Life-Environmental Sensor Data Aggregation Based on Neural Network

Sang-Hyun Lee 1, Sang-Joon Lee 2, Kyung-II Moon 1

1 Dept. of Computer Engineering, Honam University, Korea,
2 School of Business Administration, Chonnam National University, Korea
{leesang64, kimoon}@honam.ac.kr, s-lee@chonnam.ac.kr

Abstract. The difficulty in monitoring sensor networks is not only due to their inherently distributed nature but also the need for mechanisms to address their harsh operating conditions such as unreliable communications, faulty nodes, and extremely constrained resources. Researchers have proposed different monitoring models to overcome these difficulties with the ultimate goal of making monitoring easy while making full use of available data. Life-environmental monitoring is mostly composed of air quality, water quality and eco-tourism sensing data. In case of separate communication it gives high energy loss because there is requirement of some mechanism that can select multiple communications in single communication. This kind of merging is called data aggregation. Aggregation process is itself efficient process that uses the improved greedy approach. In this study, we present a secure and authentication approach for the life-environmental data aggregation. The user authentication is performed using secure hash algorithm. It will reflect participating node over the communication final stage is proposed work of neural network for checking bad packet communication over the network. The derived result showed the presented work which is more reliable and efficient than existing approach.

Keywords: Data aggregation, Hashing algorithm, Life-environmental industry, Neural network, Wireless sensor network

1 Introduction

Life-environmental sensor networks are collection of sensor nodes which cooperatively send sensed data such as air quality, water quality and eco-tourism to base station. The life-environmental sensor networks represent a significant improvement over traditional life-environmental sensors, which are deployed in the following two ways: Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required. Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused. In this paper we present the case where artificial neural network is securely performed over the wireless sensor network. To do this, we revised Holenderski et
al.’s decomposition model to support secure computing [3]. Our results show that such a combined system can indeed be built, and that its performance is on a par with traditional data aggregation and authentication algorithm.

2 Life-Environmental Wireless Sensor Network

A life-environmental wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as air quality, water quality and eco-tourism quality and to cooperatively pass their data through the network to a main location. Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to life-environmental industry (see Fig. 1). Sensor data aggregation techniques explore how the data is to be routed in the network as well as the processing method that are applied on the packets received by a sensor node. They have a great impact on the energy consumption of nodes and thus on network efficiency by reducing number of transmission or length of packet. Elena Fosolo et al in [2] defines the in-network aggregation process as follows: “In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption, thereby increasing network lifetime.”

3 Secure Hashing and Neural Network Design

Assume that a neural network consists of $L$ fully connected layers where there are $N$ neurons in each layer. The problem is to distribute this network evenly over $P$ sensor nodes by assigning to each node a partition of weights set and the corresponding neurons. The cost function to minimize is the maximum communication cost and the memory overhead per sensor node. A neural network of $L$ fully connected layers with $N$ neurons in each layer can be divided into as follows.

Each sensor node $p$ corresponds to $l$ layers ($l \leq L$) where in each layer $p$ is corresponding to $u$ upper neurons, $d$ lower neurons and all the related weights among
and $d$ neurons. If the decomposition is performed with the parameter $l = 1$, we call it horizontal decomposition whereas if the decomposition has $l > 1$ and $u = 1$, we call it vertical decomposition. Since there are $N^2$ weights in each layer, totally $L \times N^2$ weights exist in the network. If we evenly distribute them to $P$ sensor nodes, then the maximum number of weights assigned to each node is $E_{\text{max}} = \left\lfloor \frac{L N^2}{P} \right\rfloor$. If each node $p$ has $l$ layers, $u$ upper neurons, and $d$ lower neurons, $l u d \leq E_{\text{max}}$, which means that given $P, N, L, d, l, u$ is calculated as:

$$u \leq \left\lfloor E_{\text{max}} \left( 1 \times 1 \right) \right\rfloor = \left\lfloor L \times N^2 \div \left( 1 \times d \times l \right) \right\rfloor$$  \hspace{1cm} (1)$$

If $l > 1$ some of the partial summation between lower neurons and upper neurons can be calculated by the node $p$ itself, the receiving communication cost for $p$ is $R_x = (l-1) \times (N-u)+N$ if $p$ is not corresponding to the last layer. If the node $p$ is corresponding to the last layer, $R_x = (l-1) \times (N-u), l \geq 1$. As for transformation of data, since the sensor node $p$ can broadcast the message to all the nodes, the transmission cost for $p$ is $T_x = l u$, if $p$ does not have the first layer. If $p$ has the first layer, $T_x = (l-1) u$. The total communication cost for $p$ is $R_x + T_x$.

We can use pairwise key establishment for communication confidentiality and integrity. If we use the secure routing protocol, we can defend against the routing attack. To defend against node capturing and incorrect calculation attack, we should apply the voting protocol. To do this, we assume that for each weight in the original network, we build 3 identical weights for the new network, the layers and neurons are identical to those of the original network.

### 4 Result

We begin the task with modeling a wireless sensor network, comprising of ten nodes initially. The scenario containing the sensor nodes along with a base station and router is developed. First, figure 2 denotes the simulation result for different network size by using Matlab, and figure 3 represents the nodes labeled and placed in the wireless sensor networks.

![Fig. 2. Simulation for different network size](image)

The various nodes are labeled as node 1 till node 10. The position of node 1 is fixed and rests of the nodes are placed in the network using the “flood” function available with Matlab. The node is red color represent the sink node of the network.
In this study, we suggested a combined system in order to resolve some of the long standing issues in wireless sensor network technology. The similarities between wireless sensor networks and neural networks suggest that combining these technologies is reasonable. We considered the case where artificial neural network is securely performed over the wireless sensor network. To do this, we revised Holenderski et al.’s decomposition model to support secure computing. Our results show that such a combined system can indeed be built, and that its performance is on a par with traditional data aggregation and authentication algorithm. Due to the unique property of sensor networks, public keys do not need to be authenticated in the same way as it is done in the internet environment; instead, public keys can be authenticated using SHA-1 algorithm, which are much more efficient than signature verification on certificates can increase efficiency of data transfer with reduction of data losses and delays.

References