Une approche bayésienne pour une réduction efficace des données dans l'IdO

Cristanel Razafimandimby, Valeria Loscri, Anna Maria Vegni, Alessandro Neri

Une approche bayésienne pour une réduction efficace des données dans l'IdO

Cristanel Razafimandimby[1] et Valeria Loscrí[1] et Anna Maria Vegni[2] et Alessandro Neri[2]

[1] *Inria Lille - Nord Europe, Lille, France*
[2] *Department of Engineering, Roma Tre University, COMLAB Telecommunication Laboratory, Rome, Italy*

Actuellement, l'Internet des Objets (IdO) est en train de prendre une place importante dans notre vie quotidienne. Il a obtenu un grand succès dans plusieurs domaines d'application. Toutefois, malgré ce succès, l'un des plus grand défis à relever est l'énorme quantité de données générées par les dispositifs de capteur. Cela peut affecter la consommation d'énergie et peut également causer des problèmes de congestion du réseau. Pour résoudre ce problème, nous présentons dans cet article une Approche d'Inférence Bayésienne (BIA) permettant d'éviter la transmission des données fortement corrélées. BIA est basé sur une architecture hiérarchique composée de simple capteur, de passerelles intelligentes et de centres de données. L'Algorithme de Belief Propagation est utilisé pour reconstituer les données manquantes. BIA est évalué sur la base des données collectées sur les capteurs M3 déployés dans la plateforme FIT IoT-LAB. Sur les divers scénarios étudiés, les résultats montrent que notre approche réduit considérablement le nombre de données transmises et la consommation d'énergie tout en maintenant une qualité d'information acceptable.

Mots-clefs : IoT, Belief Propagation, Markov Random Fields, Cloud, Smart Device

1 Introduction

Despite of the large success of IoT, it raises yet many challenges and one of them is the management of massive amount of data generated by sensing devices. According to Cisco, the number of objects connected to the Internet is set to reach 50 billion by 2020. Harnessing cloud computing capacity is therefore needed, but unfortunately this is not enough. However, it was observed that, with the increase of sensor density, data generated by IoT devices tend to be highly redundant. Thus, uploading raw data to the cloud can become extremely inefficient due to the waste of memory and network overloading.

To address this issue, we proposed in [RLVN17a] and [RLVN17b] an efficient Bayesian Inference Approach (BIA) in the IoT context for indoor and outdoor environments. To this aim, two open data sets have been used. Although these data allowed of evaluating by simulation the efficiency of our proposal, the lack of access to the deployed sensors did not allow us to experiment our Bayesian approach directly on the sensors. In this paper, in order to validate the scalability of our BIA approach and filter the raw data directly in the sensing nodes, we run experiments on our FIT IoT-LAB platform [ABF+15] which is a very large scale infrastructure facility suitable for testing small wireless sensor devices and heterogeneous communicating objects over large scale.

2 Bayesian Inference Approach

Our main goal here is to avoid sending strongly correlated data, while keeping an acceptable level of data content accuracy. For this aim, BIA is based on Pearl's Belief Propagation algorithm that will be described below.

As a starting point before any inference procedure, the design of a graphical model should be provided. Graphical models are schematic representations of probability distributions. They consist of nodes connected by either directed or undirected edges. Each node represents a random variable, and the edges represent probabilistic relationships among variables.

Algorithm 1 One iteration of the BP algorithm

Forward pass
for *each i-th node* **do**
  for *each node* $u \in \Gamma(i), u \neq i$ **do**
    Send message $m_{ui}(y_i)$, i.e. message from the u-th to the i-th node
    Compute $m_{ui}(y_i)$ using formula (3)
  end
end
Backward pass
for *each* j*-th node* **do**
  for *each node* $u \in \Gamma(i), u \neq j$ **do**
    Send message $m_{uj}(y_j)$, i.e. message from the u-th to the j-th node
    Compute $m_{uj}(y_j)$ using formula (3)
  end
end

Models which are comprised of directed edges are known as *Bayesian networks*, whilst models that are composed of undirected edges are known as *Markov Random Fields* (MRF) [WKP13]. In this paper, we present an inference approach under the hypothesis of MRF, modeled by means of Factor Graphs. It follows that our goal is to estimate the state X of the sensed environment starting from the sets of data collected by each sensor node. Based on the remarkable Hammersley-Clifford theorem, the joint distribution $P_X(x)$ of an MRF model is given by the product of all the potential functions *i.e.*,

$$P_X(x) = \frac{1}{Z}\prod_i \theta_i(x_i) \prod_{(i,j)\in E} \psi_{ij}(x_i, x_j), \tag{1}$$

where Z is the normalization factor, x_i represents the random variable x on the node i, $\theta_i(x_i)$ is the evidence function, E is the set of edges encoding the statistical dependencies between two nodes i and j, and $\psi_{ij}(\cdot)$ represents the potential function. Note that the graphical model parameters (*i.e.*, θ_i and ψ_{ij}) can be estimated from the observed data by using a learning algorithm [†]. For simplicity, in this paper, we consider widely used pairwise MRF, *i.e.*, MRF with the maximum clique [‡] of two nodes.

For notation convenience, let us assume that X and Y are two distinct multivariate random variables with assignments $x_j \setminus j \in \{1,..,p\}$ and $y_i \setminus i \in \{1,..,n\}$. The nodes representing Y are called hidden nodes and representing X are the observed ones. So, given the i-th device in our network, x_j will be the observation of the value we intend to share (*e.g.*, pressure) and y_i will be associated to the value we want to infer, (*e.g.*, temperature)

Once the model was learned, our main goal is to compute the marginal distribution of hidden nodes (i.e, the inference). In Formula (2), for example, we consider a model composed of n variables and we want to calculate the marginal probability of the last variable i.e x_n. To this end, it is necessary to sum over all possible states of the $n-1$ variables in the model, i.e. :

$$p(y_n|x) = \sum_{y_1}\sum_{y_2}\cdots\sum_{y_{n-1}} p(y_1, y_2, y_3, ..., y_n|x). \tag{2}$$

Obviously, using (2) [§], the complexity of a complete enumeration of all possible assignments to the whole graph is $O(|\mathcal{Y}|^{n-1})$, which is intractable for most choices of n. Therefore, we need a faster algorithm like Belief Propagation (BP) [¶] [YFW03] for computing the marginal probability. BP is a well known algorithm

†. In this paper, the model structure was learned offline. Then, we put the learned model on our devices for all inference processes.
‡. A clique is defined as a fully connected subset of nodes in the graph.
§. Sums are used here to easily illustrate the algorithm complexity but they are changed by integral calculations for continuous variables
¶. Only take linear time.

for performing inference on graphical models. Let $p(y_i)$ represents the marginal distribution of i-th node, and BP allows the computation of $p(y_i)$ at each node i by means of a message passing algorithm (forward and backward pass). The message from the j-th to the i-th node related to the local information y_i is defined as :

$$m_{ji}(y_i) \propto \int \psi_{ji}(y_j, y_i)\theta_j(y_j) \prod_{u\in\Gamma(j),u\neq i} m_{uj}(y_j)dy_j, \tag{3}$$

where $\Gamma(j)$ denotes the neighbors of node j and the incoming messages from previous iteration are represented by m_{uj}. Notice that (3) will be performed between all nodes in the model until the convergence or if a maximum number of iterations I_{max} will be reached. Algorithm 1 illustrates an iteration of BP. The prediction *i.e.*, the belief at the i-th node, is computed through all the incoming messages from the neighboring nodes and the local belief, *i.e.* :

$$\hat{y}_i = belief(y_i) = k \cdot \theta_i(y_i) \prod_{u\in\Gamma(i)} m_{ui}(y_i), \tag{4}$$

where k is a normalization constant.

3 Evaluation & discussion of the results

In this paper we propose a bayesian approach in a cloud-based architecture consisting of M3 nodes, smart gateways and data centers. Our IoT network model may include multiple subnets associated with different applications. In our case, each subnet corresponds to one site of the FIT IoT-Lab testbed and is composed of IoT devices connected to each others for data sharing, and a smart gateway that relays the data flows to the cloud. The cloud in turn is responsible of data storage and all the cloud-based services.

This section provides the experimental results of our BIA approach using the FIT IoT-LAB testbed. Ten nodes from Lille site and ten nodes from Grenoble site were used for the data collection. Nodes were of the M3 type, which are equipped with an 32-bit ARM Cortex-M3 MCU, 64 kB of RAM, 256 kB of ROM, an IEEE 802.15.4 2.4 GHz radio transceiver and four different sensors (light, accelerometer, gyroscope, pressure & temperature). Data collected from all the M3 nodes has been used to build the BIA model. Each data collection has been performed every 15 minutes and the collected data consists of 2.5 days of readings.

During the 2.5 days of reading, we noticed that there is a good correlation between pressure and temperature data (it is about -0.7720841). Hence, we can infer the temperature data from pressure data and vice versa. In this paper, we decided to infer temperature from pressure. The temperature is in degrees Celsius, whilst the pressure is in mbar.

We assess our approach w.r.t. (*i*) the total number of transmitted data, (*ii*) average value of the estimation error (ER), (*iii*) average value of the distortion level as a Mean squared Error (MSE), and (*iv*) the energy consumption (EC).

In our energy consumption evaluations, we assume that the power cost for sending each temperature and pressure value is 14 mW.

Furthermore, all of our assessments are based on three different scenarios (*i.e.*, s_1, s_2, and s_3). In scenario s_1, the M3 node sends to the gateway all the temperature and pressure data it receives. This means that the gateway does not perform any inference (*i.e.*, no inference). In the second scenario s_2, the M3 nodes sends only the pressure data to the gateway, and the gateway in turn infers the corresponding temperature data by using the BP algorithm. Finally, in the scenario s_3, we consider that the M3 nodes are "smart" devices, meaning that before sending their data to the gateway, they first compute the probability $\Pr(e|T,P)$ of making an inference error e on the gateway given the temperature data T, and the pressure data P. If there is a strong probability that the error magnitude *i.e.*, $|e|$, exceeds a predefined threshold *i.e.*, $|e|_{Max}$, the M3 node sends both pressure and temperature data to the gateway, else the M3 node sends only the pressure data, and the temperature value will be inferred in the gateway using the BP algorithm. This can be expressed mathematically as the inference error probability higher than a maximum allowed value $|e|_{Max}$, and conditioned to the temperature and pressure measurements *i.e.*, T and h, is lower or at least equal to a given threshold P_e^{Max}, that is :

$$\Pr\{|e| > |e|_{Max}|T,P\} \leq P_e^{Max}, \tag{5}$$

Scenario	*#Transmitted data*	*EC* (kJ)	*MSE*	*ER*
s1	10440	1716.64	-	-
s2	5220	858.32	1.43	0.55
s3	5829	958.46	0.43	0.43

TABLE 1: Results obtained during the two days and half of readings.

It should be noted that this computation requires the knowledge of the a priori probability of inference error *i.e.*, $\Pr(e)$. Also, the value of the threshold $|e|_{Max}$ strictly depends on the application context. In our case, we set this value equal to 1. Due to the lack of space, in this article, we omit the results which can show us how the choice of $|e|_{Max}$ may influence the obtained results. A similar consideration can be applied to the probability threshold P_e^{Max}, which has been set to 0.5.

TABLE 1 illustrates the obtained results during 2.5 days of readings, for different simulated scenarios. We can notice that our Bayesian inference approach drastically reduces the number of transmitted data and the energy consumption, while maintaining an acceptable level of prediction accuracy and information quality. We can notice also that we decrease considerably the estimation error by using the scenario s_3. Indeed, the M3 nodes are smarter in this case *i.e.*, by computing the a posteriori probability of the inference error, the M3 nodes will be able to estimate the right moment and the data type to send in the gateway. However, this increases the number of transmitted data (and hence the energy consumption), as compared to scenario s_2. This is due to the fact that in s_2, the M3 node send only the pressure data without worrying of the risk of inference error in the gateway. It is important to say that we have a good quality of information in the scenario s_3 despite the fact that we have an inference error of 43%. This is due to the fact that we allow only a maximum error of one unit (i.e $|e|_{Max} = 1$).

4 Conclusions

In this paper, we have presented an inference-based approach for avoiding transmitting high correlated data in an heterogeneous IoT network. A good correlation between data was taken into account for this study. Indeed, It is important to have a good data correlation to avoid a very high error rate. Through experimentation on FIT IoT-LAB platform using the M3 nodes, we have showed that our Bayesian inference approach is scalable and reduces considerably the number of transmitted data and the energy consumption, while keeping an acceptable level of estimation error and information quality. We have also shown that the use of smart node decreases the inference error.

Références

[ABF+15] Cedric Adjih, Emmanuel Baccelli, Eric Fleury, Gaetan Harter, Nathalie Mitton, Thomas Noel, Roger Pissard-Gibollet, Frederic Saint-Marcel, Guillaume Schreiner, Julien Vandaele, et al. Fit iot-lab : A large scale open experimental iot testbed. In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pages 459–464. IEEE, 2015.

[RLVN17a] Cristanel Razafimandimby, Valeria Loscri, Anna Maria Vegni, and Alessandro Neri. A bayesian and smart gateway based communication for noisy IoT scenario. In *International Conference on Computing, Networking and Communications*, 2017.

[RLVN17b] Cristanel Razafimandimby, Valeria Loscri, Anna Maria Vegni, and Alessandro Neri. Efficient Bayesian Communication Approach For Smart Agriculture Applications. In *2017 IEEE 86th Vehicular Technology Conference*, Toronto, Canada, September 2017.

[WKP13] Chaohui Wang, Nikos Komodakis, and Nikos Paragios. Markov random field modeling, inference & learning in computer vision & image understanding : A survey. *Computer Vision and Image Understanding*, 117(11) :1610–1627, 2013.

[YFW03] Jonathan S Yedidia, William T Freeman, and Yair Weiss. Understanding belief propagation and its generalizations. *Exploring artificial intelligence in the new millennium*, 8 :236–239, 2003.