x}_j),$$

Message exchange among node $i$ and $j$
BP algorithm (1/2)

• This is a message-passing algorithm for the calculation of a posteriori probabilities of nodes of a loop-free factor graph, given a priori probabilities and observations.

• This approach represents an update to the outgoing message from the $i$-th node to the $j$-th neighboring node. So, the message update operation from $i$-th to $j$-th node related to local information $x_i$ is proportional to

$$m_{ji}(x_i) \propto \int \varphi_{ji}(x_j, x_i) \varphi_j(x_j) \prod_{u \in \Gamma_j \setminus i} m_{uj}(x_j) dx_j$$

Incoming messages from previous iteration
BP algorithm (2/2)

- The BP algorithm starts with a “belief updating” phase, where the \textit{a posteriori} probabilities of the random variable \( x_i \) are computed through the information about the evidence coming from the neighboring nodes.

\[
BEL(x_i) = \alpha \mu(x_i) \lambda(x_i) \pi(x_i)
\]

Double contribution from “child” and “parent” nodes.
Conclusions

• The problem of data sharing and message correction in an heterogeneous IoT networks scenario, with a plethora of devices for sensing applications, has been addressed.

• The IoT environment has been investigated through a Bayesian approach.

• A BP algorithm for message correction, and information update has been presented in its infancy, through the Markov Random Field and Factor Graph theory.
Thank you for your attention!

annamaria.vegni@uniroma3.it