Brain-inspired method for constructing a robust virtual wireless sensor network

Shinya Toyonaga
Graduate School of Information
Science and Technology,
Osaka University,
Suita, Osaka, Japan
Email: s-toyonaga@ist.osaka-u.ac.jp

Daichi Kominami
Graduate School of Economics,
Osaka University,
Toyonaka, Osaka, Japan
Email: d-kominami@econ.osaka-u.ac.jp

Masayuki Murata
Graduate School of Information
Science and Technology,
Osaka University,
Suita, Osaka, Japan
Email: murata@ist.osaka-u.ac.jp

***Abstract*—In future "Internet of Things" environment, wireless sensor networks (WSNs) are expected to play a crucial part by integrating them into a part of infrastructure. For this, large-scale WSNs comprising heterogeneous devices from multiple vendors should be feasible. Virtualization in WSNs is of great significance as a way to effect integration of WSNs. In this paper, we propose a method for constructing a robust virtual wireless sensor network; this method is inspired by human brain networks, which are known for their robustness and high efficiency. Through simulation experiments, we show that our proposed method has high robust connectivity and robust average path length.**

***Index Terms*—Virtual topology, Human brain network, Hierarchical modular structure.**

I. Introduction

In the recent past, considerable attention centered on wireless sensor networks (WSNs) as a vital technology for realizing the so-called "Internet of Things." WSNs are expected to play a crucial part by integrating them into a part of infrastructure shared by multiple applications [1].

Given this context, multiple vendors will deploy various types of sensor nodes in the same area. To integrate WSNs and share physical substrates of sensor nodes in such a heterogeneous environment, virtualization of WSNs is one key solution.

Although virtualization of WSNs has been worked on by many researchers [2], [3], how to make a virtual topology for each application in an overlay layer has not been discussed enough. Because environmental changes, such as diverse traffic patterns, varying traffic demands and addition/removal of virtual nodes, can occur in the virtualization of sensor networks, efficiency and connectivity are important when constructing a virtual wireless sensor network (VWSN) that must offer communication guarantees. Along these lines, we propose a method to construct a VWSN topology which has high robustness and communication efficiency by introducing the structural characteristics possessed by human brain networks which are known for their efficiency and robustness. In this paper, we define two kinds of robustness: robustness of connectivity and robustness of average path length. Robustness of connectivity is the characteristic that the size of connected component does not change so much when some nodes fail. Also robustness of average path length is the characteristic that average path length keeps its length when some nodes fail.

Brain networks have many features, but here we focus especially on their modularity and small-world properties. A brain network is composed from many modules, defined as a subset of nodes, where the nodes in the same module are densely intra-connected and the nodes in different modules are sparsely inter-connected by a few long-distance links [4]. This contributes to a high clustering coefficient and short average path length which is known for small-world properties, and leads to high communication efficiency in both global and local areas. Moreover, a highly clustered structure within modules permits many detour routes from one node to another in the same module. This leads to robust connectivity. To garner the advantages described above, we propose a method to construct a VWSN topology with a modular community structure and small-world properties.

The rest of this paper is organized as follows. In Section II, we discuss related work. In Section III, we propose a method to construct a brain-inspired VWSN topology and evaluate our proposal in Section IV. We conclude this paper and describe future work in Section V.

II. Related Work

In the existing research, virtualization of WSNs is divided into two classes: node-level virtualization and network-level virtualization [1]. Node-level virtualization is a technique that enables multiple applications to run on a single node concurrently. Three types of solutions for node-level virtualization are considered according to which component supports the concurrency: OS-based [5], virtual machine-based [6] and middleware-based solutions [7]. In network-level virtualization, a subset of sensor nodes constitutes a virtual network for running one application. This virtualization leads to resource efficiency because the remaining nodes can be used for other applications. For network-level virtualization, two types of solutions are considered: overlay-based [3] and cluster-based solutions [8]. When we follow this classification, our target is network-level virtualization with overlay-based solution. Many overlay-based solutions for network-level virtualization have been proposed [2], [3]. The main objective of them is to provide a framework of sharing physical substrates of deployed sensor nodes. However, how to make a virtual topology for each application in an overlay layer has not been discussed enough. Therefore, our focus is how to construct a robust VWSN topology for an application.

III. Method

A highly modular topology enables robust connectivity, and a small-world topology enables efficient communication. Therefore, we construct a VWSN topology with high modularity and small-world properties. In our proposal, a VWSN topology is constructed by integrating unit modules, which are groups of sensor nodes clustered together by the Newman algorithm [9], hierarchically. The Newman algorithm heuristically divides a network into some modules so that the modularity of the network is maximized. Additionally, the topology constructed by our proposal has small-world properties at each tier by adding a small fraction of long-distance links to a clustered topology. Note that our proposal and the choice of a method for dividing nodes to modules are independent. This means that any modular division algorithm can be applied.

In this paper, we assume that the reachability between any two nodes in the physical topology are guaranteed via multi-hop wireless or wired links. And then, communication between two nodes connected by a virtual link is realized via physical shortest path between them in an infrastructural topology.

A. Constructing an Nth-tier VWSN topology

In this section, we describe a means of constructing an Nth-tier VWSN topology. We divide this problem into two small subproblems, as follows.

1. The first problem is, looking on an $(N-1)$th-tier VWSN as one subnetwork, which two subnetworks are connected in the Nth tier.
2. The second problem is how to map the endpoints of between-subnetwork Nth-tier links to sensor nodes.

A method to solve the first problem is shown in Section III-A1, and a method to solve the second problem is shown in Section III-A2.

1) Constructing a virtual link in the Nth tier: In this section, we describe a method of constructing a virtual link in the Nth tier between subnetworks in the $(N-1)$th tier. From the Nth tier's view, we take a VWSN in the $(N-1)$th tier as one subnetwork (denoted by S_i^{N-1}). Note that S_*^1 denotes a module identified by the Newman algorithm and S_*^0 denotes a sensor node.

The proposed method of constructing an Nth-tier VWSN topology consists of two steps, listed as follows.

1. Initial virtual topology construction
2. Virtual long-distance link additions to the initial virtual topology

In the first step, we construct an initial virtual topology on the basis of physical connections according to the rule that two $(N-1)$th-tier subnetworks are connected by an $(N-1)$th-tier virtual link when a pair of nodes connected by a physical link belong to respective $(N-1)$th-tier subnetworks. Note that, disjoint subgraphs can exist in cases where there is no physical link between them. When this occurs, the closest subnetworks in terms of hop count are connected by an $(N-1)$th-tier virtual link in order to guarantee connectivity of the network.

In the second step, we embed new $(N-1)$th-tier virtual links in the initial virtual topology by using a preferential attachment rule according to physical distance constraints and degree. This is for providing small-world properties to the topology. The probability of adding an $(N-1)$th-tier virtual link between S_i^{N-1} and S_j^{N-1} which belong to the same Nth-tier module is as follows.

$$p_{\mathrm{intra}}^{N}(S_i^{N-1}, S_j^{N-1}) = \frac{\dfrac{G^{intra}(k_{S_i^{N-1}}, k_{S_j^{N-1}})}{F(h_{S_i^{N-1},S_j^{N-1}})}}{\displaystyle\sum_{e_{S_a^{N-1},S_b^{N-1}} \in \bar{E}^N} \dfrac{G^{intra}(k_{S_a^{N-1}}, k_{S_b^{N-1}})}{F(h_{S_a^{N-1},S_b^{N-1}})}}, \tag{1}$$

where $\bar{E}^N$ is the set of virtual links in the graph complement of the Nth-tier initial virtual topology, and F is a cost function: $F(d) = \mathrm{e}^{d/d_x}$, where d_x is constant parameter describing a cutoff for distance constraints. For this, $k_{S_i^{N-1}}$ is the degree of S_i^{N-1}, and $h_{S_i^{N-1},S_j^{N-1}}$ denotes the shortest hop count from S_i^{N-1} to S_j^{N-1} in the graph of the Nth-tier initial virtual topology. G^{intra} is a strategy function for preferential embedding of a new link by taking the degrees of the endpoint subnetworks into account. We look into three different strategies of embedding a new link: we call the chosen strategy $intra$, and it can be one of "hh," "ll," and "hl." A pair of two higher-degree nodes is connected preferentially when $intra = \mathrm{hh}$, and a pair of two low-degree nodes is connected preferentially when $intra = \mathrm{ll}$. A higher-degree node and a lower-degree node are selected preferentially and connected when $intra = \mathrm{hl}$. Each definition of G^{intra} is as follows.

$$\begin{aligned} G^{\mathrm{hh}}(k_i, k_j) &= k_i \cdot k_j, \\ G^{\mathrm{ll}}(k_i, k_j) &= k_i^{-1} \cdot k_j^{-1}, \\ G^{\mathrm{hl}}(k_i, k_j) &= \max(k_i, k_j) \cdot |k_i - k_j|. \end{aligned}$$

Figure 1 shows one example describing which subnetworks are connected by added virtual links preferentially in respective strategies.

The number of virtual links added to the Nth tier is $\lceil C_{\mathrm{intra}}^{N} |E_0^N| \rceil$, where $|E_0^N|$ denotes the number of links existing in the graph of the Nth-tier initial virtual topology and C_{intra}^{N} denotes a constant with $0 \leq C_{\mathrm{intra}}^{N} \leq 1$.

2) Constructing a virtual link between lower-tier virtual subnetworks according to the Nth-tier virtual links: In this section, we explain how to map an Nth-tier virtual link to a virtual link between nodes. To do so, we choose the endpoints of an Nth-tier virtual link among its $(N-1)$th-

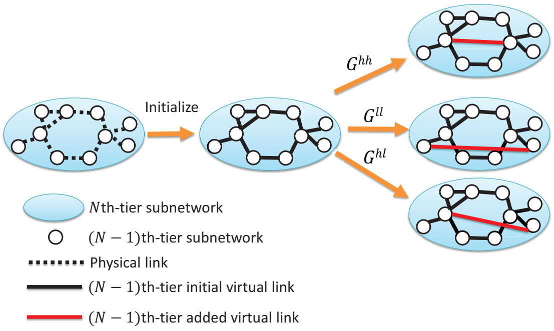

Initialize
G^{hh}
G^{ll}
G^{hl}
Nth-tier subnetwork
$(N-1)$th-tier subnetwork
Physical link
$(N-1)$th-tier initial virtual link
$(N-1)$th-tier added virtual link

Fig. 1. Example describing which subnetworks are connected by added virtual links preferentially in respective strategies

tier subnetworks and iterate this procedure until the endpoint nodes are selected.

When there is an Nth-tier virtual link between S_x^N and S_y^N, we add an $(N-1)$th-tier virtual link by choosing two endpoints from the $(N-1)$th-tier subnetworks, S_i^{N-1} and S_j^{N-1}, which satisfy $S_i^{N-1} \in S_x^N$ and $S_j^{N-1} \in S_y^N$, respectively. We assume here that the relational operator "$\in$" whose right operand is an Nth-tier subnetwork (S_x^N) means that a subnetwork denoted in its left operand belongs to S_x^N.

The probability of adding an $(N-1)$th-tier virtual link between S_i^{N-1} and S_j^{N-1} is defined as

$$p_{\text{inter}}^N(S_i^{N-1}, S_j^{N-1}) = \frac{\dfrac{G^{inter}(k_{S_i^{N-1}}, k_{S_j^{N-1}})}{F(h_{S_i^{N-1}, S_j^{N-1}})}}{\displaystyle\sum_{\substack{S_a^{N-1} \in S_x^N, \\ S_b^{N-1} \in S_y^N}} \dfrac{G^{inter}(k_{S_a^{N-1}}, k_{S_b^{N-1}})}{F(h_{S_a^{N-1}, S_b^{N-1}})}}, \tag{2}$$

where $S_x^N \neq S_y^N$, $S_i^{N-1} \in S_x^N$ and $S_j^{N-1} \in S_y^N$. G^{inter} is a strategy function for selecting endpoints S_i^{N-1} and S_j^{N-1} preferentially according to their degrees in the Nth-tier VWSN topology. We look into three different strategies of embedding a new link between subnetworks and the strategies are "HH," "LL," and "HL," with the same meanings as "hh," "ll," and "hl" mentioned above, but applied to between-subnetwork links.

Figure 2 shows one example describing which subnetworks are selected as endpoints of Nth-tier virtual link preferentially in respective strategies.

The number of virtual links for each upper-tier link is $\lceil C_{\text{inter}}^N(E^{S_x^N} + E^{S_y^N})\rceil$, where $E^{S_x^N}$ is the number of $(N-1)$th-tier virtual links embedded in Nth-tier VWSN topology of S_x^N, and C_{inter}^N denotes a constant with $0 \leq C_{\text{inter}}^N \leq 1$. A VWSN topology comprising all sensor nodes can be constructed ultimately by applying this method recursively until $N = 1$.

IV. Simulation evaluation

We evaluate our proposed method and compare it with a bio-inspired small-world network construction method (we call it bio-inspired) [10]. We briefly explain this method in

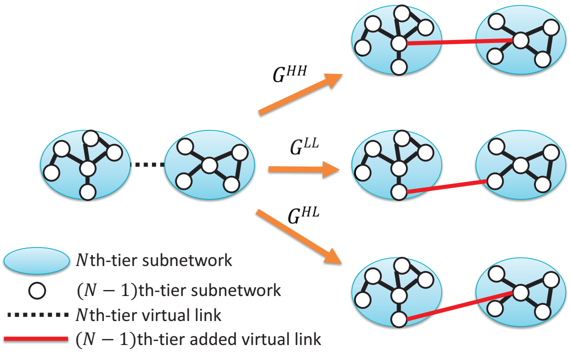


Fig. 2. Example describing which subnetworks are selected as endpoints of Nth-tier virtual link preferentially in respective strategies

Section IV-A. Our proposal, we call it the brain-inspired configuring method (BICM), has nine sets of results, resulting from choosing a combination of one of three strategies for $intra$ and one of three strategies for $inter$. To distinguish each strategy, we label each as BICM($intra$,$inter$).

A. Bio-inspired methods for attaining small-world properties

The bio-inspired method has been proposed to introduce the small-world properties to WSNs with non-uniform node density by using bio-inspired techniques [10]. Since this method is not for constructing a virtual topology, we regard the constructed topology as a virtual topology. The method consists of two steps: clustering and selecting nodes connected via long-distance links.

First, we explain the clustering algorithm, which uses a lateral inhibition technique. At the initial step, each node regards itself as a cluster head and stores its information. The information stored by node v is a combination of H_i, h_{v,H_i} and k_{H_i}. H_i is the node identifier of the cluster head of cluster i. h_{v,H_i} is the minimum hop counts from node v to H_i and k_{H_i} is the degree of H_i. Therefore, node v stores $H_i = v$, $h_{v,H_i} = 0$ and $k_{H_i} = k_v$ as default. Then, each node floods control packets which contain the stored information. Each node updates the information according to the received and stored information when it receives a control message. As an example, we assume that node w is associated with H_j, which means that it belongs to cluster j. When $k_{H_j} < k_{H_i}$ and $h_{w,H_i} < \eta$, where η restricts the maximum hop counts to the cluster head, node w changes to be associated with H_i, belongs to cluster i and updates its stored information accordingly. Further, when $k_{H_j} = k_{H_i}$ and $h_{w,H_i} < h_{w,H_j}$, node w changes to be associated with H_i and updates its stored information accordingly. When the hop counts to two different places are the same, node w randomly decides whether to keep or update the information. After this, node w floods the received packet after it increments the hop count by one. The process shown above is iterated until each node belongs to the cluster whose cluster head has the maximum degree within η hops.

Second, we explain a means of identifying nodes to be connected via long-distance links by using a flocking technique.

To efficiently decrease average path length, a peripheral node of a cluster and a centroid node of a cluster are connected by a long-distance link. A peripheral node of a cluster is a node located at the bounds of the cluster, and a centroid node of a cluster is a node whose closeness centrality is the maximum. Closeness centrality is the inverse number of the sum of the shortest hop counts from a node to all the others in the network within clusters. This is defined as

$$Closeness(v_i) = \frac{1}{\sum_{w \neq v_i, w \in C_i} sd(v_i, w)}, \tag{3}$$

where $sd(v_i, w)$ is the minimum hop count between two nodes. Centroid node c_i floods a control message in cluster i to determine the peripheral nodes of cluster i. At this time, each node in cluster i acquires the hop count to c_i. After that, a node from which the hop count to c_i is the maximum compared with its neighbors behaves as a peripheral node.

Each peripheral node v chooses the number of antenna elements ϕ at random and decides a beam width and a beam length. The value of ϕ is in range from 2 to Φ. The beam length and the beam width are given by ϕr and $\frac{2\pi}{\phi^2}$ respectively, where r is the communication range in nondirectional mode. Each peripheral node v looks for centroid nodes lying within a radius of ϕr and lists them up as a candidate of endpoints to be connected via a long-distance link. Then, peripheral node v eliminates c from the candidates on condition that a neighboring peripheral node and centroid node c are already connected. Finally, node v chooses the node to which the shortest hop count is the maximum among the candidates and a long-distance link is embedded between it and node v.

B. Evaluation metrics

We evaluate a VWSN topology in terms of small-worldness, average path length in the virtual network, average path length in the physical network, total number of virtual links, modularity, robustness of connectivity, and robustness of average path length.

In [11], the metric ω which described small-worldness of topology was proposed. ω is calculated from the clustering coefficient, that of an equivalent lattice network, average path length, and that in an equivalent random network. For this purpose, equivalence between networks indicates that they have the same degree distribution. Formally, ω is defined as

$$\omega = \frac{L_{rand}}{L} - \frac{C}{C_{latt}}, \tag{4}$$

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

We define two types of average path length, denoted by APL, APL in the virtual network (vAPL) and APL in the physical network (pAPL). The value of vAPL is APL when nodes connected by a virtual link can communicate with each other directly. The value of pAPL is APL when nodes connected by a virtual link communicate with each other via the shortest multi-hop path in the physical network. Actual APL in physical networks may change depending on a means of realizing a long-distance link in the physical network. Thus, vAPL suggests the minimum APL and pAPL suggests the maximum APL in a VWSN.

In [9], the metric Q which describes modularity was proposed. The definition of modularity is the following:

$$Q = \sum_i (e_{ii} - a_{ii}^2), \tag{5}$$

where i denotes a group identifier and e_{ii} denotes the ratio of the number of links whose endpoints belong to the same group to the total number of edges; a_{ii} is the probability that at least one of the endpoints of an uniformly randomly chosen link belongs to group i. Then, a_{ii}^2 is the expected probability that both endpoints of a link belong to the same group.

The robustness of connectivity and APL are evaluated by removing nodes one at a time. We evaluate the robustness of connectivity by comparing the decrease in component size which describes the number of nodes belonging to the maximally connected subgraph; we evaluate the robustness of APL by comparing the increase in APL. When all paths between node i and node j are lost owing to the removal of nodes, APL is calculated by looking on the hop count between them as the number of nodes. We suppose two modes of node removal: random failure and targeted attack. In the random failure mode, we randomly choose a node to be removed in the next time step. In the targeted attack mode, we choose the highest degree node to be removed in the next time step.

C. Evaluation of three-tiered VWSN topology

In this section, we evaluate a VWSN topology constructed based on the network which consists of two sensor networks and one wired link. Two sensor networks, each comprising 150 sensor nodes, are embedded in an area of size 1000×1000 m^2. For one of the two sensor networks, 150 sensor nodes are deployed at randomly chosen locations within the rectangular domain with corners, denoted in meters along the coordinates of the point (x, y), at $(0, 0)$ and $(400, 1000)$; the other 150 sensor nodes are deployed at randomly chosen locations within the rectangular domain given by $(600, 0)$ and $(1000, 1000)$. Additionally, two sensor networks are connected by one wired link whose endpoint nodes are static once selected.

In this simulation, we construct a three-tiered VWSN topology based on this physical topology and evaluate it. Table I shows the parameter settings. We use OMNeT++ [12] to perform the simulation experiments. When we use the physical topology mentioned above, the value of $E^{S_x^1} + E^{S_y^1}$ is comparatively large, and, hence, the number of virtual links embedded between first-tier modules is large; this results in low modularity. Therefore, we set C_{inter}^1 to the lower value than C_{inter}^N in the higher tier.

TABLE I
PARAMETER SETTINGS

method	parameter	value
BICM	C^N_{intra}	0.1
	$C^N_{\text{inter}}(N \neq 1)$	0.1
	C^1_{inter}	0.01
Bio-inspired	η	4
	Φ	6

1) Structural properties: In this section, we evaluate structural properties of a VWSN topology and summarize, in Table II, its small-worldness ω, vAPL, pAPL, total number of virtual links and modularity Q.

Although a BICM-based VWSN possesses small-world properties, it is comparatively lattice-like. In BICM, a means of selecting the endpoints of the inter-module links has strong effects upon vAPL and pAPL. In case of $inter$ = HH or $inter$ = HL, the vAPL of an entire network is relatively small because long-distance links are embedded between nodes with high degree. In contrast, vAPL of an entire network is relatively large in case of $inter$ = LL. A bio-inspired VWSN shows the most small-world properties because ω approximately equals zero. Moreover, though the number of virtual links is the largest, it achieves the smallest vAPL and pAPL among all the methods because of the flocking technique. Because peripheral nodes do not connect to centroid nodes to which its neighbor has already been connected, the long-distance links are dispersed all around the network. Moreover, APL is drastically reduced because a peripheral node chooses the centroid node to which the shortest hop count is the largest as an endpoint of a long-distance link.

TABLE II
COMPARISON OF VWSNS CONSTRUCTED BY EACH METHOD

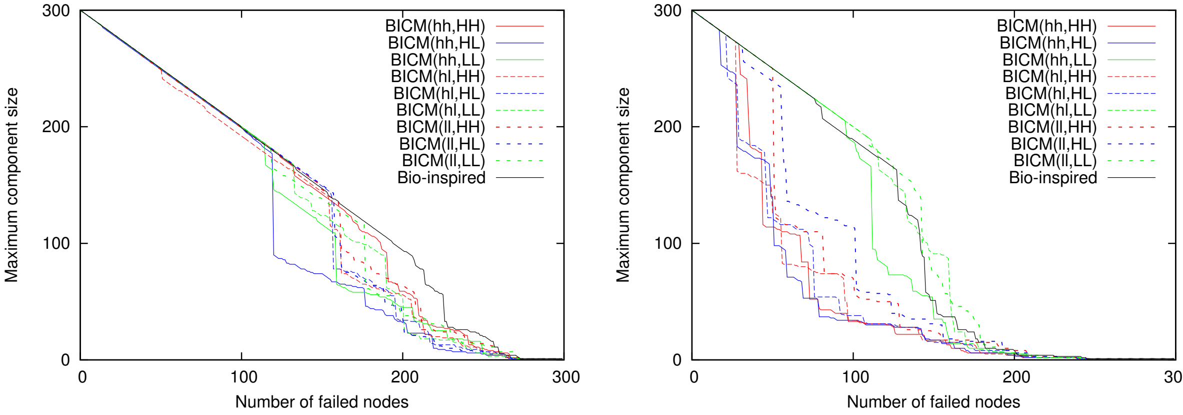
	ω	vAPL	pAPL	# of virtual links	Q
BICM(hh,HH)	-0.419	4.56	10.65	1576	0.829
BICM(hh,LL)	-0.491	5.28	13.47	1576	0.834
BICM(hh,HL)	-0.428	4.69	10.86	1577	0.831
BICM(ll,HH)	-0.403	4.71	10.11	1578	0.839
BICM(ll,LL)	-0.434	5.14	11.25	1576	0.842
BICM(ll,HL)	-0.365	4.46	11.01	1577	0.834
BICM(hl,HH)	-0.400	4.42	10.35	1578	0.834
BICM(hl,LL)	-0.410	4.80	11.74	1579	0.806
BICM(hl,HL)	-0.400	4.63	10.98	1577	0.833
Bio-inspired	-0.163	3.57	8.13	1683	0.730

2) Robustness of connectivity: The robustness of connectivity in regard to random failure and targeted attack are evaluated in this section. Figures 3a and 3b show the decrease in component size when removal modes are set to random failure and targeted attack, respectively. Note that the probability that the nodes at the end of a wired link fail is smaller than the other nodes because such nodes can charge their batteries through the wired link. From this, we suppose that the nodes at the end of a wired link do not fail.

The decrease in component size is almost the same for each method in case of random failure. In BICM, when removal mode is set to targeted attack, links between modules are removed with high probability, which may result in sharp decrease of component size. In case of $inter$ = LL, a VWSN has high robustness of connectivity because it remains the component sizes high. A VWSN constructed by the bio-inspired method also has high robustness of connectivity because the whole physical topology remains in its virtual topology.

3) Robustness of average path length: The robustness of vAPL and pAPL in regard to random failure and targeted attack are evaluated in this section. Figures 4a and 4b show the tendency toward the increase in vAPL when removal modes are set to random failure and targeted attack, respectively. In Figure 4a, sharp increase of vAPL is caused by the failure of an endpoint node of an inter-module link and the magnitude of such a jump of vAPL describes the impact of a node failure. This jump can be seen at any results of BICM and the bio-inspired method. It is noteworthy that the failure of one endpoint node of an inter-module link can cause the sharp increase of vAPL when using strategy of $inter$ = HH or $inter$ = HL. This is because long-distance links are concentrated to a small fraction of endpoint nodes of an inter-module link. On the other hand, the VWSN constructed by BICM with strategy $inter$ = LL is robust since long-distance links are decentralized. When we construct a VWSN by bio-inspired method, a pair of a centroid node and a peripheral node is connected by a long-distance link. This means that two modules are likely to be connected by two or more long-distance links, between a centroid node and a peripheral node. Therefore, vAPL increases sharply in bio-inspired method when several centroid nodes are failed. Because vAPL does not increase sharply until multiple centroid nodes fail, bio-inspired VWSN is robust of vAPL. In targeted attack, however, a BICM-based VWSN with the strategy $inter$ = HH or $inter$ = HL, or bio-inspired-based VWSN, is vulnerable on vAPL. This is because a node with high degree which is connected by inter module link is removed at an early step. When removal mode is set to targeted attack, a BICM-based VWSN with strategy $inter$ = LL is highly robust in terms of vAPL.

Figures 5a and 5b show the tendency toward increase in pAPL when removal mode is random failure and targeted attack, respectively. Robustness of pAPL of a VWSN constructed by respective method is on the same level as robustness of vAPL against random failure. A VWSN constructed by the bio-inspired method has a lower pAPL because its topology is almost the same as those of the physical network and almost all the physical shortest paths are available. On the other hand, since communication between modules is allowed only via nodes selected as endpoints of virtual links, extra hops caused by detour are more common in our proposal. When removal mode is targeted attack, a BICM-based VWSN with the strategy $inter$ = LL is highly robust in terms of pAPL. A bio-inspired VWSN has the highest robustness on pAPL in regard to targeted attack because its topology is the almost



(a) Against random failure

(b) Against targeted attack

Fig. 3. Robustness of connectivity

same as that of physical networks. From the above, BICM with the strategy $inter$ = LL is the method which achieves high robustness with regard to both vAPL and pAPL.

When we consider all results, multi-tiered VWSNs constructed by our proposed method have small-worldness, communication efficiency, robustness of connectivity, and robustness of APL. The evaluation of two-tiered VWSN topology give the same results as shown above. This suggests that the sub-networks observed at an arbitrary tier (scale level) of the VWSN constructed by our method will have similar properties.

V. Conclusions

In this paper, we proposed a method to construct a VWSN topology; this method was inspired by brain networks. Our proposal consists of three steps: dividing sensor networks into unit modules, constructing a virtual topology possessing the small-world properties in each tier, and mapping the endpoints of a virtual link to nodes. We investigate combinations of three strategies for constructing virtual links within a tier and three strategies for configuring virtual links in lower tiers on the basis of virtual links in a higher tier.

Simulation experiments showed that the strategy for configuring virtual links in lower tiers plays a significant role in the robustness and communication efficiency of the constructed VWSN topology. When no less than one of the endpoints of an inter-module long-distance link has high degree, global communication efficiency can be improved but its topology is vulnerable against targeted attack. When lower-degree nodes in different modules are selected as the endpoint nodes of a virtual long-distance link, global communication efficiency remains slightly low but all three kinds of robustness (connectivity, vAPL, and pAPL) against targeted attack are high. Comparing a VWSN topologies, a VWSN topology constructed by our method is seen to have a higher robustness of vAPL against targeted attack than a topology constructed by the bio-inspired method does.

In future work, we hope to create a protocol to configure the VWSN topology adaptively in accordance with environmental changes. Because of the modular structure, a small adjustment of a few virtual links between modules should be sufficient to achieve that.

Acknowledgment

This work was supported by a Grant-in-Aid for JSPS Fellows 26·1639.

References

[1] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: A survey," *accepted for IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, Mar. 2015.

[2] I. Ishaq, J. Hoebeke, I. Moerman, and P. Demeester, "Internet of things virtual networks: Bringing network virtualization to resource-constrained devices," in *Proceedings of IEEE International Conference on Green Computing and Communications (GreenCom)*, Nov. 2012, pp. 293–300.

[3] I. Khan, R. Jafrin, F. Zahra Errounda, R. Glitho, N. Crespi, M. Morrow, and P. Polako, "A data annotation architecture for semantic applications in virtualized wireless sensor networks," *ArXiv e-prints arXiv:1501.07139*, pp. 1–9, Jan. 2015.

[4] D. Meunier, R. Lambiotte, and E. T. Bullmore, "Modular and hierarchically modular organization of brain networks," *Frontiers in neuroscience*, vol. 4, no. 200, pp. 1–11, Dec. 2010.

[5] R. Chu, L. Gu, Y. Liu, M. Li, and X. Lu, "Sensmart: Adaptive stack management for multitasking sensor networks," *IEEE Transactions on Computers*, vol. 62, no. 1, pp. 137–150, Jan. 2013.

[6] P. Levis and D. Culler, "MatÉ: A tiny virtual machine for sensor networks," in *Proceedings of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems*. ACM, Dec. 2002, pp. 85–95.

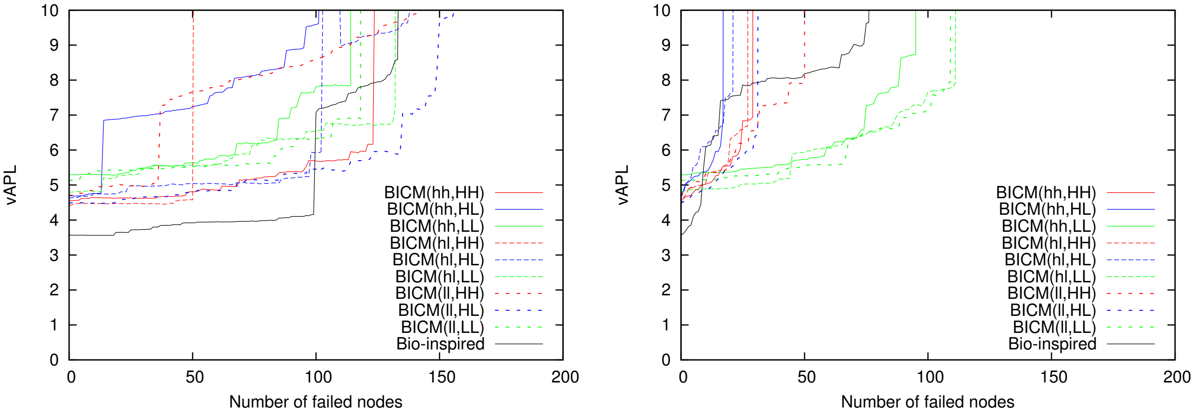
[7] C.-L. Fok, G.-C. Roman, and C. Lu, "Agilla: A mobile agent middleware for self-adaptive wireless sensor networks," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 4, no. 3, pp. 16:1–16:26, Jul. 2009.

[8] H. Bandara, A. P. Jayasumana, and T. H. Illangasekare, "A top-down clustering and cluster-tree-based routing scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2011, pp. 1–17, Mar. 2011.

[9] M. E. Newman, "Modularity and community structure in networks," *Proceedings of the National Academy of Sciences*, vol. 103, no. 23, pp. 8577–8582, Apr. 2006.

[10] 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, no. 8, pp. 909–931, Mar. 2012.

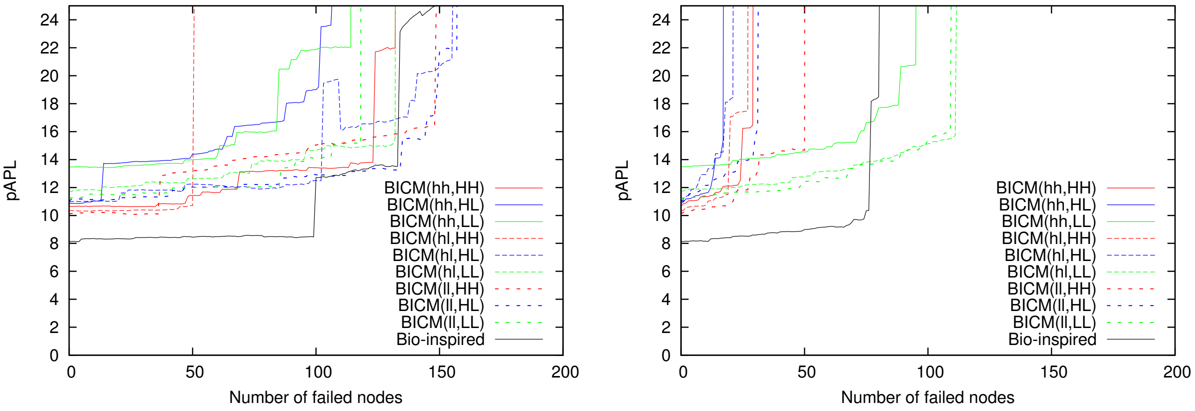
[11] Q. K. Telesford, K. E. Joyce, S. Hayasaka, J. H. Burdette, and P. J. Laurienti, "The ubiquity of small-world networks," *Brain Connectivity*, vol. 1, no. 5, pp. 367–375, Nov. 2011.



(a) Against random failure

(b) Against targeted attack

Fig. 4. Robustness of average path length in the virtual network (vAPL)



(a) Against random failure

(b) Against targeted attack

Fig. 5. Robustness of average path length in the physical network (pAPL)

[12] A. Varga, “Omnet++,” in *Modeling and Tools for Network Simulation*. Springer Berlin Heidelberg, 2010, pp. 35–59. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-12331-3_3