Effective Utilization of Centrality Schemes in Clustered Nodes of Internet of Things

Sheikh Salman Hassan, Choong Seon Hong*
Department of Computer Science and Engineering,
Kyung Hee University, Yongin, 446-701 Korea
Email: {salman0335, cshong}@khu.ac.kr

Abstract

The Internet of things (IoT) is the network where physical devices, sensors, appliances, and other various things can interact with each other without human interaction. The IoT has many sarcastic and non-sarcastic utilities which are totally emerged in latest technologies. However, there are various challenges in IoT network implementations, where proper utilization of resources is high-ranked issue. In this paper, we proposed an effective scheme of clustering in IoT network to find out the optimal sink nodes to enhance the utilization of resources in terms of increased data throughput between IoT nodes and core network. In this way, proper energy distribution for sparse network can be done according to the requirements of nodes on the basis of their data rate. Various centrality approaches are used to find out the optimal sink nodes to deploy the clustered IoT network. Numerical results are provided to show the performance of centrality approaches against the increased network size.

I. Introduction

Internet of things (IoT) is a huge domain of networking in the modern era which covers various perspectives related to the extension of the Internet and Web into the physical arena. The widespread deployment of spatially distributed devices with embedded system i.e, identification, sensing and/or actuation capabilities [1]. The accumulation of information from gadgets will permit buyers, organizations and even whole associated urban communities to run all the more effective. Be that as it may, gathering a lot of information presents challenges. Different approaches are proposed to solve the challenges of network security [2] and resource allocation where energy efficiency and bandwidth allocation has key importance [3].

In huge IoT network, mostly nodes are dealing with small amount of data i.e, wireless sensor, smart devices. In an IoT network, it is not feasible for an individual node to connect with the core network. This problem can be solved by forming the clusters in IoT nodes. To address this issue, firstly, we form a cluster of some nodes and then find the suitable sink node from that cluster to connect this cluster with the core network. Sink node can be found by using centrality techniques of graph theory. [4].

Clustering of different IoT devices like wireless sensors, wearable IoT devices, smart TV's and phone are assembled into groups and the main node of this bunch, usually called as the "group head (CH)", accumulates and transmits the detected information from various nodes in the bunch to the base station (BS) which makes the interaction of this system to the rest of the world. Typically, a good approach is that every node interacts with its neighbors only or with the cluster head node (sink node) for less energy consumption.The sink node uses more energy than other nodes because of its data transmitting power and connection with the gateway [5].

This work proposed a centrality based method to identify a node or nodes which are optimal to work as a sink node in the network topology by applying different schemes of graph theory. In our scenario, we have a cluster of nodes in the IoT network which is connected to the core network with the help of gateway. We have to find the sink nodes by applying centrality approach in cluster.

II. System Model

The system model consists of $\mathcal{N}$ number ($\mathcal{N}$=1,2,3....,40) of IoT nodes in clustered form connected with backhaul which in turn is connected to the cloud (Internet). Moreover, we also have a $\mathcal{S}$ number ($\mathcal{S}$=1,2,3) of sink nodes which belongs to set of $\mathcal{N}$ nodes. Some of the nodes are consuming very less amount of energy because of low amount of workload while other nodes are consuming high energy because of different parameters like placement in the network, connection with other nodes and data capacity.

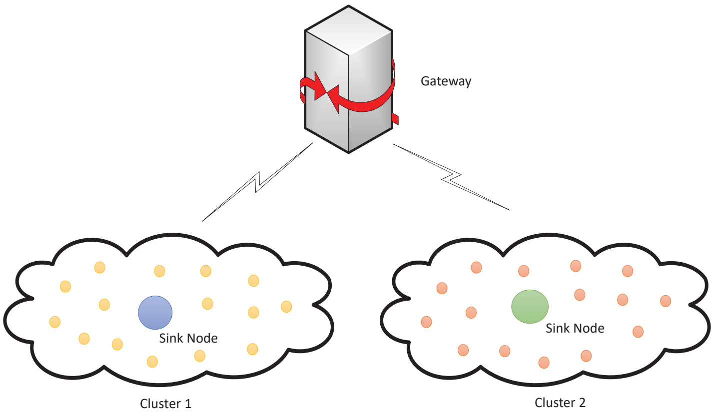

Fig. 1: System Model of IoT Nodes Network

III. Centrality-based Clustering Solution

Centrality approach is suitable to examine the optimal sink node in clustered network. The connections between different nodes and the differential significance of nodes regarding key estimations, for example, the speed of gathering of data flow and recurrence of getting data is inspected. Such information is utilized to find the centrality using different centrality approaches given as follows:

A. Degree Centrality

The main goal of this approach is to deduce the very connected individuals nodes, popular nodes, who are likely to hold most information or nodes who can quickly connect with the wider network. By applying this on a cluster, we get node counts in a network. We also get the information about the one hop neighbor of an individual node to rest of the nodes within a network. Let G (V,E) is a node network graph having vertices's (nodes, V) and edges (paths, E). Degree centrality can be found as follows:

$$C_D(G) = \frac{[\sum_{i=1}^{|V|}(C_D(v^*) - C_D(v_i))]}{H}, \quad (1)$$

where, $C_D(v)$ is the degree of centrality of a vertex v and $H = |V|^2 - 3|V| + 2$. v^* is the optimal sink node having the highest degree in network. The value of H will be maximum if graph G contains one central node connected to all others nodes of the network.

B. Betweenness Centrality

This centrality approach is different from the other centralities in a way that, it uses the approach to get information about nodes having much repetition in the paths of connecting multiple nodes, which tell us about nodes that are acting as a "bridges" between nodes in a network. First, it finds all the shortest paths and then counts how many times each node falls on that particular path. The main objective of this is to find the individual nodes who influence the flow around a system. Following is the equation of degree centrality:

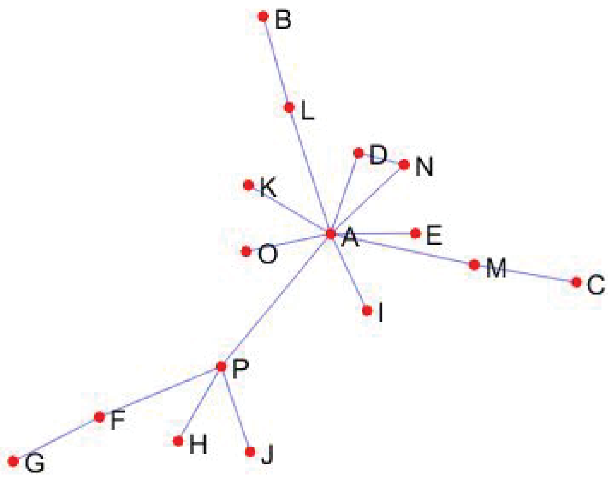

Fig. 2: Cluster of nodes

$$C_B(v) = \sum_{s \neq v \neq t \neq \in V} \frac{\sigma_s t(v)}{\sigma_s t}, \quad (2)$$

where, v is the vertex of graph $G = (V, E)$, $\sigma_s t$ is the overall count for smallest paths from node s to t and $\sigma_s t(v)$ is the count of that respective paths which pass through v.

C. Closeness Centrality

This centrality measures the closeness of a node with all other nodes of the network. This is done by finding the shortest path between all the nodes, then assigning each node a cost for the connected paths. The ultimate goal of this procedure is to deduce each and every node which are the best suitable to influence the overall network more rapidly. Following is the equation of closeness centrality:

$$C(x) = \frac{1}{\sum d_y(y, x)}, \quad (3)$$

where, $d_y(y, x)$ is the distance between vertices's x and y. For the generalization, we need to multiply above equation with $N - 1$, where N shows the count of nodes in the given graph.

We have the target to choose that optimal sink node/nodes which are most suitable in the whole topology for the communication with rest of the other network's nodes and core network. To find those particular nodes, we are applying three different schemes for finding best suitable nodes to connect with the core network with minimum energy cost. This node

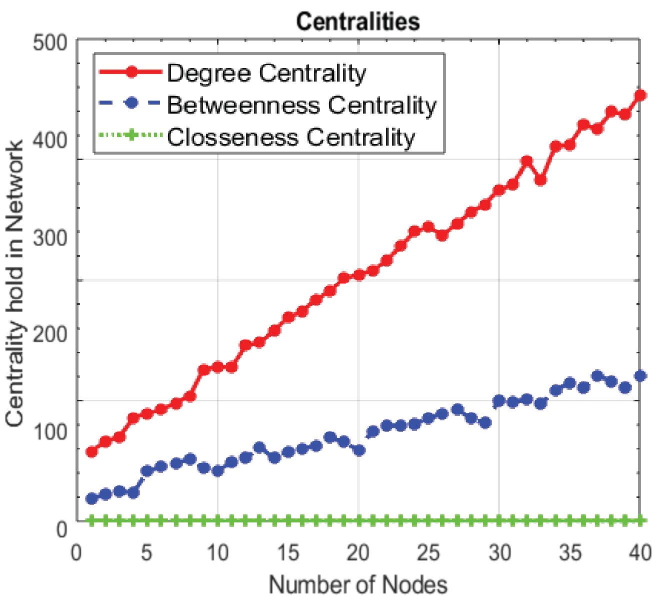

Fig. 3: The Plot of three centralities connection with nodes

is analyzed based on network requirements. For example, degree centrality is the easiest way to find node connectivity. Sometimes it is valuable to take a look at in-degree (number of inbound connections) and out-degree (number of outbound connections) as cleared measures, for instance when taking an example of value-based information or account activity. Betweenness is useful for analyzing communication dynamics. The high betweenness count indicates that the particular node holds authority over other nodes. It can also have more controls collaboration between, disparate clusters in a network, or indicates that they are on the periphery of both clusters. Closeness centrality can help to find good broadcasters, but in a highly connected network, we can find often all nodes have a similar score. The more useful thing is that we can utilize closeness to find influencer within a single cluster.

IV. Simulation

For the simulation of the system, we construct a model of the network which contained 50 nodes of IoT devices sparse in different locations within the same network. The topology which has been applied in Matlab shown in Fig. 2. The red dot represents the nodes of the IoT network and blue color lines show the edges (connection) of these nodes.

The graph generated after simulation of network showed that degree centrality has shown that we can access 92% of the network, betweenness centrality have 35% connectivity in network and closeness centrality has almost 10% network coverage. It is clearly seen that for selection of sink node for the core network connection in IoT network implementation degree centrality has optimal results.

V. Conclusion

In this paper, we presented a technique for proper clustering in IoT nodes network by finding the optimal nodes which should interact with the core network. Three types of centralities are used to find the optimal sink nodes. Simulation results show that degree centrality technique is most suitable because if the node connectivity in a system is very high then it has very high throughput. Results showed that for the selection of sink nodes in IoT network for the core network, we can choose the node which has more directly connected nodes in network.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2015-0-00567, Development of Access Technology Agnostic Next-Generation Networking Technology for Wired-Wireless Converged Networks)
*Dr. CS Hong is the corresponding author.

References

[1] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7):1497–1516, 2012.

[2] Sabah Suhail, Shashi Raj Pandey, and Choong Seon Hong. Detection of malicious node in rpl-based internet of things through provenance. , pages 1171–1173, 2018.

[3] Sabah Suhail and Choong Seon Hong. A secure provenance-aware model for internet of things. , pages 1154–1156, 2016.

[4] Hayato Nomura, Haruhisa Ichikawa, and Yuusuke Kawakita. Reference node selection for range-based localization using hierarchical clustering. In *Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on*, pages 140–143. IEEE, 2018.

[5] Shashi Raj Pandey, Sabah Suhail, Yan Kyaw Tun, and Choong Seon Hong. Resource allocation strategy for latency sensitive iot traffic. , pages 398–400, 2018.