Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 2, pp. 507–512
DOI : 10.47974/JIOS-1572

Note on placement of security nodes in graphs associated to the Internet of Things

Nader Jafari Rad *
Department of Mathematics
Shahed University
P. O. Box 3319118651
Tehran
Iran

Roslan Hasni †
Special Interest Group on Modeling and Data Analytics (SIGMDA)
Faculty of Ocean Engineering Technology and Informatics
Universiti Malaysia Terengganu
21030 Kuala Nerus
Terengganu
Malaysia

Abstract

Consider a network (graph) consisting of nodes and edges. We refer to a subset D of nodes as a dominating set or D-set if every node which is outside D, it is connected to a node inside D. If a D-set D has a further property that no pairs of nodes outside D, are connected, then we call D an outer-independent dominating set or just O-I-D-set. With the aim of deploying some security services within an IoT network, Godquin, Barbier, Gaber, Grimault and Le Bars in [J. Inf. Security Appl. 55 (2020) 102640] proposed a method employing a graph network, where they presented a formula for the protection according to some types of a D-set. The proposed formula works properly with protection 100% if the employed graph is tree, but if it is not tree then we always do not reach such rate, unless we choose the D-set such that it has a further property of absence of edges outside the D-set. In this short paper,

* *ORCID-ID:* 0000-0001-7406-1859
† *ORCID-ID:* 0000-0003-3695-2145

* *E-mail:* n.jafarirad@gmail.com (Corresponding Author)
† *E-mail:* hroslan@umt.edu.my

© Taru Publications

we propose a new formula for the protection using O-I-D-sets and we prove that all graphs reach the protection of 100% in this new setting.

Subject Classification (2010): *05C69.*

Keywords: *IoT, Security, Dominating set, Outer-independent dominating set.*

1. Introduction

In the platform of the fog computing which was introduced by Bonomi et al. [4], the nodes associated to fog are placed in at all strategic locations which lie between end-user device and the cloud. Identification of the matter related to the suitable placing for some of the edge-nodes and the placing of some of the services within them leaded to a new migration from cloud to edge. Instead of placing a security service on every device which is not realistic based on many reasons, the security services can be placed on some special nodes namely security node as devices that host a Network Security Function (NSF), and then every device in the network can communicate, directly, to a security node, [3]. Among the most important problems in IoT, is the service placement using graph models that has been received most attention by several researchers, (see for example, [1, 8, 9, 10, 12]). Besides representing IoT networks as graph models, very few researches rely on deep graph theory properties. Banerjee and Maiti in [2], used the concept of graph centrality in IoT networks. Stellios et al. [11] considered the attacker model to be suitable for network of IoT which composes of three types of categories which the first is device accessibility, the second is attacker capabilities and the third is motivations.

Recently, in 2020, Godquin et al. proposed in [5] a method which aimed to deploy some security services in a network which models an IOT, where they considered some capabilities, for example, memory and hardwares. They formalized the problem through an undirected graph $N = (V, E)$, where V, corresponds to the devices and E corresponds to devices connections. The secure nodes considered as a D-set (dominating set) in such a way that each vertex on the network is straightly joined to a secured vertex. A shortest path is called there secure if the vertices, which we call sender and receiver, are joined together or if each vertex of that pair is belong to the given D-set or connected to vertex in the D-set. Godquin et al. defined a variant as the quality of a dominating set to be the percentage of high-priority with respect to the given dominating set. Notice that the greater percentage coinsides with the higher overall quality. They presented the protection formula using a D-set in the following, by determining the percentage of all pairs of nodes of the network that satisfy at least one secured shortest path as follows.

$$P = \sum_{a,b \in V(N)} D(a,b) / \binom{n}{2} \tag{1}$$

where $D(a,b)=1$ in (1) if there is a secured shortest path from the node a to the node b, and $D(a,b)=0$ if there does not exist such path. Figure 1 demonstrates a graph with ten vertices which we darkened the vertices to belong to our D-set, (black vertices form a D-set. We see that all paths between each pair of vertices are secured.

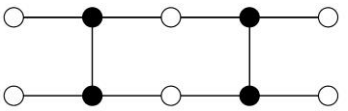


Figure 1
A D-set (Black vertices)

In this paper, we show that the protection formula (1) does not work in real if the graph is not a tree, and propose a new formula for the protection. We also prove that with our new protection formula all graphs reach the protection of 100% if we assume that the secure vertices (dominating set) form an outer-independent dominating set.

2. Graph theory notations and terminology

A graph namely N is a pair (V,E) such that $V=V(N)$ is the set of vertices (or nodes) and E as the set of edges, in which each edge associated to a pair of vertices. For a member $e=\{a,b\}$ of E, we usually say that vertices a and b are connected or adjacent. The degree of a vertex is the number of vertices that are connected with it and the degree of v we denote by $d(v)$. A path (of length k) in the N is a sequence $v_0 \dots v_k$, where each node v_i is connected to node v_{i+1}, for each $i=0,1,\dots,k-1$. The integer k in the sequence is referred as the length of such path and the nodes v_0 and v_k are called terminal or end-vertices. A cycle-graph or just cycle is a graph obtained from a path by connecting the end-vertices of the path. A graph is connected provided that there is a path between every pair of nodes. A connected graph which contains no cycle we call a tree. Trees play importantly in being a graph connected. In a network, for a subset D, we call D a dominating set or D-set subject to that every vertex not-belonging to D is connecting to some vertex which is inside D. The minimum cardinality among all possible D-sets in a network is the domination number of the network. A D-set such as D is called an outer-independent dominating set or O-I-D-set if $V(G)-S$ is an independent set, that is, there is no edge within $V(N)-S$. For mathematical properties of domination variants, the reader can consult [6, 7], where the second focuses on the outer-independent version. This version is close to vertex packing sets in graph that have various applications, as it can be easily verified that for those graphs that no degree one vertex exists, this version of domination is the same packing set.

3. New Proposed Formula

Considering the graph in Figure 1 in which the red vertices form a dominating set, the protection Formula (1) yields a protection of 204%:

$$P = \frac{\sum_{a,b\in V(N)} D(a,b)}{\binom{n}{2}} = \frac{92}{45} \times 100 = 204\%$$

which is not real and shows that the Formula 1 needs to be revisited. We observed that the Formula 1 is indeed correct if the graph is a tree, since in any tree there is precisely one path between any pair of vertices of the tree. But in the case that the graph is not a tree, there will be at least two (shortest) paths between some pairs of vertices. We propose the following new formula:

$$P = \sum_{a,b\in V(N)} D'(a,b) / \sum_{a,b\in V(N)} D(a,b) \quad (2)$$

where $D'(a,b)$ counts secured paths between a and b, and $D(a,b)$ is the number of all paths between a and b. Notice that as before a path is secured if the vertices are connected together or if each node among that pair is either belong to D-set or adjacent to one vertex of D-set. Now the protection according to Formula 2 on the graph of Figure 1 is as follows:

$$P = \frac{\sum_{a,b\in V(N)} D\prime(a,b)}{\sum_{a,b\in V(N)} D(a,b)} = \frac{92}{92} \times 100 = 100\%.$$

According to our calculations, there are 92 secured paths and the total number of paths is also equal to 92, which means that all graph paths are secured. So according to Formula (2), the amount of graph protection is equal to 100%. We have examined Formula (2) on all graphs, which gives us an understandable and correct answer. In the following, we prove that if the security nodes form an O-I-D-set, then the protection value according to the Formula (2) is always 100%.

Theorem 1: *If N is an n-vertex graph and D is an O-I-D-set graph, then the protection based on Formula (2) is 100%.*

Proof: Let N be an n-vertex graph and D be an O-I-D-set. For any vertex x outside D, all of neighbors of x belong to D. This implies that each path between two vertices a and b is secured. Consequently, $\sum_{a,b\in V(N)} D'(a,b)$ and $\sum_{a,b\in V(N)} D(a,b)$ are equal, and thus the protection is 100%.

Since every two distinct O-I-D-sets give equal protections of 100%, we obtain the following result.

Theorem 2: *The protection based on the O-I-D-sets is independent with respect to the choice of the O-I-D-sets.*

As conclusion, we thus have proposed a new formula for the protection, namely, Formula (2), which uses an O-I-D-set, and as we have shown in Theorem 1, its gives us 100% protection. Furthermore, any O-I-D-set gives us the desired protection, as it was shown in Theorem 2.

References

[1] J. Ahamed, M. Zahid, M. Omar, and K. Ahmad, "AES and MQTT based security system in the internet of things," *J. Discrete Math. Sci. Cryptogr.,* vol. 22, pp. 1589–1598 (2019).

[2] P. S. Banerjee and B. Maiti, "Optimality criterion for the insertion of multi-interface nodes to improve connectivity in heterogeneous IoT framework," in Proc. 2017 Devices for Integrated Circuit (DevIC), *IEEE*, pp. 556–560 (2017).

[3] L. R. Battula, "Network Security Function Virtualization (NSFV) towards Cloud computing with NFV Over Openflow infrastructure: Challenges and novel approaches," in Proc. 2014 Int. Conf. Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, pp. 1622–1628 (2014).

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. 1st MCC Workshop on Mobile Cloud Computing, ACM, pp. 13–16 (2012).

[5] T. Godquin, M. Barbier, C. Gaber, J.-L. Grimault, and J.-M. Le Bars, "Applied graph theory to security: A qualitative placement of security solutions within IoT networks," *J. Inf. Secur. Appl.,* vol. 55, p. 102640 (2020).

[6] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, Fundamentals of Domination in Graphs. Boca Raton, FL, USA: CRC Press (1998).

[7] M. Krzywkowski, "An upper bound on the 2-outer-independent domination number of a tree," *C. R. Math. Acad. Sci. Paris,* vol. 349, pp. 1123–1125 (2011).

[8] R. Sharma, P. Jindal, and B. Singh, "Study and analysis of key generation techniques in internet of things," *J. Discrete Math. Sci. Cryptogr.,* vol. 23, pp. 373–383 (2020).

[9] O. Skarlat, M. Nardelli, S. Schulte, M. Borkowski, and P. Leitner, "Optimized IoT service placement in the fog," *Serv. Oriented Comput. Appl.* (SOCA), vol. 11, pp. 427–443 (2017).

[10] O. Skarlat, M. Nardelli, S. Schulte, and S. Dustdar, "Towards QoS-aware fog service placement," in Proc. 2017 IEEE 1st Int. Conf. Fog and Edge Computing (ICFEC), *IEEE*, pp. 89–96 (2017).

[11] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.,* vol. 20, no. 4, pp. 3453–3495 (2018).

[12] Y. Xia, X. Etchevers, L. Letondeur, T. Coupaye, and F. Desprez, "Combining hardware nodes and software components ordering-based heuristics for optimizing the placement of distributed IoT applications in the fog," in Proc. 33rd Annu. ACM Symp. *Applied Computing* (SAC '18), ACM Press, pp. 751–760 (2018).

Received September, 2023