Master's Thesis

Title

Configuring robust virtual wireless sensor networks for Internet of Things inspired by brain functional networks

Supervisor

Professor Masayuki Murata

Author

Shinya Toyonaga

February 10th, 2014

Department of Information Networking

Graduate School of Information Science and Technology

Osaka University

Master's Thesis

Configuring robust virtual wireless sensor networks for Internet of Things inspired by brain functional networks

Shinya Toyonaga

Abstract

In future, wireless sensor networks (WSN) are expected to be integrated into the Internet of things and to play an important role not only for data collection but for communication infrastructure. In that situation, multi-vendor and heterogeneous WSNs should be federated to make a large scale WSN. As one way to realize the integration of WSNs, virtualization technology in WSN is of great significance. Although many techniques for virtualization of sensor networks have been studied, environmental changes, such as diverse traffic patterns or addition or removal of virtual nodes, are not considered. Since future WSNs will face with a wide variety of requirements, it is critically important to construct a virtual sensor network (VSN) which provides short delay time of packet communication and a guarantee of network connectivity in a network of arbitrary scale. In this thesis, we propose a method for constructing a VSN inspired by brain functional networks known for robustness, high efficiency and adaptive evolvability. To earn the advantages shown above, we particularly pay our attention to modularity and small world property which brain functional networks have and we apply them to virtual topology construction. Through simulation experiments, compared to a VSN topology constructed by an existing clustering technique for achieving small world properties, our VSN topology is highly robust in terms of connectivity and average path length.

Keywords

Wireless sensor networks

Virtual sensor networks

Brain functional networks

Contents

List of Figures

List of Tables

1 Introduction

Wireless sensor networks (WSN) has a great importance because of the broad range of its commercial applications such as smart home, health care and industrial automation [1]. Furthermore, WSN is recently attracting a great deal of attention as a required technology to realize the Internet of Things. WSN are expected to be integrated into the Internet of Things and to play an important role not only for a specific application such as a data collection but for communication infrastructure shared by multiple applications [2, 3]. In that situation, sensor nodes which have various functions and properties are deployed in the same area by multiple vendors. Virtualization of WSN is one of key solutions for integrating such heterogeneous WSNs into one large WSN and sharing physical sensor substrate. Virtualization of WSN can be defined as a separation of a function for WSN into two parts, physical sensor infrastructure and applications working on aggregated resources. The expected advantages of virtualization of WSN are providing flexibility, cost efficiency, diversity, security and manageability [1, 4–6].

Although many researchers have worked on virtualization of WSN, objectives and assumptions of its use are different and technical challenges are left to be solved, for example, constructing an arbitrary virtual sensor network (VSN) with flexibility, reusability, resource efficiency, security, privacy, manageability, scalability, programmability and allowability of heterogeneity [1, 7]. Because environmental changes, such as diverse traffic patterns or addition or removal of virtual nodes, are anticipated in virtualization of sensor networks, to construct a VSN with certain communication efficiency and connectivity is particularly important. Therefore, we propose an algorithm for constructing a VSN topology with high communication efficiency and robustness by introducing complex network features. In this thesis, we define two kinds of robustness. One is robustness of connectivity and the other is robustness of average path length.

Many researchers introduce small world properties, which is one class of complex network, to sensor networks and show that small number of long-distance links added to a sensor network improve communication efficiency drastically [8, 9]. For that reason, we can construct a VSN topology with high communication efficiency by introducing structural properties of complex network to sensor networks. Although WSN with small world properties has high communication efficiency, it is said that a topology with a property of some classes of complex networks is vulnerable against targeted attack on nodes with high degree or on long-distance links [10]. To address this problem, we focus on the brain functional network because it shows highly robust features and evolves adaptively depending on communication demands or environmental changes, while it has multiple features of complex network.

The brain functional network has small world properties and modular community structure [11]. Small world properties are described by high efficiency and high clustering. These features lead to efficient information dissemination globally and locally. Moreover, highly clustering structure gives many detour routes from one node to another. This leads to robustness in terms of connectivity. The brain functional network is organized by a large number of modules, each of which processes information, such as cognitive, emotional, perceptual or motor processing information. A network with modular community structure can adapt to changes of demands by configuring a small number of links between modules. Therefore, the brain functional network can negotiate trade-offs between wiring cost and communication efficiency rapidly, resulting in its evolvability to changing cognitive demands. Therefore, we propose an algorithm to construct a VSN topology with small world properties and modular community structure for high communication efficiency, robustness and evolvability.

The rest of this thesis is organized as follows. Section 2 shows the topological properties of the brain functional network and advantages by applying them to WSN. We propose a model for constructing a VSN topology inspired by brain functional network in Section 3 and evaluate our proposal in Section 4. In Section 5, we conclude this thesis and describe future work.

2 Brain functional networks

In this section, we explain topological properties of brain functional networks and describe expected advantages applying these properties to wireless sensor networks. A brain functional network has small world properties and a modular community structure. Small world topology has high topological efficiency in local and global areas and robustness. Modular community structure of a brain functional network has adaptivity and evolvability [11–16].

2.1 Small world property

Small world properties are characterized by a short average path length and a high clustering coefficient. In this thesis, we regard path length as a hop count on the shortest path between a pair of two nodes. Path length in whole network is quantified by average path length (APL), defined as

$$APL = \frac{1}{N(N-1)} \sum_{i,j} sd(i,j), \tag{1}$$

where N is the number of node and sd is the minimum hop count between node i and node j. A short APL means that global communication efficiency is high. Clustering structure of a network is quantified by average clustering coefficient (CC) defined as

$$CC = \frac{1}{N} \sum_{i} \frac{2e_i}{k_i(k_i-1)}, \tag{2}$$

where k_i is a degree of node i and e_i is the number of links that exist between neighbor nodes of node i. A topology with high CC has many topological motifs of a triangle, which means that the nearest neighbors of a given node have a high probability to be connected with each other. High CC means that local communication efficiency is high due to its densely connected structure in a local region.

2.1.1 Long-distance connections

One of factors contributing to global communication efficiency in a brain functional network is myelinated long-distance links [11]. An electric conductivity of a myelinated link is high. When long-distance areas are connected by these links, communication delay between them gets short and these links enable a close cooperation between different functional areas.

2.1.2 Highly clustering structure

A brain functional network is a spatial network. This means that connecting functional areas is strongly influenced by distance between functional areas due to wiring and running metabolic costs [11]. Therefore, short-length links tend to be constructed and maintained, resulting in a high clustering coefficient. Because local areas are connected densely, segregated processing and synchronization can be done rapidly.

2.2 Modular community structure

A brain functional network has a modular community structure in which nodes within the same module are densely connected by short-distance links but sparsely connected to a node in other modules by long-distance links. Moreover, a brain functional network demonstrates a property of hierarchical modularity. Each module in a brain functional network is composed of a set of sub-modules and each sub-module is composed of a set of sub-sub-modules [11, 16]. This modular community structure allows a brain functional network to balance trade-off between efficiency and metabolic costs, in other words communication delay and connection distance, can be rapidly negotiated by functional systems only by configuring long-distance inter module links [11]. When there is greater demand for cognitive processing, networks adopt a more efficient structure by constructing costly long-distance links, and when cognitive demand is lower, brain networks get more clustered and less costly. Moreover, because connections between modules are sparse, it seems that brain network can be evolved adaptively under environmental changes. In modular systems, each module can configure its structure adaptively, which has little influence on outside of the module. Therefore, modular structure gives whole system evolvability by segregated configuration of each module.

A wireless sensor network is a spatial network, because it is strongly constrained by physical distance. For most of wireless sensor networks densely deployed, a topology of such networks naturally has a regular lattice property and a high clustering coefficient. Therefore, a wireless sensor network favors segregated processing. Moreover, there are many detour routes from one node to another due to topological motifs of a triangle. This leads to high robustness of connectivity against failure of nodes or links. When we introduce a hierarchical modular structure to wireless sensor networks, it is expected that its topology can evolve adaptively to changes of resource or traffic demands. Existence of a long-distance connection which connects two physically distant sensor nodes leads to reduction of communication delay of a whole network because of shortened average path length.

When a physical long-distance link, such as directional beam or long range omnidirectional transmission, can be assigned to a virtual link, improvement of communication efficiency in virtual networks directly means that in physical networks. However, because communication capabilities of sensor nodes are constrained, endpoints of a virtual link may not be able to communicate with each other directly. One of the solutions is that a virtual link is assigned to a path containing available physical long-distance links.

3 A method for configuring virtual wireless sensor networks using properties of brain functional networks

3.1 Overview

A topology having high modularity enables efficient segregated information processing and local synchronization and a topology having small world properties enables efficient global communication. Therefore, we propose a model which constructs a VSN topology having high modularity and small world properties.

Considering a geographical constraint, we assume that a minimum unit of a module is a group of sensor nodes divided by Newman algorithm [17]. We simply call this minimum unit of a module as a unit module. We describe Newman algorithm in detail in Section 3.2. We construct a VSN topology by integrating these unit modules hierarchically. At the same time, it has small world properties in any scale of layer. By repeating integration of sub-modules with a new module having small world properties, a VSN topology constructed finally has a high modularity and small world properties.

An example of hierarchical VSN is shown in Figure 1. The first layer VSN is a network in a unit module which corresponds to a group of sensor nodes divided by Newman algorithm. The second layer VSN is a network constructed by connecting unit modules. The third layer VSN is a network constructed by connecting sensor networks which is deployed for different purposes.

At first, we propose an algorithm which constructs a VSN topology in the first layer, that is to say this constructs a small world network in a unit module by adding virtual long-distance links. In Section 3.3, we explain the method for constructing a VSN topology in the first layer in detail. Then, in Section 3.4, we show the method for constructing a VSN topology in an Nth layer by connecting modules in an $(N-1)$th layer.

3.2 Modular division for a physical sensor network

Newman algorithm is a heuristic algorithm which divides a network in several modules for the maximization of the modularity. The definition of the modularity, denoted by Q, is as following.

$$Q = \sum_i (e_{ii} - a_i^2), \tag{3}$$

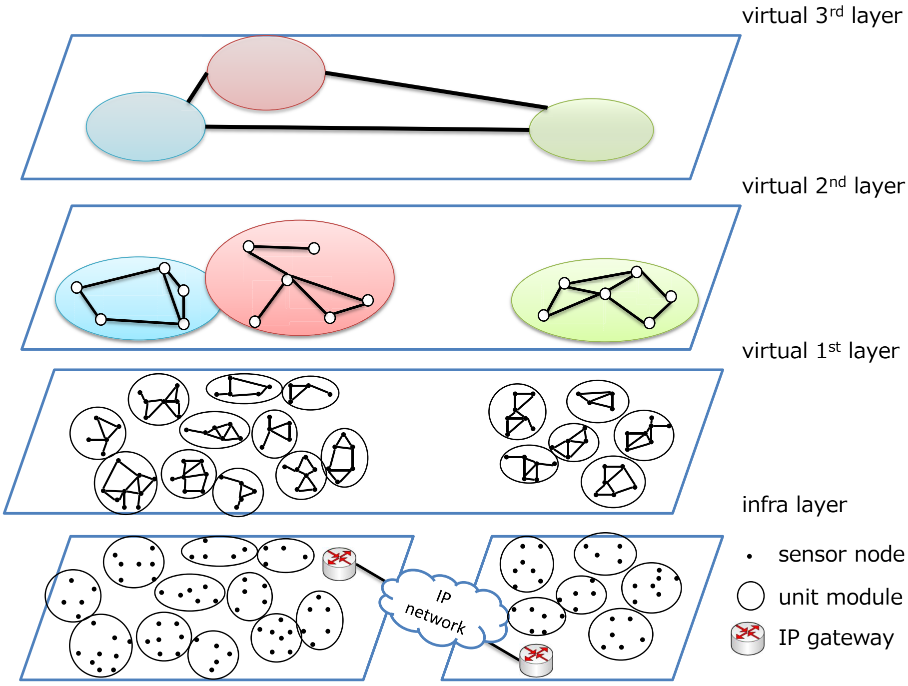

Figure 1: Example of hierarchical VSN topology

where i is a group ID and e_{ii} is a ratio of edges whose endpoints belong to the same group i. a_i is a probability that at least one of endpoints belongs to the group i. Then, a_i^2 is an expected ratio that edges whose endpoints belong to the same group i to all edges.

In Newman algorithm, modules are divided into two modules recursively as long as a condition for halt is not satisfied. At first, we explain the method of the first division in which a whole network is regarded as one group and divided into two groups. For a particular division of the network into two groups let $s_i = 1$ if a node i belongs to group 1 and $s_i = -1$ if it belongs to group 2. And let A is an adjacency matrix, $A_{ij} = 1$ if node i and node j is connected and $A_{ij} = 0$ if node i and j is unconnected. The expected number of links between node i and node j can be described by $\frac{k_i k_j}{2m}$, where k_i is a degree of node i and m is a total number of links embedded in a whole network, that is, $m = \frac{1}{2}\sum_i k_i$. Under these assumptions, the modularity can be calculated by Equation (4).

$$\begin{aligned} Q &= \frac{1}{2m}\sum_{i,j}(A_{ij}-\frac{k_ik_j}{2m})\frac{(s_is_j+1)}{2} \\ &= \frac{1}{4m}\sum_{i,j}(A_{ij}-\frac{k_ik_j}{2m})s_is_j, \end{aligned} \tag{4}$$

where $\frac{(s_is_j+1)}{2} = 1$ if node i and node j belong to the same group and $\frac{(s_is_j+1)}{2} = 0$ if node i and node j belong to different groups. The second equality follows from the observation that $2m = \sum_i k_i = \sum_{i,j} A_{ij}$.

Equation (4) can conveniently be written in matrix form as shown in Equation (5).

$$Q = \frac{1}{4m}s^{\mathrm{T}}Bs, \tag{5}$$

where s is the column vector whose elements are the s_i. B is a symmetric matrix whose elements are $B_{ij} = A_{ij} - \frac{k_ik_j}{2m}$. The aim of Newman algorithm is maximization of the modularity Q by choosing a value of the vector s which means choosing an appropriate division of the network.

By writing s as a linear combination of the normalized eigenvectors u_x of B, that is $s = \sum_x a_x u_x$, Equation (5) can be described as Equation (6).

$$\begin{aligned} Q &= \frac{1}{4m}\sum_x a_x u_x^{\mathrm{T}} B \sum_y a_y u_y \\ &= \frac{1}{4m}\sum_x (u_x^{\mathrm{T}} s)^2 \beta_x, \end{aligned} \tag{6}$$

where β_x is an eigenvalue of the eigenvector u_x. Newman assumes that the eigenvalues are labeled in decreasing order, $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$. From Equation (6), to decide the most appropriate s equals to decide the best weight of each eigenvalue. Therefore, the most simple method to maximize Q is to place all of the weight in the term involving the largest eigenvalue β_1 by setting s to αu_1. Because there is a constraint that the elements of s must be ± 1, Newman maximizes $u_x^{\mathrm{T}} s$ by setting $s_i = 1$ if the corresponding element of u_1 is positive and $s_i = -1$ otherwise. Then, node i belongs to group 1 if $s_i = 1$ and it belongs to group 2 if $s_i = -1$.

Decision of module can be realized by applying the same algorithm to each divided group recursively. However, if this dividing procedure is applied to subgraph after simply deleting the links between the two parts, the value of modularity in Equation (4) will change due to the change of degrees. Instead, Newman uses the alternative modularity ΔQ to calculate the correct modularity and to further divide a group g of size n_g in two groups. The definition of ΔQ is

$$\begin{aligned}
\Delta Q &= \frac{1}{2m}(\frac{1}{2}\sum_{i,j\in g} B_{ij}(s_i s_j + 1) - \sum_{i,j\in g} B_{ij}) \\
&= \frac{1}{4m}(\sum_{i,j\in g} B_{ij} s_i s_j - \sum_{i,j\in g} B_{ij}) \\
&= \frac{1}{4m}\sum_{i,j\in g}(B_{ij} - \delta_{ij}\sum_{k\in g} B_{ik}) s_i s_j \\
&= \frac{1}{4m} s^{\mathrm{T}} B^{(g)} s \qquad (7)
\end{aligned}$$

where δ_{ij} is a Kronecker δ-symbol and $B^{(g)}$ is the $n_g \times n_g$ matrix with elements indexed by the labels i, j of nodes within group g. An element of $B^{(g)}$ is

$$B^{(g)}_{ij} = B_{ij} - \delta_{ij}\sum_{k\in g} B_{ik}. \qquad (8)$$

Because Equation (7) has the same form as Equation (5), the dividing algorithm can be applied.

By using Newman algorithm, modular structure can be detected and the modularity Q is maximized. However, according to its heuristic manner, in some cases there is a module composed of only one node, which is unsuitable for sensor networks. Therefore, we coordinate Newman algorithm to suit for sensor networks. After divide a sensor network into modules by Newman algorithm, node i which belongs to module g checks modules its neighbor nodes belong to. If there is no neighbor node belonging to module g, then node i finds that it is isolated and moves to one of the smallest modules its neighbor nodes belong to.

3.3 Configuring a 1st layer virtual sensor network by connecting sensor nodes within the same module

In this section, we explain how to construct a small world network in an intra-module which is detected by using the algorithm described in Section 3.2. To create a network with small world properties, we add a small number of long-distance links, called shortcuts, to initial regular lattice network.

We assume that initial topology of an intra-network is the same as the topology of a physical network, that is to say two nodes which belong to the same module and are deployed in communication range of each other are also connected logically. Then, we propose a model based on [18, 19], in which virtual shortcuts are added in consideration of both constraint of physical distance and the preferential attachment rule.

In [18], the authors have proposed an enhancing a robustness of scale free network model (ESF) in which new links are added to Barabasi Albert model (BA) topology [20] in consideration of degrees. At first, a scale free network is constructed by BA model. The number of added links is $C|E_0|$, where $|E_0|$ is the number of links embedded in the constructed scale free network and C is a constant value of 0 to 1. Authors define the probability of adding a new link between unconnected node i and node j as

$$p_{ESF}(i,j) = \frac{k_i^\alpha \cdot k_j^\alpha}{\sum_{e_{a,b} \in \bar{E}} k_a^\alpha \cdot k_b^\alpha}, \tag{9}$$

where k_i is a degree of node i, $e_{a,b}$ is a pair of nodes and $\bar{E}$ is the set of links in the complementary graph. α is a parameter, called enforcing parameter. When $\alpha > 0$, a new link is added preferentially to a node with higher degree and the constructed topology is robust on connectivity against random failure but vulnerable against targeted attack. When $\alpha < 0$, a new link is added preferentially to a node with lower degree and the constructed topology have an allowable robustness of connectivity against both of random failure and targeted attack.

Airport network model (Airport model) is proposed in [19]. Airport model can construct a spatial network topology with scale free property by considering physical distance constraints. Airport model is based on preferential attachment algorithm and either of two processes described below which is determined with probability Π at each time step.

Probability Π: adding a new link between two nodes already in the network

Probability ($1 - \Pi$): adding a new node and links between it and m nodes already in the network

The probability of adding a link between node i and node j which are already in the network is shown in Equation (10) and the probability of adding a link between a new node and node j is shown in Equation (11).

$$p_{Airport}(i,j) \propto \frac{k_i k_j}{F(d_{i,j})}. \tag{10}$$

$$p_{Airport}(j) \propto \frac{k_j}{F(d_{i,j})}. \tag{11}$$

k_i is a degree of node i, $d_{i,j}$ is a physical distance between node i and node j and F is a monotonously increasing function. Authors investigate two different functional forms for the function F, which are $F1(d) = d^r$ and $F2(d) = \mathrm{e}^{d/d_x}$ where r and d_x are a constant parameter describing a cutoff of distance constraint. In this thesis, we use $F2(d)$.

By merging two models explained above, we propose a preferential attachment model based on degree and physical distance constraint as

$$p_{\mathrm{intra}}(i,j) = \frac{\frac{G^{intra}(k_i,k_j)}{F2(h_{i,j})}}{\sum_{e_{a,b}\in\bar{E}} \frac{G^{intra}(k_a,k_b)}{F2(h_{a,b})}}, \tag{12}$$

where node i and node j belong to the same module M, $\bar{E}$ is the set of links in complementary graph of intra-module network and $h_{i,j}$ is the minimum hop count from node i to node j. The reason why we use hop count instead of physical distance is that the same method can be applied to constructing an upper layer VSN topology. The function G^{intra} is a strategy of selecting a new link preferentially according to degrees of endpoint nodes. We investigate a four different strategies for adding a new link in intra-module network and the name of each strategy $intra$ is labeled by "hh', "ll", "hl" and "r". When $intra = \mathrm{hh}$, a pair of two nodes with higher degree is selected preferentially for a new link, and when $intra = \mathrm{ll}$, a pair of two nodes with lower degree is selected for a new link. When $intra = \mathrm{hl}$, a node with higher degree and another with lower degree are selected preferentially and connected. When $intra = \mathrm{r}$, a pair of two nodes are selected randomly regardless of their degrees. Each definition of G^{intra} is as follows.

$$G^{\mathrm{hh}}(k_i,k_j) = k_i \cdot k_j. \tag{13}$$

$$G^{\mathrm{ll}}(k_i,k_j) = k_i^{-1} \cdot k_j^{-1}. \tag{14}$$

$$G^{\mathrm{hl}}(k_i,k_j) = \max(k_i,k_j) \cdot |k_i - k_j|. \tag{15}$$

$$G^{\mathrm{r}}(k_i,k_j) = 1. \tag{16}$$

The number of added virtual links is $\lceil C_{\mathrm{intra}}|E_0|\rceil$, where $|E_0|$ is the number of links embedded in the initial intra-module network and C_{intra} is a constant value of 0 to 1.

3.4 Configuring an Nth layer virtual sensor network by connecting $(N-1)$th layer virtual sensor networks

In this section, we explain the method to construct an Nth layer VSN topology. This problem can be divided into two small sub-problems as shown below.

1. In an Nth layer, regarding an $(N-1)$th layer VSN as one subnetwork, the first problem is how to select a pair of two subnetworks to be connected.

2. The second problem is how to select an endpoint sensor nodes at infra-layer based on inter-subnetwork links in Nth layer.

We explain how to solve the first problem in Section 3.4.1, and the second problem in Section 3.4.2.

3.4.1 Constructing an intra Nth layer virtual link

In this section, we propose a method to construct an Nth layer virtual link between $(N-1)$th layer subnetworks. We regard VSN in an $(N-1)$th layer as one subnetwork (Sub_i^{N-1}).

Proposed method to construct a VSN topology in intra Nth layer subnetwork is organized by two steps described below.

1. Constructing an initial virtual topology

2. Adding virtual shortcut links to initial virtual topology

In step 1, initial virtual topology is constructed based on physical connection. When a pair of nodes has physical link and they belong to different $(N-1)$th layer subnetworks, these $(N-1)$th layer subnetworks are connected by an Nth layer virtual link. Note that, there is a case that unconnected subgraphs exist because there is no physical link between them. In such a situation, the closest subnetworks are connected by an Nth layer virtual link to guarantee its connectivity.

In step 2, new Nth layer virtual links are added to the initial virtual topology constructed in step 1 similar to the proposed model in Section 3.3. Proposed model is

$$p_{\mathrm{intra}}^{N}(Sub_i^{N-1}, Sub_j^{N-1}) = \frac{\frac{G^{intra}(k_{Sub_i^{N-1}} \cdot k_{Sub_j^{N-1}})}{F2(h_{Sub_i^{N-1}, Sub_j^{N-1}})}}{\sum_{e_{Sub_a^{N-1}, Sub_b^{N-1}} \in \bar{E^N}} \frac{G^{intra}(k_{Sub_a^{N-1}} \cdot k_{Sub_b^{N-1}})}{F2(h_{Sub_a^{N-1}, Sub_b^{N-1}})}}, \tag{17}$$

where $(N-1)$th layer subnetwork Sub_i^{N-1} and Sub_j^{N-1} belong to the same Nth layer subnetwork and $\bar{E^N}$ is the set of links in the complementary graph of the Nth layer initial virtual topology. $k_{Sub_i^{N-1}}$ is a degree of Sub_i^{N-1} and $h_{Sub_i^{N-1}, Sub_j^{N-1}}$ is the minimum hop count from Sub_i^{N-1} to Sub_j^{N-1} in graph of Nth layer initial virtual topology.

The strategy function G^{intra} is the same one shown in Section 3.3 and we use the same strategy as the strategy to construct a 1st layer VSN topology.

The number of added Nth layer virtual links is $\lceil C^N_{\text{intra}}|E^N_0|\rceil$, where $|E^N_0|$ is the number of links embedded in the Nth layer initial intra-subnetwork topology and C^N_{intra} is a constant value of 0 to 1.

3.4.2 Constructing a virtual link between under layer virtual sensor networks based on Nth layer virtual link

In this section, we explain the method to construct virtual links between the sensor nodes which belong to different subnetworks based on Nth layer virtual link. We select endpoints of an Nth layer virtual link from subnetworks in under layer recursively.

When there is an Nth layer virtual link between Sub^{N-1}_x and Sub^{N-1}_y, we construct an $(N-1)$th layer virtual link by selecting endpoints from $(N-2)$th layer subnetworks $Sub^{N-2}_i \in Sub^{N-1}_x$ and $Sub^{N-2}_j \in Sub^{N-1}_y$. We assumed that the relational operator "$\in$" whose right operand is an Nth layer subnetwork (Sub^N_i) means that its left operand is a subnetwork in a lower Nth layer and composes Sub^N_i.

The probability to add a link between Sub^{N-2}_i and Sub^{N-2}_j as endpoints of an Nth layer virtual link is defined as

$$p^N_{\text{inter}}(Sub^{N-2}_i, Sub^{N-2}_j) = \frac{\frac{G^{inter}(k_{Sub^{N-2}_i}, k_{Sub^{N-2}_j})}{F2(h_{Sub^{N-2}_i, Sub^{N-2}_j})}}{\sum_{Sub^{N-2}_a \in Sub^{N-1}_x, Sub^{N-2}_b \in Sub^{N-1}_y} \frac{G^{inter}(k_{Sub^{N-2}_a}, k_{Sub^{N-2}_b})}{F2(h_{Sub^{N-2}_a, Sub^{N-2}_b})}}, \quad (18)$$

where $Sub^{N-1}_x \neq Sub^{N-1}_y$ and $Sub^{N-2}_i \in Sub^{N-1}_x, Sub^{N-2}_j \in Sub^{N-1}_y$.

The function G^{inter} is a strategy of selecting endpoints Sub^{N-2}_x and Sub^{N-2}_y preferentially according to their degrees in $(N-1)$th layer VSN topology. We investigate a four different strategies for adding a new link in inter-subnetwork and the name of each strategy $inter$ is labeled by "HH", "LL", "HL" and "R". When $inter =$ HH, a pair of two nodes with higher degree is selected preferentially for a new link, and when $inter =$ LL, a pair of two nodes with lower degree is selected for a new link. When $inter =$ HL, a node with higher degree and another with lower degree are selected preferentially and connected. When $inter =$ R, a pair of two nodes is selected randomly regardless of their degrees. Each definition of G^{inter} is as follows.

$$G^{HH}(k_{Sub_i^{N-2}}, k_{Sub_j^{N-2}}) = k_{Sub_i^{N-2}} \cdot k_{Sub_j^{N-2}}. \tag{19}$$

$$G^{LL}(k_{Sub_i^{N-2}}, k_{Sub_j^{N-2}}) = k^{-1}_{Sub_i^{N-2}} \cdot k^{-1}_{Sub_j^{N-2}}. \tag{20}$$

$$G^{HL}(k_{Sub_i^{N-2}}, k_{Sub_j^{N-2}}) = \max(k_{Sub_i^{N-2}}, k_{Sub_j^{N-2}}) \cdot |k_{Sub_i^{N-2}} - k_{Sub_j^{N-2}}|. \tag{21}$$

$$G^{R}(k_{Sub_i^{N-2}}, k_{Sub_j^{N-2}}) = 1. \tag{22}$$

Note that Sub^1 means a module which is detected by using the algorithm described in Section 3.2 and Sub^0 means a sensor node.

The number of added virtual links per upper layer link is $\lceil C_{\text{inter}}(E^{Sub_x^{N-1}} + E^{Sub_y^{N-1}})\rceil$, where $E^{Sub_x^{N-1}}$ is the number of links embedded in the $(N-1)$th layer VSN topology of Sub_x^{N-1} and C_{inter} is a constant value of 0 to 1. However, when $N = 2$, the value of $(E^{Sub_x^1} + E^{Sub_y^1})$ is relatively large, accordingly the number of added virtual links between modules is large, resulting in small modularity. Therefore, when $N = 2$, the number of added virtual links is $\lceil \alpha C_{\text{inter}}(E^{Sub_x^1} + E^{Sub_y^1})\rceil$ where α is a constant value of 0 to 1. By applying this algorithm recursively till $N = 2$, we can finally construct a VSN topology composed of whole sensor nodes.

4 Simulation experiments

In this section, we evaluate our proposal through comparison with Bio-inspired small world network model (Bio-inspired) [21]. We briefly explain Bio-inspired in Section 4.1. Our proposed model, called brain-inspired configuring model (BICM), has 16 kinds of results by combination of 4 strategies of $intra$ and 4 strategies of $inter$. Therefore, we identify each strategy by two arguments of $intra$ and $inter$, such as BICM($intra$,$inter$).

4.1 Bio-inspired techniques for achieving small world properties

Bio-inspired is a model which achieves small world properties using bio-inspired techniques in wireless network with non-uniform node density [21]. The algorithm is composed of two steps, identifying clustering by using Lateral Inhibition technique and identifying nodes that construct long-distance links by using Flocking technique. The first step is described in Section 4.1.1 and the second step is described in Section 4.1.2. Authors assume that a long-distance link is realized by creating the directional beam because a power consumption is the same as when omnidirectional transmission.

4.1.1 Clustering by using Lateral Inhibition technique

In this section, we explain the clustering algorithm by using Lateral Inhibition technique. At first, each node v floods a control packet contained node ID of cluster head it is associated (H_i), the minimum hop count from it to $H_i(h_{v,H_i})$ and the degree of $H_i(k_{H_i})$. Initially, all the nodes consider themselves as cluster heads and store their information $H_i = v$, $h_{v,H_i} = 0$ and $k_{H_i} = k_v$. When a node w receives a control message, it updates stored information based on stored and received information. We assume that node w stores information that it belongs to cluster j and is associated H_j. When $k_{H_j} < k_{H_i}$ and $h_{w,H_i} < g$, where g is the maximum gradient of cluster, node w is associated H_i and updates its stored information to belong to the cluster i. Further, when $k_{H_j} = k_{H_i}$ and $h_{w,H_i} < h_{w,H_j}$, node w is associated H_i and updates its stored information. When a hop count is also the same, then the node w decides to update the stored information to the received information randomly. Then node w broadcasts the updated information after incrementing the hop count by 1. This process is repeated till all the nodes are associated the cluster head which is the maximum degree within g hops.

4.1.2 Constructing a long-distance link by using Flocking technique

In this section, we explain identifying nodes that construct long-distance links by using Flocking technique. In Bio-inspired model, a long-distance link is constructed between a centroid and a peripheral nodes of a cluster to reduce average path length efficiently. A centroid node of a cluster is a node with the maximum closeness centrality and a peripheral node of a cluster is a node deployed at boundary of the cluster. Closeness centrality is the fraction of shortest distance between a node to all other nodes in the network of intra cluster and defined as

$$Closeness(v_i) = \frac{1}{\sum_{w \neq v_i, w \in C_i} \mathrm{sd}(v_i, w)}, \tag{23}$$

where sd is the minimum hop count between two nodes. To identify peripheral nodes of cluster i, a centroid node c_i of cluster i broadcasts a control message and each node in the cluster gets a hop count to c_i. Then, the node with the maximum hop count to c_i in those of its neighbors declares itself as a peripheral node.

Each peripheral node v_i randomly selects the number of antenna elements m which is a value of 2 to M and determines a beam length and a beam width. A beam length is mr, where r is a communication range in omnidirectional mode, and a beam width is $\frac{2\pi}{m^2}$. Each peripheral node v_i searches centroid nodes existing within the circle of radius mr and nominates them for the endpoint of a long-distance link. When a neighboring peripheral node already connected to the centroid node c_j, a peripheral node v_i excludes c_j from candidates. Then, node v_i selects the node to which the minimum hop count is the maximum in candidates and constructs a long-distance link to it.

4.2 Evaluation metrics

The evaluation metrics are small worldness, clustering coefficient, average path length in virtual network, average path length in physical network, modularity, the total number of virtual links, robustness of connectivity and robustness of average path length.

The metric of small worldness, ω, are proposed in [22]. ω compares network clustering to an equivalent lattice network and average path length to a random network. Equivalent network means that the degree distribution is the same as that of the original network. ω is defined as

$$\omega = \frac{L_{rand}}{L} - \frac{C}{C_{latt}}, \tag{24}$$

Table 1: Parameter settings

model	parameter	value
BICM	C_{intra}	0.1
	C_{inter}	0.1
	α	0.1
Bio-inspired	g	4
	M	6

where L is average path length and C is clustering coefficient of the original network, L_{rand} is average path length of equivalent random network and C_{latt} is clustering coefficient of equivalent lattice network. ω is in range [-1,1]. The original network has small world properties when $\omega \sim 0$, it has a lattice like property when $\omega \sim -1$ and it has a random like property when $\omega \sim 1$.

When we evaluate APL in the virtual network (vAPL), we assume that nodes connected by a virtual link can communicate with each other in one hop. When we evaluate APL in the physical network (pAPL), we assume that nodes connected by a virtual link communicate with each other in shortest multihop path of physical network. According to the method to realize a long-distance link in physical network, actual APL in physical network may change. Therefore, vAPL indicates the minimum APL and pAPL indicates the maximum APL.

The metric of modularity is Q shown in Section 3.2.

We evaluate robustness of connectivity and APL by removing a node one by one. We evaluate the decline in a component size which is the number of nodes in the maximum connected component when we evaluate robustness of connectivity and we evaluate the increase in APL when we evaluate robustness of APL. If there is no path from node i to node j according to removal of nodes, we calculate APL with regarding the hop count between them as the number of nodes (N). We assume two kinds of removal models, random error and targeted attack. The node removed in the next time step is selected randomly in random error, and the node with the largest degree is selected to be removed in the next time step in targeted attack.

The parameter settings are shown in Table 1 and we used OMNeT++ [23] for simulation experiments.

4.3 Two-layered virtual sensor networks without a long wired connection

In this section, we evaluate a virtual sensor network which is constructed by one sensor network. In our model, a constructed virtual sensor network is two-layered.

In simulation, 500 sensor nodes are deployed at random places in the area of 1000m $\times$ 1000m and the communication range is 100m. An example of a physical sensor network is shown in Figure 2. We construct a virtual sensor network based on such a physical topology and evaluate it.

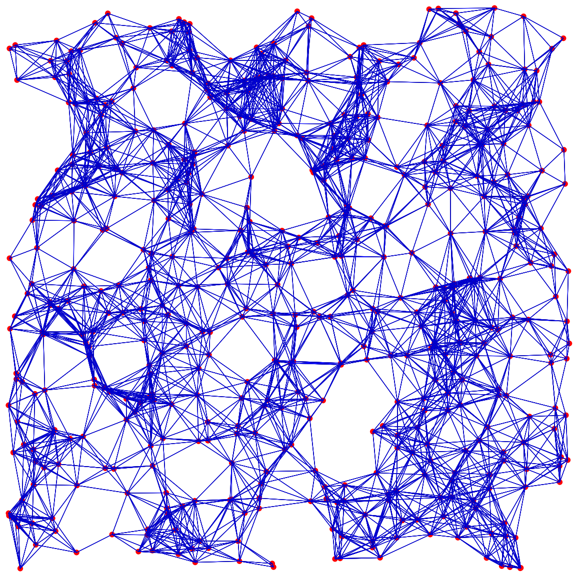

Figure 2: Example of a physical sensor network

4.3.1 Small world properties

In this section, we evaluate a constructed VSN topology and summarize small worldness (ω), CC, vAPL, pAPL, the total number of virtual links and modularity (Q) in Table 2.

A VSN constructed by BICM model has small world properties but relatively lattice like properties. In BICM, a link which has great influence on vAPL and pAPL is a link between modules. When the strategy $inter$ is HH or HL, vAPL of a whole network tends to be small because the long-distance link is constructed at high degree nodes. On the contrary, vAPL tends to be large when the strategy $inter$ is LL. When the strategy $inter$ is R, vAPL tends to be large because a distance constraint is only considered. However, when $inter = \mathrm{R}$, pAPL tends to be small because a constructed virtual network is similar to physical network due to distance constraints.

A VSN constructed by Bio-inspired model has the highest small worldness due to $\omega \sim 0$. Further, although the number of virtual links is the largest, vAPL and pAPL is the smallest of all the models. This is due to Flocking technique. The long-distance links are distributed all over the network because each peripheral node does not construct a long-distance link to the centroid node which is already connected with its neighbor node. Moreover, APL reduces drastically because each peripheral node selects the centroid node to which the minimum hop count is the maximum in the candidates and constructs a long-distance link to it.

Table 2: Comparison of VSN constructed by each models in one sensor network

	ω	CC	vAPL	pAPL	# of virtaul links	Q
BICM(hh,HH)	-0.389	0.657	4.09	8.33	3591	0.814
BICM(hh,LL)	-0.410	0.606	4.56	8.82	3593	0.840
BICM(hh,HL)	-0.390	0.627	4.23	8.56	3592	0.847
BICM(hh,R)	-0.454	0.624	4.85	7.90	3591	0.825
BICM(ll,HH)	-0.337	0.589	4.11	8.28	3595	0.823
BICM(ll,LL)	-0.337	0.571	4.21	8.15	3597	0.838
BICM(ll,HL)	-0.310	0.579	4.05	8.71	3593	0.852
BICM(ll,R)	-0.371	0.575	4.47	7.94	3595	0.833
BICM(hl,HH)	-0.327	0.616	3.92	8.42	3597	0.799
BICM(hl,LL)	-0.363	0.583	4.38	8.15	3594	0.830
BICM(hl,HL)	-0.312	0.605	3.92	8.57	3592	0.824
BICM(hl,R)	-0.410	0.590	4.72	7.74	3596	0.825
BICM(r,HH)	-0.384	0.643	4.11	8.40	3589	0.844
BICM(r,LL)	-0.425	0.607	4.47	8.50	3592	0.847
BICM(r,HL)	-0.365	0.618	4.13	8.43	3591	0.836
BICM(r,R)	-0.456	0.620	4.76	7.92	3592	0.833
Bio-inspired	-0.219	0.580	3.56	6.65	3749	0.742

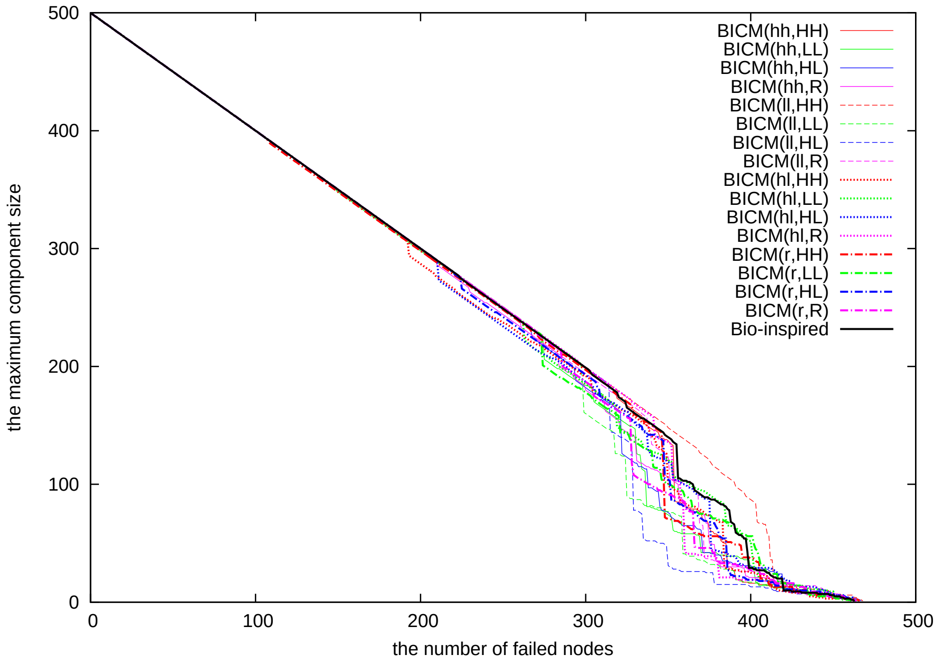

Figure 3: Robustness of connectivity against random failure when a VSN is constructed by one sensor network

4.3.2 Robustness of connectivity

In this section, we evaluate robustness of connectivity against random fail and targeted attack.

Figure 3 and Figure 4 show the decline of a component size when nodes are removed by random fail and targeted attack respectively. The decline of component size of each model is almost same. In BICM, when nodes are removed by targeted attack, a link which has great influence on the decline of a component size is also a link between modules. A VSN constructed by the strategy $inter = \mathrm{LL}$ or $inter = \mathrm{R}$ is highly robust in terms of connectivity because it keeps a component size high. A VSN constructed by Bio-inspired is highly robust in terms of connectivity because it is based on lattice regular graph.

4.3.3 Robustness of average path length

In this section, we evaluate robustness of vAPL and pAPL against random fail and targeted attack. Figure 5 and Figure 6 show the increase tendency of vAPL when nodes are removed by random fail and targeted attack respectively. In BICM, a link which has great influence on robustness of

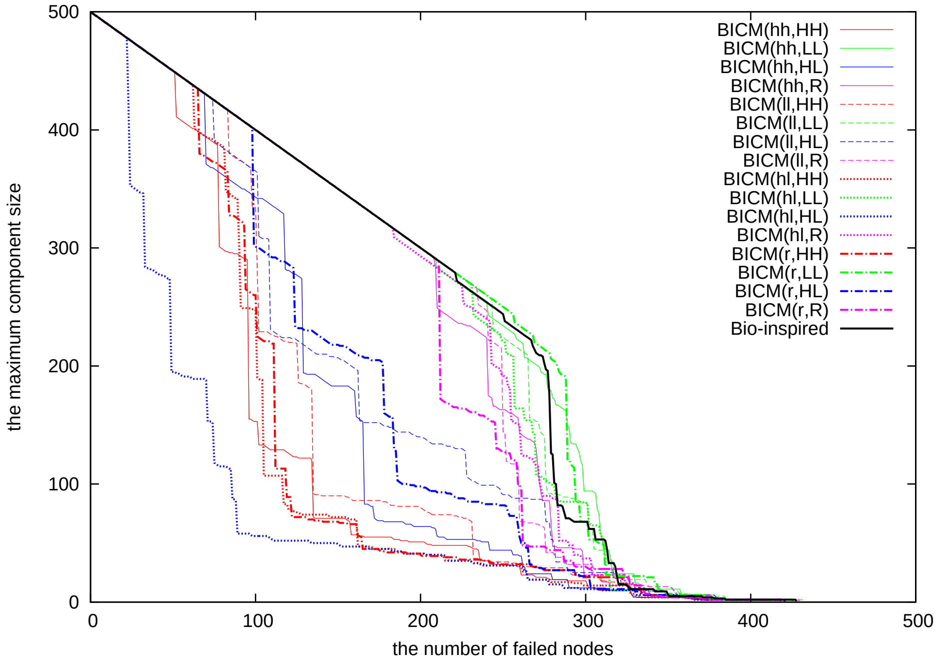

Figure 4: Robustness of connectivity against targeted attack when a VSN is constructed by one sensor network

vAPL is a link between modules. All the VSN constructed by each model have a highly robust against random fail in terms of vAPL. A VSN constructed by BICM of the strategy $inter = \mathrm{HH}$ or $inter = \mathrm{HL}$ or by Bio-inspired has smaller vAPL because a long-distance link is constructed to the node with high degree or closeness centrality. However, they are vulnerable of vAPL against targeted attack due to the same reason. When the nodes are removed by targeted attack, a VSN constructed by BICM of the strategy $inter = \mathrm{LL}$ or $inter = \mathrm{R}$ has highly robust in terms of vAPL.

Figure 7 and Figure 8 show the increase tendency of pAPL when nodes are removed by random fail and targeted attack respectively. All the VSN constructed by each model have a highly robust of pAPL against random fail. The VSN constructed by BICM of the strategy $inter = \mathrm{R}$ or by Bio-inspired has smaller pAPL because the both of constructed topologies are almost same as physical network and almost all paths are shortest paths in the physical network. When nodes are removed by targeted attack, a VSN constructed by BICM of the strategy $inter = \mathrm{LL}$ or $inter = \mathrm{R}$ has highly robust of pAPL. The VSN constructed by Bio-inspired has the highest robustness of pAPL against targeted attack because it is based on physical network.

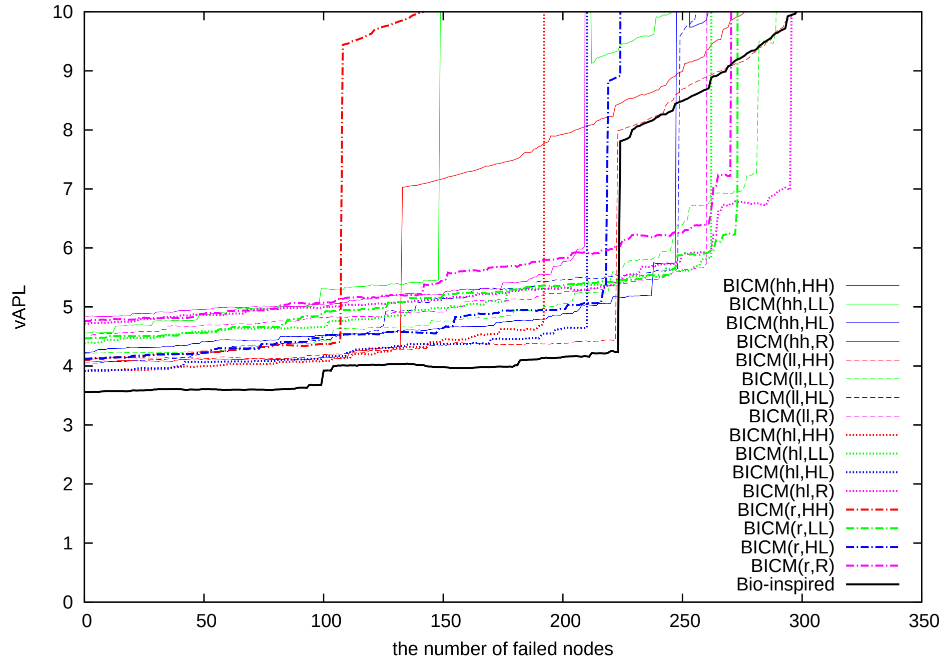

Figure 5: Robustness of vAPL against random failure when a VSN is constructed by one sensor network

From the above, the highly robust model in both vAPL and pAPL is BICM with the strategy $inter = \text{LL}$.

4.4 Three-layered virtual sensor networks with a long wired connection

In this section, we evaluate a virtual sensor network which is constructed by two sensor networks which are connected by one wired link. In our model, a constructed virtual sensor network is three-layered.

In simulation, two sensor networks, each of which is composed of 200 sensor nodes, are embedded in the area of 1000m $\times$ 1000m. For one of two sensor networks, 200 sensor nodes are deployed at random places in the area of $0\text{m} \le x \le 400\text{m}$, $0\text{m} \le y \le 1000\text{m}$, and 200 sensor nodes are deployed at random places in the area of $600\text{m} \le x \le 1000\text{m}$, $0\text{m} \le y \le 1000\text{m}$ for the other. One wired link is embedded between two sensor networks and sensor nodes of its endpoints are statically selected. When the wireless communication range is 100m, an example of a physical sensor network is shown in Figure 9. We construct a VSN based on such a physical topology and evaluate it.

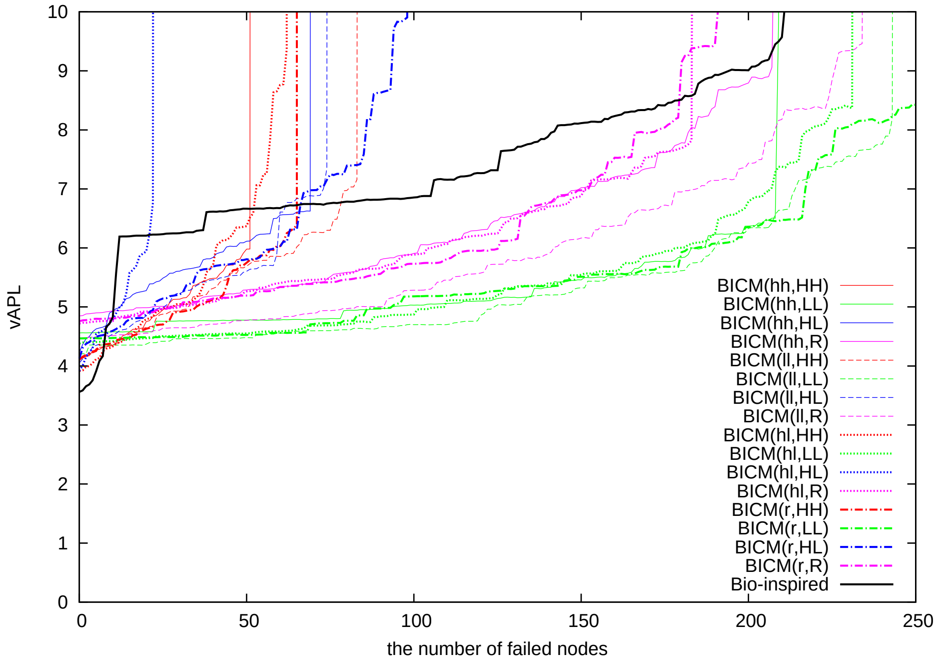

Figure 6: Robustness of vAPL against targeted attack when a VSN is constructed by one sensor network

4.4.1 Small world properties

In this section, we evaluate a constructed VSN topology and summarize small worldness (ω), CC, vAPL, pAPL, the total number of virtual links and modularity (Q) in Table 3.

Table 3 shows the almost same tendency as the properties of the VSN constructed by one sensor network. This implies that multi-layered VSN can be constructed by applying our proposed algorithm recursively and its topology has similar properties to those of two-layered VSN. A VSN constructed by BICM model has small world properties but relatively lattice like properties. In BICM, a link between modules has great influence on vAPL and pAPL. When the strategy $inter$ is HH or HL, vAPL of a whole network tends to be small because a long-distance link is constructed at high degree nodes. On the contrary, vAPL tends to be large when the strategy $inter$ is LL. A VSN constructed by Bio-inspired model has the highest small worldness due to $\omega \sim 0$. Further, although the number of virtual links is the largest, vAPL and pAPL is the smallest of all the models according to Flocking technique.

Table 3: Comparison of VSN constructed by each models in two sensor networks connected by one wired link

	ω	CC	vAPL	pAPL	# of virtual links	Q
BICM(hh,HH)	-0.387	0.660	4.20	10.25	2722	0.849
BICM(hh,LL)	-0.451	0.621	4.89	11.12	2722	0.843
BICM(hh,HL)	-0.406	0.638	4.43	10.51	2721	0.847
BICM(hh,R)	-0.419	0.640	4.47	9.51	2723	0.841
BICM(ll,HH)	-0.312	0.593	4.09	10.46	2727	0.851
BICM(ll,LL)	-0.368	0.579	4.46	10.25	2727	0.844
BICM(ll,HL)	-0.342	0.587	4.32	10.95	2722	0.848
BICM(ll,R)	-0.358	0.584	4.46	9.42	2724	0.826
BICM(hl,HH)	-0.347	0.629	4.16	10.12	2722	0.840
BICM(hl,LL)	-0.428	0.606	4.89	10.16	2716	0.854
BICM(hl,HL)	-0.371	0.618	4.28	10.72	2720	0.853
BICM(hl,R)	-0.434	0.612	4.93	9.67	2718	0.849
BICM(r,HH)	-0.461	0.653	4.74	10.06	2716	0.851
BICM(r,LL)	-0.452	0.618	4.85	11.45	2721	0.848
BICM(r,HL)	-0.385	0.630	4.29	10.47	2725	0.849
BICM(r,R)	-0.474	0.637	4.94	9.42	2722	0.840
Bio-inspired	-0.203	0.587	3.56	8.23	2787	0.769

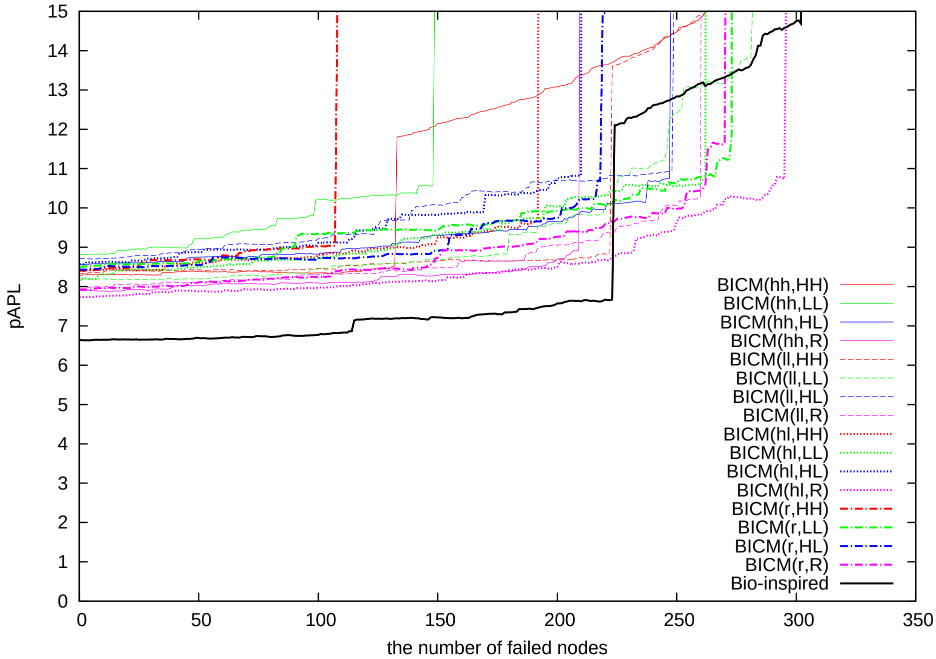

Figure 7: Robustness of pAPL against random failure when a VSN is constructed by one sensor network

4.4.2 Robustness of connectivity

In this section, we evaluate robustness of connectivity against random fail and targeted attack.

Figure 10 and Figure 11 show the decline of a component size when nodes are removed by random fail and targeted attack respectively. Note that there are few opportunities to fail the node which is the endpoint of a wired link than other nodes because it is assumed to be supplied energy through wired link. Therefore, we assume that the node connected by a wired link does not fail.

The decline of a component size of each model is almost same. In BICM, when nodes are removed by targeted attack, a VSN constructed by the strategy $inter = \mathrm{LL}$ or $inter = \mathrm{R}$ is highly robust in terms of connectivity because it keeps a component size high. A VSN constructed by Bio-inspired is highly robust in connectivity because it is based on lattice regular graph. These features are also observed in Section 4.3.2.

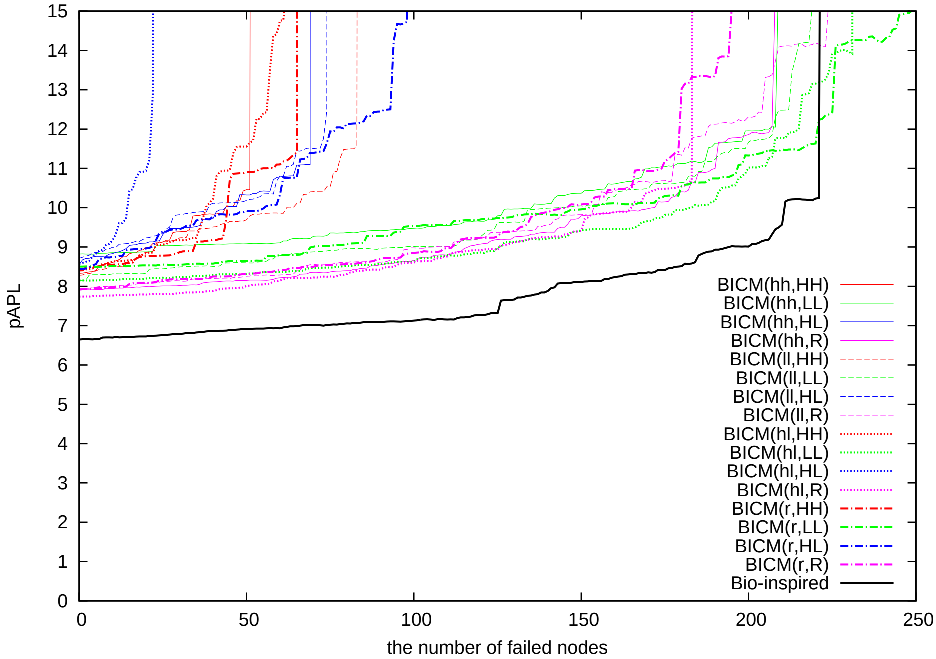

Figure 8: Robustness of pAPL against targeted attack when a VSN is constructed by one sensor network

4.4.3 Robustness of average path length

In this section, we evaluate robustness of vAPL and pAPL against random fail and targeted attack. The results show an almost same tendency as the results of a VSN which is constructed by one sensor network. Figure 12 and Figure 13 show the increase tendency of vAPL when nodes are removed by random fail and targeted attack respectively. All the VSN constructed by each model have a high robustness against random fail in terms of vAPL. A VSN constructed by BICM of the strategy $inter$ = HH or $inter$ = HL or by Bio-inspired has smaller vAPL because a long-distance link is constructed to the node with high degree or closeness centrality. However, they are vulnerable of vAPL against targeted attack due to the same reason. When nodes are removed by targeted attack, a VSN constructed by BICM of the strategy $inter$ = LL or $inter$ = R has high robustness of vAPL.

Figure 14 and Figure 15 show the increase tendency of pAPL when nodes are removed by random fail and targeted attack respectively. All the VSN constructed by each model have a highly robust of pAPL against random fail. A VSN constructed by BICM of the strategy $inter$ = R or by

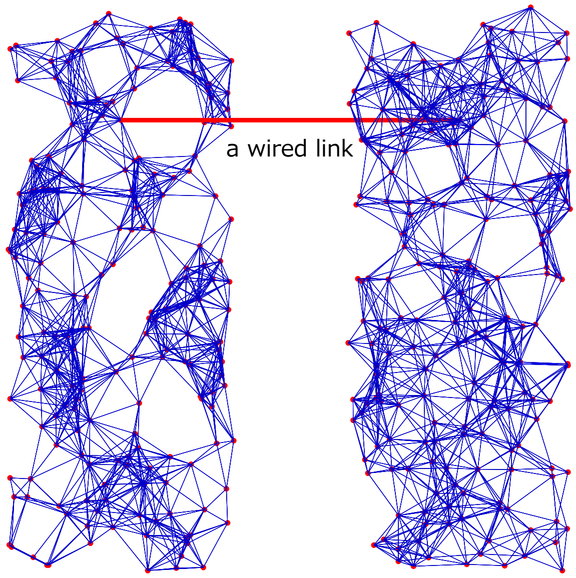

Figure 9: Example of a physical sensor network composed of two sensor networks connected by one wired link

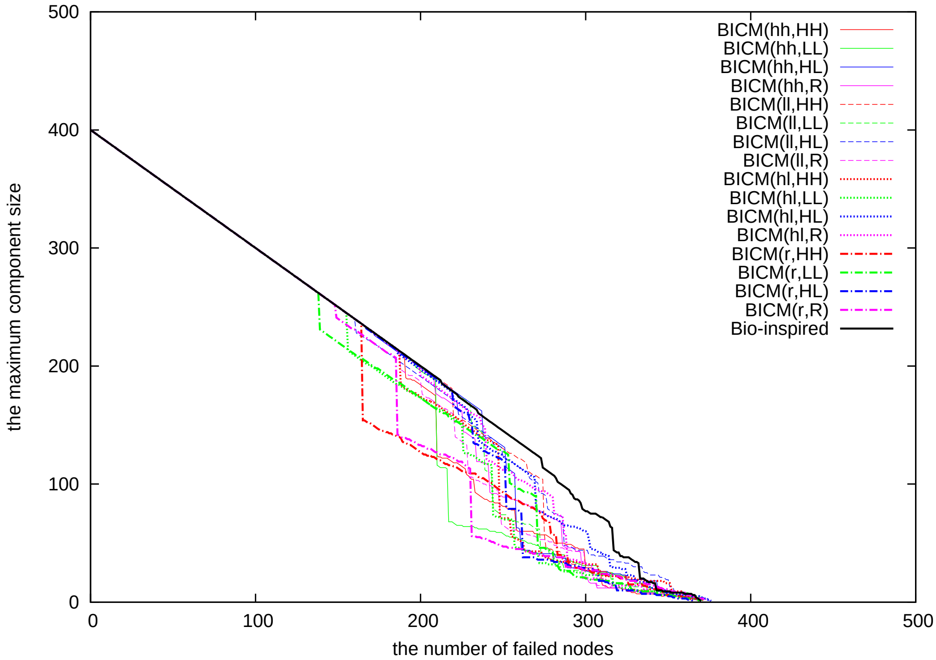

Figure 10: Robustness of connectivity against random failure when a VSN is constructed by two sensor networks with one wired link

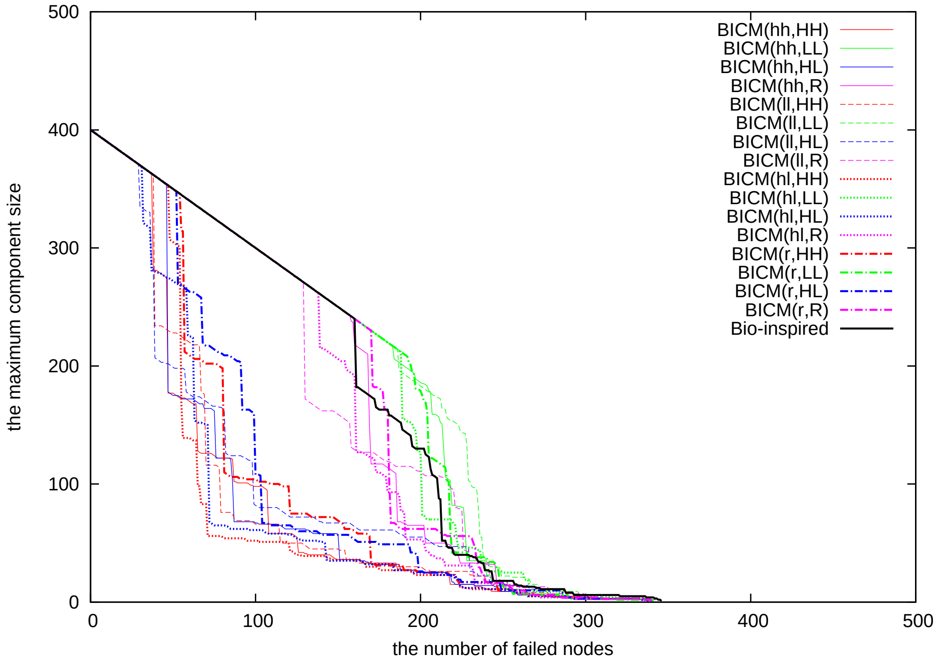

Figure 11: Robustness of connectivity against targeted attack when a VSN is constructed by two sensor networks with one wired link

Bio-inspired has smaller pAPL because both of constructed topologies are almost same as physical network and almost all paths are shortest paths in the physical network. When nodes are removed by targeted attack, a VSN constructed by BICM of the strategy $inter$ = LL or $inter$ = R has high robustness of pAPL. A VSN constructed by Bio-inspired has the highest robustness of pAPL against targeted attack because it is based on physical network.

From the above, the highly robust model in both vAPL and pAPL is BICM with the strategy $inter$ = LL.

When we consider all results, multi-layered VSN constructed by our proposed algorithm has a certain small worldness, communication efficiency, robustness of connectivity and robustness of APL. This suggests that subnetworks observed on arbitrary scale of VSN constructed by our algorithm have similar properties.

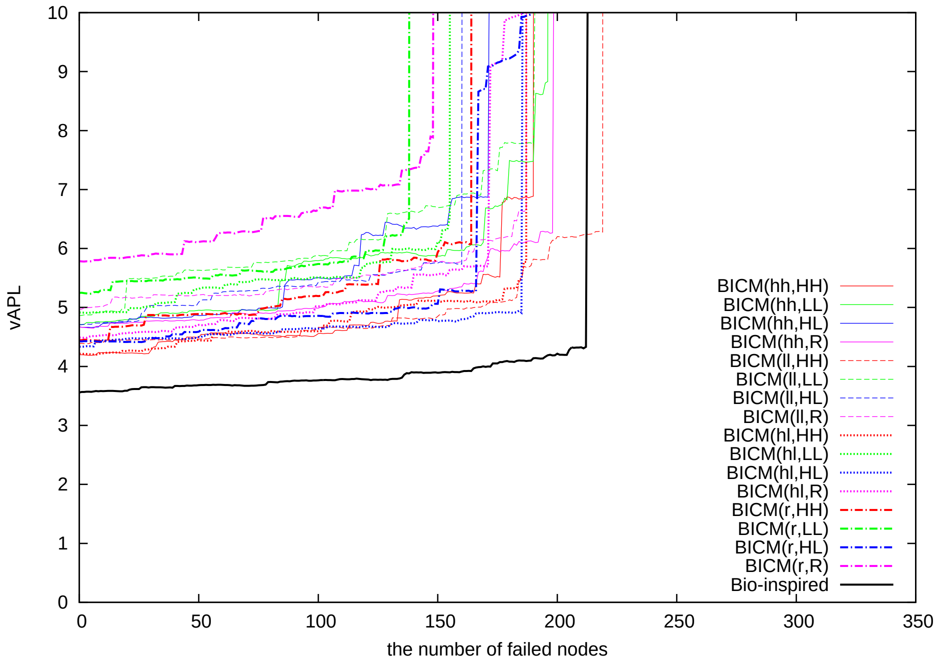

Figure 12: Robustness of vAPL against random failure when a VSN is constructed by two sensor networks with one wired link

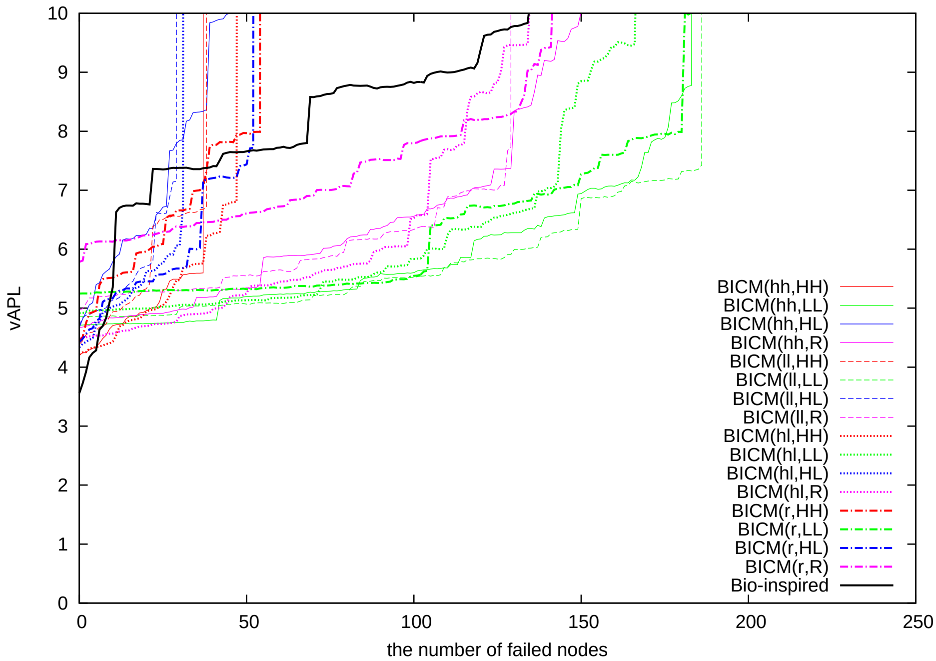

Figure 13: Robustness of vAPL against targeted attack when a VSN is constructed by two sensor networks with one wired link

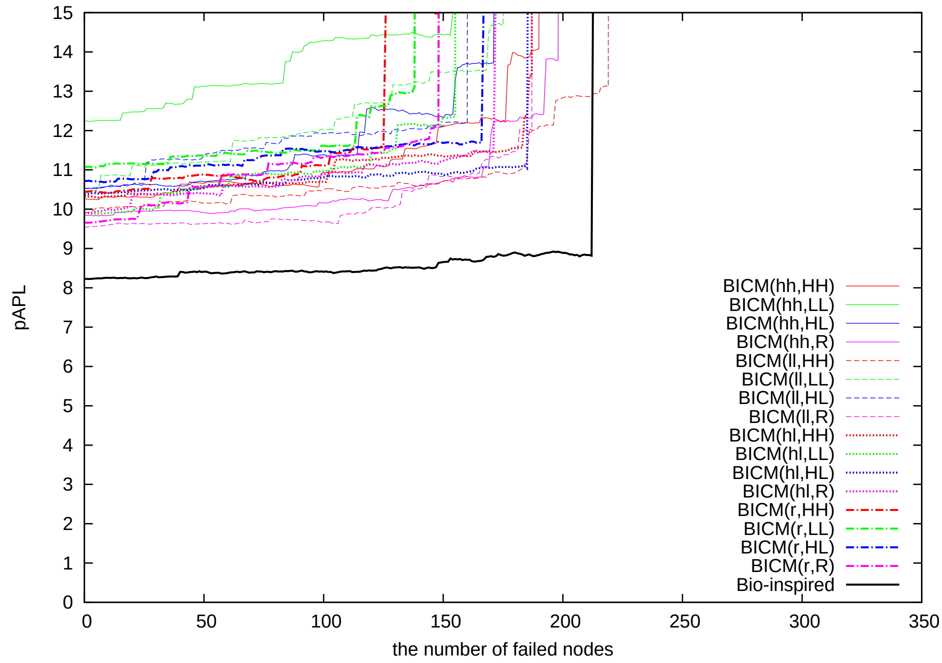

Figure 14: Robustness of pAPL against random failure when a VSN is constructed by two sensor networks with one wired link

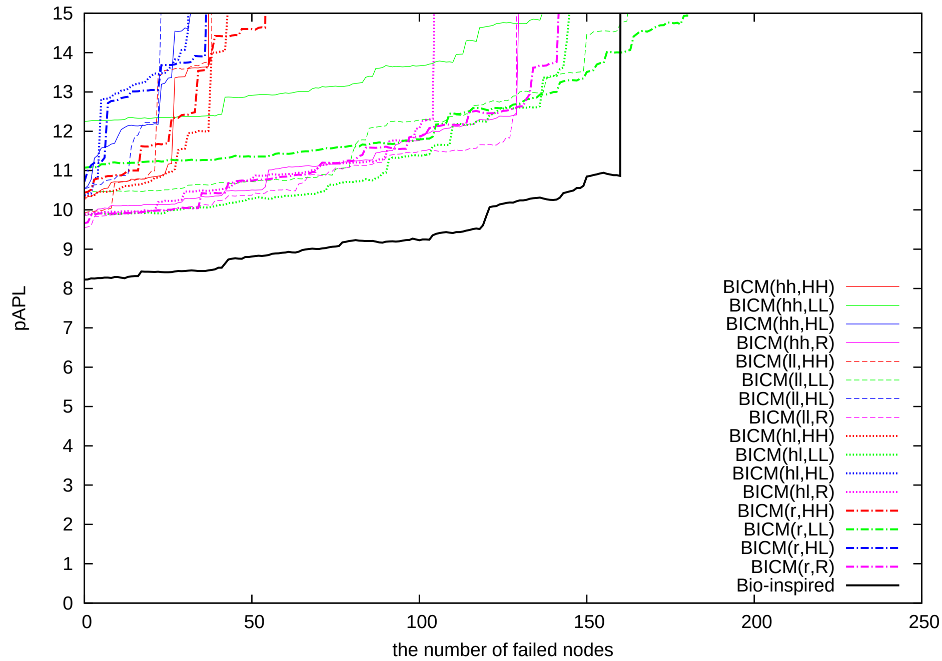

Figure 15: Robustness of pAPL against targeted attack when a VSN is constructed by two sensor networks with one wired link

5 Conclusion and Future Work

In this thesis, we propose a model for constructing a VSN topology inspired by brain functional networks. Our proposed model is organized by three steps, dividing sensor networks into unit modules, constructing a virtual topology with small world property in each module and integrating multiple modules or subnetworks of under layer. We investigate combinations of four strategies $intra$ for constructing an intra Nth layer virtual links and four strategies $inter$ for configuring virtual links of under layer based on a virtual link of Nth layer.

The results of the simulation experiments show that the strategy $inter$ plays an important role for communication efficiency and robustness of constructed VSN topology. When at least one of the endpoints of virtual long-distance link between modules has high degree, global efficiency is improved but robustness against targeted attack declines. When nodes which are within different modules and have low degree are connected by a virtual long-distance link, global efficiency is slightly low but all of three kinds of robustness, in terms of connectivity, vAPL and pAPL, against targeted attack are high. Comparing with a VSN topology constructed by Bio-inspired, a VSN topology constructed by our model has a high robustness of vAPL against targeted attack.

In this thesis, we analyze only static properties of virtual topology composed of all sensor nodes. Therefore, we need to consider the followings in future work. At first we need consider the method to realize a virtual link in physical network. The packet forwarded along a virtual link should be conveyed with short delay. For example, creating directional beam, increasing omnidirectional transmission range or forwarding by multi hop with priority will do. Secondly, when there are multiple demands for constructing VSNs which compete for resources such as energy, memory or bandwidth, we need investigate the model constructing resource efficient VSN topologies. Thirdly, we want to construct a protocol for configuring a VSN topology adaptively according to environmental changes, such as diverse traffic patterns, addition or removal of virtual nodes or modules. Due to modular community structure, small adjustment of a few numbers of virtual links between modules will achieve that.

Acknowledgements

This thesis would not accomplish without a lot of great supports of several people. First, I would like to express my sincere gratitude to my supervisor, Professor Masayuki Murata of Osaka University, for his continuous support and valuable advice throughout my studies, and providing me this precious study opportunity in his laboratory. Furthermore, I show my deepest appreciation to Assistant Professor Daichi Kominami of Osaka University. He devoted a great deal of time for me and gave me an excellent guideline of my research and considerable supports.

Moreover, I would like to appreciate to Professor Naoki Wakamiya, Associate Professor Shin'ichi Arakawa and Assistant Professor Yuichi Ohsita of Osaka University for beneficial comments and suggestions on this study.

In addition, I heartily thank Ms. Kazama, Ms. Negita and Ms. Yabiki secretaries' doing a lot of help, and the encouragement at times. Furthermore, I would like to express sincere appreciation to my senior associates, Mr. Takuya Iwai, Ms. Naomi Kuze. I received a lot of advices from them and they kindly provided consultation for me.

Finally, I would like to thank all the members of the Advanced Network Architecture Laboratory at the Graduate School of Information Science and Technology, Osaka University, for support and meaningful discussion about my research and hearty encouragement.

References

[1] M. M. Islam, M. M. Hassan, G.-W. Lee, and E.-N. Huh, “A survey on virtualization of wireless sensor networks,” *Sensors*, vol. 12, pp. 2175–2207, Feb. 2012.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, pp. 2787–2805, Oct. 2010.

[3] N. Javaid, I. Khan, M. Ullah, A. Mahmood, and M. Farooq, “A survey of home energy management systems in future smart grid communications,” in *Proceedings of the 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA2013)*, pp. 459–464, Oct. 2013.

[4] L. Sarakis, T. Zahariadis, H.-C. Leligou, and M. Dohler, “A framework for service provisioning in virtual sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 1–19, Apr. 2012.

[5] I. Ishaq, J. Hoebeke, I. Moerman, and P. Demeester, “Internet of Things virtual networks: Bringing network virtualization to resource-constrained devices,” in *Proceedings of the 8th IEEE International Conference on Green Computing and Communications (GreenCom2012)*, pp. 293–300, Nov. 2012.

[6] N. Namatame, J. Nakazawa, and H. Tokuda, “Logical sensor network: An abstraction of sensor data processing over multidomain sensor network,” *ISRN Sensor Networks*, vol. 2012, pp. 1–9, Oct. 2012.

[7] A. Merentitis, F. Zeiger, M. Huber, N. Frangiadakis, K. Mathioudakis, K. Sasloglou, G. Mazarakis, V. Gazis, and Z. Boufidis, “WSN trends: Sensor infrastructure virtualization as a driver towards the evolution of the Internet of Things,” in *Proceedings of the 7th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2013)*, pp. 113–118, Sept. 2013.

[8] G. Zheng, S. Liu, and X. Qi, “Scale-free topology evolution for wireless sensor networks with reconstruction mechanism,” *Computers & Electrical Engineering*, vol. 38, pp. 643 – 651, May 2012.

[9] J. Huang, Q. Xie, and B. Huang, "Creating small-world model for homogeneous wireless sensor networks," in *Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM2012)*, pp. 1–4, Sept. 2012.

[10] Z. Bao, Y. Cao, L. Ding, and G. Wang, "Comparison of cascading failures in small-world and scale-free networks subject to vertex and edge attacks," *Physica A: Statistical Mechanics and its Applications*, vol. 388, pp. 4491 – 4498, Oct. 2009.

[11] E. Bullmore and O. Sporns, "The economy of brain network organization," *Nature Reviews Neuroscience*, vol. 13, pp. 336–349, May 2012.

[12] C.-h. Park, S. Y. Kim, Y.-H. Kim, and K. Kim, "Comparison of the small-world topology between anatomical and functional connectivity in the human brain," *Physica A: Statistical Mechanics and its Applications*, vol. 387, pp. 5958–5962, Oct. 2008.

[13] L. K. Gallos, H. A. Makse, and M. Sigman, "A small world of weak ties provides optimal global integration of self-similar modules in functional brain networks," *Proceedings of the National Academy of Sciences*, vol. 109, pp. 2825–2830, Feb. 2012.

[14] S. Achard, R. Salvador, B. Whitcher, J. Suckling, and E. Bullmore, "A resilient, low-frequency, small-world human brain functional network with highly connected association cortical hubs," *The Journal of Neuroscience*, vol. 26, pp. 63–72, Jan. 2006.

[15] P. E. Vertes, A. F. Alexander-Bloch, N. Gogtay, J. N. Giedd, J. L. Rapoport, and E. T. Bullmore, "Simple models of human brain functional networks," *Proceedings of the National Academy of Sciences*, vol. 109, pp. 5868–5873, Mar. 2012.

[16] D. Meunier, R. Lambiotte, and E. T. Bullmore, "Modular and hierarchically modular organization of brain networks," *Frontiers in Neuroscience*, vol. 4, pp. 1–11, Dec. 2010.

[17] M. E. Newman, "Modularity and community structure in networks," *Proceedings of the National Academy of Sciences*, vol. 103, pp. 8577–8582, Apr. 2006.

[18] J. Zhao and K. Xu, "Enhancing the robustness of scale-free networks," *Journal of Physics A: Mathematical and Theoretical*, vol. 42, pp. 1–8, Jan. 2009.

[19] R. Guimera and L. A. N. Amaral, "Modeling the world-wide airport network," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 38, pp. 381–385, Mar. 2004.

[20] A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Physica A: Statistical Mechanics and its Applications*, vol. 272, pp. 173–187, Oct. 1999.

[21] R. Agarwal, A. Banerjee, V. Gauthier, M. Becker, C. K. Yeo, and B. S. Lee, "Achieving small-world properties using bio-inspired techniques in wireless networks," *The Computer Journal*, vol. 55, pp. 909–931, Mar. 2012.

[22] Q. K. Telesford, K. E. Joyce, S. Hayasaka, J. H. Burdette, and P. J. Laurienti, "The ubiquity of small-world networks," *Brain Connectivity*, vol. 1, pp. 367–375, Nov. 2011.

[23] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*, pp. 35–59, Springer, 2010.