2016 IEEE First International Conference on Internet-of-Things Design and Implementation

A Bayesian Packet Sharing Approach for Noisy IoT Scenarios

Anna Maria Vegni*, Valeria Loscrí†, Alessandro Neri*, and Marco Leo‡
*Department of Engineering, Roma Tre University
COMLAB Telecommunication Laboratory, Rome, Italy
Email:{*amvegni, neri*}@uniroma3.it
†Inria Lille - Nord Europe, Lille, France
Email: valeria.loscri@inria.fr
‡RadioLabs Consortium, Rome, Italy
Email: marco.leo@radiolabs.it

***Abstract*—Cloud computing and Internet of Things (IoT) represent two different technologies that are massively being adopted in our daily life, playing a fundamental role in the future Internet. One important challenge that need to be handled is the enormous amount of data generated by sensing devices, that make the control of sending useless data very important. In order to face with this challenge, there is a increasing interest about predictive approaches to avoid to send high spatio-temporal correlated data. Belief Propagation (BP) algorithm is a method of performing approximate inference on arbitrary graphical models that is becoming increasingly popular in the context of IoT. By exploiting BP, we can derive effective methods to drastically reduce the number of transmitted messages, while keeping high the data throughput in the global information system. In this paper, we propose a BP approach in a hierarchical architecture with simple nodes, gateways and data centers. We evaluate the error bounding and propose a corrective mechanism to keep a certain quality of the global information in the architecture considered.**

Keywords*—*IoT, Belief Propagation, Markov Random Fields, Cloud.

I. Introduction

Recently, with the evolution of the Internet and related technologies, there has been an evolution of a new emerging paradigm, namely the Internet of Things (IoT) [2]. In IoT scenarios, a large number of devices –and more in general objects– are seamlessly connected to each another for information sharing through the Internet. All these devices connected to the IoT may be of heterogeneous types with respect to their operational mode, and communication technologies. As one of the main strengths behind the IoT paradigm, it is the high impact on several aspects of everyday-life, from working to the domestic fields. As an instance, domotics [10], and smart cities [4] are main application scenarios where the IoT paradigm is expected to play a leading role in the next future.

From the above considerations, and due to the huge amount of heterogeneous devices, information sharing among IoT devices is one of the biggest challenges. Classic Internet approaches need to be revised to address the complex requirements imposed by IoT. This asks for the development of intelligent algorithms for routing [1], information sharing security [6], novel network paradigms [7], new services [11], and advanced techniques for data fusion [3]. A few related works have addressed the issue of forwarding data among IoT devices, by modeling the IoT network as a Bayesian network [3], [8], [9]. Under this hypothesis, Bijarbooneh *et al.* [3] present an adaptive sensing belief propagation algorithm, where each node updates its belief about the environment status by incorporating its local measurement with the beliefs of its neighboring nodes and the belief obtained in the past.

In this paper, we address the connectivity issue among IoT heterogeneous devices for data sharing, under the hypothesis of Bayesian Networks and Markov Random Fields, both modeled by means of Factor Graphs. We assume each IoT device represents a node in the IoT network with some sensing and processing capabilities. Moreover, these devices may be located at different places across the globe. They are connected to the Internet, although the rate of data transfer, and the supported security level may be different. Each node needs to get information about its local environment, in order to perform some task and/or to provide this information to a higher decision level. As an instance, an IoT node deployed in a domestic network may need information about current and future usage of some limited resources, like energy or communication bandwidth, to orchestrate their consumption with the help of the other IoT devices controlling specific appliances. Data exchange among devices allows a single node to increase its own knowledge of global information and optimize the scheduling of the tasks that it has to accomplish with the usage of a shared resource.

This paper introduces a data sharing approach based on Pearl's Belief Propagation (BP) algorithm in the IoT context with a cloud-based architecture. BP is an iterative technique mainly used for solving inference problems. In the IoT context, the belief of a device (*e.g.*, a sensor node) is the data measurement. The BP infers the measurements of other neighboring devices, especially in cases where the data is missing. Moreover, the BP technique allows to correct the errors that can occur in the data propagation; at each run, the BP provides to the devices both spatial and temporal cooperation. Indeed, in BP-based approaches, each sensor node determines its belief by incorporating its local measurement with the beliefs of its neighboring nodes, as well as its beliefs obtained in the past run. Then, at each run, we assume a node is able to (*i*) reduce the own distortion level (*i.e.*, estimation error on

978-1-4673-9948-7/16 $31.00 © 2016 IEEE
DOI 10.1109/IoTDI.2015.28

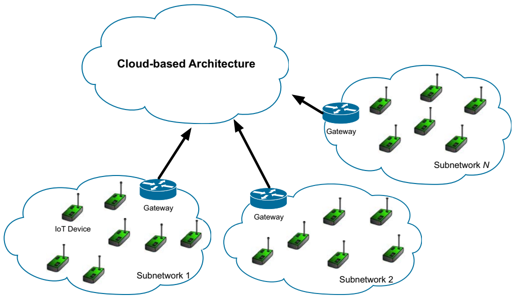

Figure 1: A cloud-based IoT network model.

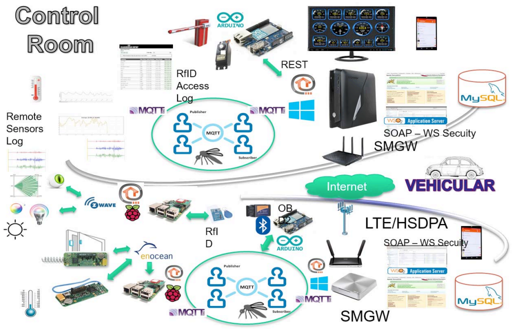

Figure 2: DAHMS's proof of concept architecture.

global information), and (*ii*) provide an update of the global information to be shared with other neighboring nodes.

This paper is organized as follows. Section II describes the reference cloud-based architecture for the IoT scenario. Due to the heterogeneity of the IoT devices, we assume a multi-network scenario with a plethora di interconnected devices. In Section III we present our technique based on BP algorithm, for data sharing in a noisy IoT scenario. The presence of errors along the message reconstruction phase occurring at each receiver node can be mitigate through our BP's algorithm. Finally, conclusions are drawn at the end of this paper.

II. Network Model

In our architecture, we consider different entities with specific computational and communication capabilities and functionalities. As illustrated in Figure 1 the IoT network model may comprise several sub-networks associated with different applications. Indeed, due to the huge amount of IoT devices, we assume each sub-network is composed by IoT devices connected to each others for data sharing, and a gateway that interacts with the "external world". The role of the gateways consists into relaying the messages to the cloud, which is responsible of typical cloud-based services (*e.g.*, data fusion, storage, etc.).

Each device performs sensing and processing activities. Our network model supports multi-hop routing, and the gateways collect data and forward them to the cloud. To support high scalability of the architecture, gateways implement publish-subscribe message passing mechanisms based on message brokers. Depending on the device capabilities, publish-subscribe mechanisms can be supported even at IoT node level. In this scenario, we assume that each IoT node can be in two states, either idle or active. A node is in a idle state, when it disconnects its radio, and it cannot send and receive data. On the other hand, a node is in active state when it can perform sensing activities, and can send and receive messages.

Moreover, presence of errors in the connectivity links among IoT devices has to be accounted for. This can affect communication reliability, and also cause packet losses. Packet retransmission are then necessary to overcome packet errors and losses. At the same time, the increase of message retransmissions affects energy consumption on each IoT devices, latency in information sharing, and in the extreme case, network congestion. So, in order to keep low the effective number of retransmissions, each active sensor implements an 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.

The proposed architecture has been adopted by the authors in the design of the proof of concept of DAHMS and LogOn projects, both funded by the Italian Ministery of Economic Development in the framework "New Technologies for the Made in Italy", carried out at the Radiolabs research center labs. DAHMS (Distributed Architecture Home Modular Multifunctional Systems) scope is the improvement of the quality of life and the degree of self-sufficiency of chronically ill and elderly and disabled persons through the integration of Home Automation and remote heath-care functionalities. LogOn (Logistic Open Network) concerns the goods logistic in historical art cities with high level of tourism economy.

Both projects include fixed and mobile IoT devices, typically based on Raspberry and Arduino platforms, able to notify events, send data and receive data and commands from a set of local and remote control interfaces, including those implemented on Android and iOS smartphones. In Figure 2 the Secure Mediation GateWay (SMGW) represents the conjunction element among the devices within the Control Room and on-board (vehicular) devices. The information messages sent from each device follow a publish/subscribe framework able to forward MQTT (MQ Telemetry Transport) messages, provided by the Mosquitto message broker. MQTT is a messaging protocol working on the top of TCP/IP, that has been projected for specific situations where low impact and limited bandwidth are required. All the devices are equipped with MQTT and will be in charge to forward informations about events or commands. Through the federated system of SMGW, the informations published via MQTT will be available in a seamless way from each intraSMGW domain, as described in the architectural scheme of SMGW. Within each domain, the devices are in charge of exchanging event/commands and messages with the SMGW. Also, the SMGW exports each message in a secure way towards all the other SMGWs. At this aim the WS-Security extension to SOAP, published by OASIS has been adopted.

III. A BP Technique for Error Correction

In this section, we investigate the proposed BP technique in IoT noisy scenarios. Our aim is to reduce the message errors through an iterative algorithm that corrects and updates the received data at each run. With regards to Figure 1, each device is initiated in active mode, and transmits messages to its own neighbors. A message is related to local data measurements, sampled at a fixed time step. The global information, related to a given sub-network, is then obtained from the contributions coming from each IoT device within the subnetwork.

Let us assume that the distributed sensing system consists of N IoT nodes, interconnected in various ways. Each IoT node collects a set of data provided by several sensors. Our scope is then 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 $\{\mathbf{R}_i\}$. Here $\mathbf{X}$ is modeled as a dynamical Random Field. More in detail we focus our attention to the case in which the dynamical (*i.e.* temporal) behavior of the system can be described by a linear model, while the spatial behavior is described by a Markov Random Field (MRF).

We incidentally recall that given a finite rectangular lattice $L = \{(i,j), \quad 1 \leq i \leq N_1, \quad 1 \leq j \leq N_2\}$, a neighborhood system associated with L is, by definition, a collection of subsets $\eta = \{\eta_{ij}\}$ with the property that each subset η_{ij}, namely the neighborhood of i, j, is such that:

- $(i,j) \in \eta_{ij}$,
- if $(k,l) \in \eta_{ij}$, then $(i,j) \in \eta_{kl}, \quad \forall (i,j) \in L$

It follows that a random field $\mathbf{X}$ is said to be a MRF w.r.t. (L, η) if and only if:

$$\begin{aligned} & P\left(X(i,j)/X(k,l),(k,l) \in L - \{(i,j)\}\right) = \\ & = P\left(X(i,j)/X(k,l),(k,l) \in \eta_{ij} - \{(i,j)\}\right), \\ & \forall (i,j) \in L. \end{aligned}$$

Then, in the distributed estimation scheme we can take advantage of the Hammersley-Clifford Theorem, stating that the joint distribution of a MRF w.r.t. (L, η) is of the form

$$P_{\mathbf{X}}(\mathbf{x}) = \frac{1}{Z} \exp\left\{-U(\mathbf{x})\right\}, \tag{1}$$

where Z is a normalizing constant and

$$U(\mathbf{x}) = \sum_{\forall clique\ c} V_c(\mathbf{x}), \tag{2}$$

is the energy function, and $V_c(\mathbf{x})$ is the potential associated with clique $c \in C$. The only constraint on the clique potential $V_c(\mathbf{x})$ is that it depends only on the restriction of $\mathbf{x}$ to C. Nevertheless, here we focus our attention on those MRFs for which the potential function consists only of a set of *singleton potentials*, defined on single variables, and on a set of pairwise potentials, defined on pairs of variable.

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). FGs use *factor nodes* to describe the factorization property of the joint distribution, as the one stated by the Hammersley-Clifford Theorem. At this aim, for sake of compactness of the notation, and without loss of generality, we assume that the sensor data $\mathbf{D}_i$ and $\mathbf{D}_j$ provided by the sensors respectively connected to the *i*-th and *j*-th node cover two non-overlapping areas, and that the overall state space $\mathcal{X}$ is the Cartesian product of the state subspaces $\mathcal{X}_i$ associated to the environmental variables related to the areas covered by the individual nodes.

By associating each node i of a sub-network, with a random variable $\mathbf{X}_i$ that represents the local information, and by considering a set of edges E, we can write the joint distribution as:

$$P_{\mathbf{X}}(\mathbf{x}) = \prod_i \psi_i(\mathbf{x}_i) \prod_{(i,j)\in E} \psi_{ij}(\mathbf{x}_i, \mathbf{x}_j), \tag{3}$$

where the function $\psi_{ij}()$ represents the message exchange among node i and j. In practice, $p(\mathbf{x}_i)$ represents the marginal distribution of i-th node, and the BP allows the computation of the marginal distribution at each node i.

From rate-distortion theory, given a one-dimensional random variable $\widehat{X}\,(X)$ is the representation of X, so that

$$\widehat{X} \in \left\{1, 2, ..., 2^{nR}\right\}, \tag{4}$$

where R are the bits needed for the representation of X. Then, the *distortion function* is a mapping $d : \mathcal{X} \times \widehat{\mathcal{X}} \to \mathbb{R}^+$, from the set of source alphabet pairs $\mathcal{X}$ into the set of non-negative real numbers. It measures the cost of representing symbol x by $\hat{x}$. By assuming a squared-error distortion *i.e.*,

$$d\left(x, \widehat{x}\right) = \left(x - \widehat{x}\right)^T \left(x - \widehat{x}\right), \tag{5}$$

we can derive the distortion between sequences x^n and $\hat{x}^n$ as

$$d\left(x^n, \hat{x}^n\right) = \frac{1}{n} \sum_{i=1}^{n} d\left(x_i, \hat{x}_i\right). \tag{6}$$

It follows that the distortion associated with a $(2^{nR}, n)$ code is defined as:

$$D = E\left[d\left(X^n, g_n\left(f_n\left(X^n\right)\right)\right)\right], \tag{7}$$

where $f_n : \mathcal{X}^n \to \left\{1, 2, ..., 2^{nR}\right\}$, and $g_n : \left\{1, 2, ..., 2^{nR}\right\} \to \hat{\mathcal{X}}^n$.

Finally, we can derive the *information rate distortion function* $R(D)$ for a source X with distortion measure $d(x, \hat{x})$ as:

$$R\left(D\right) = \min I\left(X; \hat{X}\right), \tag{8}$$

where $I(X; \hat{X})$ is the mutual information. Notice that Eq. (8) is subject to the following constraint

$$p\left(\hat{x}|\, x\right) : \sum\nolimits_{(x,\hat{x})} p\left(x\right) p\left(\hat{x}|\, x\right) d\left(x, \hat{x}\right) \leq D, \tag{9}$$

that is, the minimization of the mutual information is over all conditional distribution $p\left(\hat{x}|\, x\right)$ for which the jointly distribution $p(x, \hat{x})$ satisfies the expected distortion constraint.

From (7), the expectation value respect to the probability distribution on $\mathcal{X}$ is as follows:

$$D = \sum x^n p\left(x^n\right) d\left(x^n, g_n\left(f_n\left(x^n\right)\right)\right). \tag{10}$$

Now, in order to solve previous equation, we need the estimation of x_i. This can be provided through the BP algorithm. This is a message passing algorithm for the calculation of *a posteriori* probabilities of nodes of a loop-free FG, given *a priori* probabilities and observations. As known, the BP algorithm is a graphical model to represent conditional independence relations of large numbers of random variables.

Since the BP algorithm is a message-passing technique between nodes, and represents an update to the outgoing message from i-th node to j-th neighboring node, we can state that the message from i-th to j-th node related to the local information $\mathbf{x}_i$ is proportional to

$$m_{ji}(\mathbf{x}_i) \propto \int \psi_{ji}(\mathbf{x}_j, \mathbf{x}_i)\psi_j(\mathbf{x}_j) \prod_{u\in\Gamma_j\setminus i} m_{uj}(\mathbf{x}_j)d\mathbf{x}_j, \quad (11)$$

where the incoming messages from previous iteration are represented by m_{uj}. This equation represents the *message update operation* that is performed in the BP's algorithm. Notice that the BP is capable to compute the exact marginalization in the case of tree-structured graphical models, and this means that (11) converges in a finite number of iterations, limited to a superior bound, that is the length of the longest path in the graph.

The BP algorithm starts with a "belief updating" phase, where the a posteriori probabilities of the random variable $\mathbf{x}_i$ associated to the i-th node, *i.e.* $BEL(\mathbf{x}_i)$, is computed through the information about the evidence coming from the neighboring nodes *i.e.*, $BEL(\mathbf{x}_i) = \alpha\mu(\mathbf{x}_i)$, where $\mu(\mathbf{x}_i)$ represents the double contribution from "child" and "parent" nodes w.r.t. the i-th node *i.e.*,

$$\mu\left(\mathbf{x}_i\right) = \lambda\left(\mathbf{x}_i\right)\pi\left(\mathbf{x}_i\right), \quad (12)$$

with

$$\lambda\left(\mathbf{x}_i\right) = \prod_j \lambda_{\mathbf{x}_j}\left(\mathbf{x}_i\right), \quad (13)$$

$$\pi\left(\mathbf{x}_i\right) = \sum_{\mathbf{u}_1,\ldots,\mathbf{u}_n} P\left(_i \right| \mathbf{u}_1, ..., \mathbf{u}_n) \prod_k \pi_{\mathbf{x}_i}\left(\mathbf{x}_k\right), \quad (14)$$

where j and k are the indexes for the child and parent nodes, respectively. Figure 3 depicts a schematic of an IoT FG, assumed as a graph with parent and child nodes with respect to the $\mathbf{x}_i$ node. The computation of the a posteriori probability of the node $\mathbf{x}_i$, given all evidence except for the information coming from the j-th child node, is obtained through the parent-to-child message for the child node whose information is excluded. The message from the i-th parent node $\mathbf{x}_i$ to the j-th child node $\mathbf{y}_j$ is denoted as $\pi_{\mathbf{y}_j}\left(\mathbf{x}_i\right)$, whose expression is:

$$\pi_{\mathbf{y}_j}\left(\mathbf{x}_i\right) = \alpha \prod_{m\neq j} \lambda_{\mathbf{y}_m}\left(\mathbf{x}_i\right) \sum_{\mathbf{u}_1,\ldots,\mathbf{u}_n} P\left(\mathbf{x}_i\right| \mathbf{u}_1, ..., \mathbf{u}_n) \prod_k \pi_{\mathbf{x}_i}\left(\mathbf{u}_k\right). \quad (15)$$

Finally, the computation of the conditional probability of the evidence coming from the children of $\mathbf{x}_i$ given different possible values for the random variable corresponding to the i-th node is obtained through the message exchange from the j-th child node to the k-th parent node as:

$$\lambda_{\mathbf{x}_i}\left(\mathbf{u}_i\right) = \beta \sum_{\mathbf{x}_i} \lambda\left(\mathbf{x}_i\right) \sum_{\mathbf{u}_k; k\neq i} P\left(\mathbf{x}_i\right| \mathbf{u}_1, ..., \mathbf{u}_n) \prod_{k\neq i} \pi_{x_i}\left(\mathbf{u}_k\right). \quad (16)$$

IV. Conclusions

In this paper, we addressed the issue of data sharing and message correction in an heterogenous IoT networks scenario, with a plethora of devices for sensing applications. A multi-hop IoT environment has been investigated through a Bayesian approach. Specifically, a BP algorithm for message correction, and information update has been presented in its infancy. The spatio-temporal behavior of the system has been described by a linear model, and through the Markov Random Field theory. Future works will address the assessment of the proposed algorithm in an extended simulated scenario.

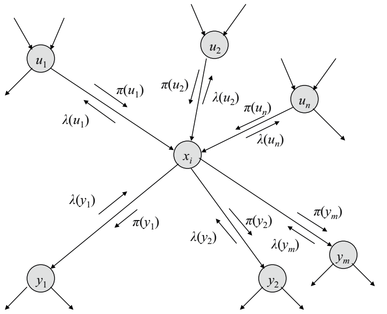

Figure 3: Architecture of the IoT Bayesian network as a graph, for the computation of the BP algorithm.

Acknowledgment

This work has been partially supported by DAHMS and LogOn projects.

References

[1] S.A. Alvi, G.A. Shah, and W. Mahmood. Energy efficient green routing protocol for internet of multimedia things. In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*, pages 1–6, April 2015.

[2] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Comput. Netw.*, 54(15):2787–2805, October 2010.

[3] F.H. Bijarbooneh, W. Du, E.C.-H. Ngai, X. Fu, and J. Liu. Cloud-assisted data fusion and sensor selection for internet-of-things. *Internet of Things Journal, IEEE*, PP(99):1–1, 2015.

[4] D. Bonino, M.T.D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. Udsen, J.A.C. Soto, and M. Spirito. Almanac: Internet of things for smart cities. In *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on*, pages 309–316, Aug 2015.

[5] R. Giuliano, F. Mazzenga, A. Neri, and A.M. Vegni. Security access protocols in iot networks with heterogenous non-ip terminals. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, pages 257–262, May 2014.

[6] Jiong Jin, J. Gubbi, Tie Luo, and M. Palaniswami. Network architecture and qos issues in the internet of things for a smart city. In *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, pages 956–961, Oct 2012.

[7] N. Kumar, N. Chilamkurti, and S. Misra. Bayesian coalition game for the internet of things: an ambient intelligence-based evaluation. *Communications Magazine, IEEE*, 53(1):48–55, January 2015.

[8] Bin Liu, Zhenfeng Xu, Junjie Chen, and Geng Yang. Toward reliable data analysis for internet of things by bayesian dynamic modeling and computation. In *Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on*, pages 1027–1031, July 2015.

[9] V. Miori and D. Russo. Anticipating health hazards through an ontology-based, iot domotic environment. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pages 745–750, July 2012.

[10] R. Tnjes, E.S. Reetz, K. Moessner, and P.M. Barnaghi. A test-driven approach for life cycle management of internet of things enabled services. In *Future Network Mobile Summit (FutureNetw), 2012*, pages 1–8, July 2012.