Improving Quality of IoTs Based on Wireless Sensor Network Security: A Deep Belief Network with Dempster-Shafer Theory

Xu Huang

**Abstract**

It is well known that Internet of Things (IOTs) becomes part of our daily life, one of the IOTs definitions states that it has certainly an umbrella term for a very broad range of applications, technologies, and use the cases as they are enabled uniquely addressed via an Internet IP address and recognize, capture, transmit, and receive data, depending on their purpose. No doubt about that wireless sensor networks (WSNs) are one of major useful tools for those applications, with their security that becomes a fundamental concern. A new adaptive WSN security based on a deep belief network (DBN) with the Dempster–Shafer theory (DST) has been discussed and presented in this presentation. There are two types, in terms of applications, depending on our proposes and conditions: 1. If we have some information about the contaminated pattern of the observed network from the previous experience, this method can use the reference patterns as the evidence regarding the class membership of each input pattern under the considerations. Then, the evidence is represented by the basic belief assignments by the Dempster’s rule of combination. Hence, we can identify the abnormal nodes and fix related problems; 2. If we do not have the contaminated pattern, we may take each duration of a period time as a picture shot that is based on the outcomes of DST observing. With appropriate window size and interval time, depending on the requirements, the reasonable hidden layers can be built up for a DBN. The final test data can be obtained from the outcomes of the DBN. This procedure can be implemented in a multilayer DBN network with specific architecture such as consisting of one input layer, a few hidden layers and one output layer. The weight vector, the receptive field and the class membership of each prototype for type 1 can be determined by minimizing the mean squared differences or empirical data between the classifier outputs and target values. For the type 2, a threshold, based on the required conditions, will be used for a decision whether the observed node is at the normal status or not. After training, the classifier computes for each input vector and provides a description of the uncertainty pertaining to the class of the current pattern, given the available evidence for the type 1 and the obtained pattern for the observed network for type 2. The obtained information may be used to implement various decision rules allowing for ambiguous pattern rejection and novelty detection. The outputs of several classifiers may also be combined in a sensor fusion context, yielding decision procedures which are very robust to sensor failures or changes in the system environment. The advantage of this proposed method is not just its performance in real-time effectively for type 1 also it is effective for type 2 as it does not need the knowledge about the normal or malicious node in advance with very high average accuracy. It also can be used as one of maintaining tools for the regulations of the deployed WSNs. All those advantages, together with AI technologies, will improve the quality service for IoTs.