Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 on line
SPM: www.spm.uem.br/bspm

(3s.) **v. 2023 (41)** : 1–6.
ISSN-0037-8712 in press
doi:10.5269/bspm.51446

Graph Modelling of Social Internet of Things $(S - IoT)$ centered Home Automation using Medium Domination Approach

Aaysha Khan and Jana Shafi

ABSTRACT: Preceding years predict Internet of Things (IoT) to be trend in technology domain as it possesses superior intelligence and methods to access data as well able to construct networks anywhere which we are witnessing today. Today IoT devices are well implemented and are a topic and product of interest for many. In midst of this Social Internet of Things $(S - IoT)$ emerged which is understood as the added ingredient in IoT networks enables improvement in accessing data, its procession, real time decisions and many more new functions and all of this with ideal price [1]. Social Internet of Things $(S - IoT)$ led to the interesting development of enabling Internet of things to be socially connected in network with each other which permits them to socially interact with each other and have their respective profiles for their identification all similar to humans. This magical innovation led internet networks to be more complicated. In this paper we are modelling objects of $(S - IoT)$ centered homes as network graphs with medium domination number approach. The key notion here is to inspect the total number of objects connected that dominate every pair of objects in a network graph and average value of this is defined as "the medium domination number". We evaluated new results and relations along with further vulnerability methods and developed an algorithm of complexity $O(n_2)$.

Key Words: Home and building automation, internet of things, social web of things, medium domination, graphs, $(S - IoT)$.

Contents

1. INTRODUCTION

Today lives get benefitted from (IoT) technology but at the same time it is also a source of barriers and complexity for designers, developers of tele-communication systems and applications unless new models are developed and implemented. It is well believed that the social methodology in (IoT) will accomplish the requirements of developers, users, and designers [2].The Social Internet of Things $(S - IoT)$ model's objectives are: to divide people and things in two classes; to permit objects to build their own social networks; to agree humans to execute procedures to guard their confidentiality and allow to only access the outcome of self-governing inter-object communications happening in social network. In human's vision extremely intelligent smart objects may not be recognized effective rather than of social objects which withdraw more attention [3].The $(S - IoT)$ model allows users to manage and access internet-enabled objects and also authorizes the user to share these objects with other users [4]. Social Network Sites rise in popularity with Web 2.0 technology and has been extended by an interactive and open web services for social relation among people and their internet of things [5]. Presently, Social Internet of

Submitted December 15, 2019. Published April 19, 2020

Typeset by $\mathcal{B}^{S}\mathcal{P}_{\mathcal{M}}$style.
© Soc. Paran. de Mat.

things understood as a merging model of Social Network Sites (SNS) and IoT. The notion is to fetch Social Networking Sites facilities and structures, for instance social graphs into an integrated system [6]. A network paradigm as a graph has vertices signify the classes and edges represent the relation among the vertices. In the concept of graph, few stability methods have been considered broadly such as edge connectivity, connectivity, tenacity, vertex covering, integrity and domination. These factors take consideration into the zone of edges and vertices. In a theory of graph each vertex is skilled of guarding all vertices in its neighborhood as well in domination each vertex is essential to be secured [7]. In a network of communication, if there is interruption on any vertex and line, it lost its efficiency. Usually, modeled graph networks are more stable which are preferred in network plan. Vulnerability value of a communication network is the network resistance to interruption of few vertices until communication of network failure [7]. We inspect relations among other vulnerability procedures and graph medium domination number.

2. SOCIAL OBJECT CONSTRUCTION

As we know that today humans are connected with each other with the help of social networks similarly objects are also now constitutes in social network [8]. Social objects similar humans grounded as co-work object relationship and co-location object relationship which are established as a part of the initialization and implementation of a “location-based application” profile or a “situation-based application” profile. Regular Changes are classically based on the time duration of co-location or co-working and communication/reputation, frequency [9-10].

3. MACHINE TO MACHINE INTEGRATION: ($S-IoT$) Based Home Automation

Now days, wireless sensor networks (WSN) have been widely used in HBA (home and building automation) setting. It is used to refer with various terms such as intelligent buildings, Smart Homes, integrated home systems. The objective of HBA is to extend automated on-off operations with different types of control , monitoring and communication between smart devices. It permits influencing machine-to-machine (M2M) emerging technologies in executing on big measure automation. The interaction which occurs among machines without human interference or may be including humans is known as machine-type-communication (MTC). Currently, machine-to-machine M2M has emerged as the key feature in IoT which predicts smart objects inter-connection through the world anywhere anytime. These smart objects exemplified as mobile phones, tablets, RFID tags, computers, and sensors which in common share and exchange detected data. Further, different Wireless sensor networks (WSNs) are compulsory to communicate with each other awhile connected which leads to the heterogeneous form of network assigning each object unique Internet protocol (IP) address.

4. METHOD AND RESULTS

4.1. $S-IoT$ centered Home automation

The IoT model in which objects or devices are intelligently design such that they are able to restricted, obtain data, practice and exchange them as a Smart Home or Smart Building is a vibrant application chiefly in the development of IoT, as they enable connections among individual (citizen, consumer) and covering layers of IoT concepts approval (Smart City, Smart Grid) [11, 12].Conversely, objects act wisely builds a network, accomplish tasks via sensors. These devices sense their particular jobs and communicate with other devices if required which extend their networks. These networks effect in groups with same kind of interests etc., see, [10].

4.2. Medium Domination

In a communication network, if there is a disruption on some vertices and lines, it loses its effectiveness. Generally, a network can be modeled by a graph. A more stable model is preferred in network design. Vulnerability value of a communication network is the resistance of network to disruption of some vertices until communication of network breakdown. A graph G is denoted by $G = (V, E)$ where V and E are vertices and edges sets of G respectively. The length of a shortest $u-v$ path in a connected G is called the distance from a vertex u to a vertex v. It is denoted by (u, v) [13]. Two u-paths are said to be internally disjoint if they have no common vertex, other than u and v. The degree of a vertex V in a graph G is defined as the number of edges incident on v and is denoted by (v). A set$S \subseteq G$ is a dominating set if every vertex in $V - S$ is adjacent to a vertex in S. The minimum cardinality of a dominating set S is called dominating number of G and is denoted by (G). There are the many parameters of domination number such as connected, independent and total domination numbers [14]. The connected domination number (G) is the minimum cardinality of a connected dominating set [7]. The medium domination number of a graph.

For any connected, undirected simple graph, the medium domination number is a notion which uses neighborhood of each pair of vertices. In this paper, we examine how many vertices are capable of dominating both u and v. We will calculate total number of vertices that dominate all pairs of vertices and then evaluate the average of this value and it is called "the medium domination number" of graph, see, [15]. Here the number of vertices that dominate both of u and v is denoted by $dom(u, v)$. We will use the medium domination number as a new vulnerability measure to check the stability of a connected, undirected, simple graph G based on $S - IOT$ smart home.

Definition 4.1. *For $G = (V, E)$ and $\forall u, v \in V$; if u and v are adjacent they dominate each other, then at least $dom(u, v) = 1$.*

Definition 4.2. *For $G = (V, E)$ and $\forall u, v \in V$; the total number of vertices that dominate every pair of vertices is defined as*

$$TDV(G) = \sum dom(u, v), \forall u, v \in V(G).$$

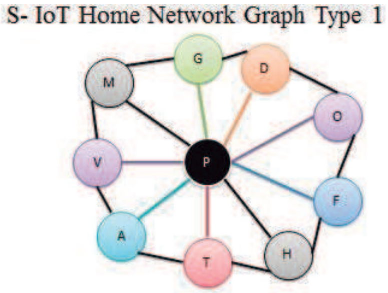
Definition 4.3. *For any connected, undirected, simple graph G of order n, the medium domination number of G is defined as*

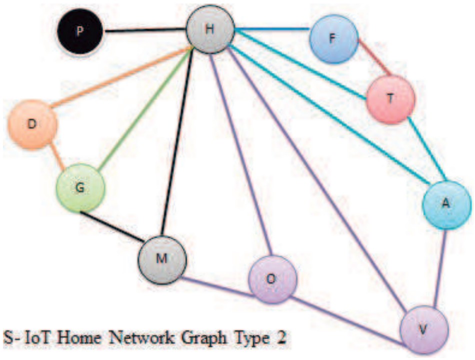
$$MD(G) = \frac{TVD(G_2)}{\binom{n}{k}}$$

4.3. Modelling of Social Internet of Things $S - IoT$ based Home Automation as Graphs

$S - IoT$ based home automation networks can be modeled as graphs of connected (edges) smart objects (vertices) with each other. In the graphs, the regular smart appliances are considered as vertices and connection of them depicts the edges. Two different kinds of $S - IoT$ based home automation network graphs are examined and evaluated in accordance with Medium Domination approach. G_1 and G_2 that have the same number of vertices and connectivity are shown in Figure 2.1.

The connectivity of the two networks graph is slightly different where in the first graph house owner or person in charge is directly connected to all the objects as well all the objects also connected to each other in such a way that suppose the vertex v_1 is directly connected to its adjacent vertices v_2 and v_3 as well with the P (person). The second graph depicts the indirect involvement of person in charge or owner with house devices as it handovers the full control to the home systems which is automatically controlling other devices of course with the consent of the owner. The resultant graph is isolating the P (person) connection with other devices except the home system, as H is all over connected. The other devices are connected in the same way as seen in the earlier graph.





S- IoT Home Network Graph Type 2

Table 1: S-IoT based home automation graph vertices

Abbreviations
A = Air Condition
D = Door
H = Home System
G = Geyser
F = Refrigerator
M = Music Player O = Oven
P = Person or house owner
T = Television
V = Vacuum Cleaner

4.4. Medium Domination Evaluation

Now, both the graphs are evaluated with medium domination approach to find out most secured graph networks among them.

Table 2: S-IoT based home automation graph vertices

Graph 1 Evaluation
For graph 1: dom(M,P)= 3, dom(M,G)=2, dom(M,D)=2, dom(M,O)=1, dom(M,F)=1, dom(M,H)=1, dom(M,T)=1, dom(M,A)=2, dom(M,V)=2, dom(GP)=3, dom(GD)=2, dom(G,O)=2, dom(G,F)=1, dom(G,H)=1, dom(G,T)=1, dom(G,A)=1, dom(G,V)=2, dom(D,P)=3, dom(D,O)=2, dom(D,F)=2, dom(D,H)=1, dom(D,T)=1, dom(D,A)=1, dom(D,V)=1, dom(O,P)=3, dom(O,F)=2, dom(O,H)=2, dom(O,T)=1, dom(O,A)=1, dom(O,V)=1, dom(F,P)=3, dom(F,H)=2, dom(F,T)=2, dom(F,A)=1, dom(F,V)=1, dom(H,P)=3, dom(H,T)=2, dom(H,A)=2, dom(H,V)=1, dom(T,P)=3, dom(T,A)=2, dom(T,V)=2, dom(A,P)=3, dom(A,V)=2, dom(V,P)=3

$$TVD = \sum (u,v) = 75. \tag{4.1}$$

$$MD(G_1) = TVD(G_1)/\binom{n}{2} = 75/\binom{10}{2} = 1.66 \tag{4.2}$$

Graph 2 Evaluation
For graph 2:dom(P,H)=1, dom(P,F)=1, dom(P,T)=1, dom(P,A)=1, dom(P,V)=1, dom(P,O)=1, dom(P,M)=1, dom(P,G)=1, dom(P,D)=1, dom(H,F)=2, dom(H,T)=3, dom(H,A)=3, dom(H,V)=3, dom(H,O)=3, dom(H,M)=3, dom(H,G)=3, dom(H,D)=3, dom(F,T)=2, dom(F,A)=2, dom(F,V)=1, dom(F,O)=1, dom(F,M)=1, dom(F,G)=1, dom(F,D)=1, dom(T,A)=2, dom(T,V)=2, dom(T,O)=1, dom(T,M)=1, dom(T,G)=1, dom(T,D)=1, dom(A,V)=2, dom(A,O)=2, dom(A,M)=1, dom(A,G)=1, dom(A,D)=1, dom(V,O)=2, dom(V,M)=2, dom(V,G)=1, dom(V,D)=1, dom(O,M)=2, dom(O,G)=2, dom(O,D)=1, dom(M.G)=2, dom(M,D)=2, dom(G,D)=2

$$TVD = \sum(u,v) = 73 \tag{4.3}$$

$$MD(G_1) = TVD(G_1)/\binom{n}{2} = 75/\binom{10}{2} = 1.62 \tag{4.4}$$

5. DISCUSSION

As of the domination definition all the networks which can be considered as graph of vertices and edges implies that neighboring vertices are protecting every vertex in the network. Some medium domination number definitions and theorem of a graph are also discussed. In this search, the key notions is each $s, t \in V$ (vertices) must be sheltered and are able to calculate the vertices number that are capable of dominating together s and t (vertices). In this paper, $S - IoT$ led home automation two unlike network graph's total number of smart objects (vertices) that dominate every pair of vertices is tested, the average value is calculated and result is compared with the high medium domination number of both graphs. An algorithm for the retrieval of medium domination number of a graph also computed with $O(n2)$ time complexity.

Acknowledgements. Authors are very thankful to the Deanship of Scientific Research, Prince Sattam bin Abdulaziz University for supporting this work.

References

1. D. Dutta, C. Tazivazvino, S. Das and B.K. Tripathy, Social Internet of Things ($SIoT$): Transforming smart object to social object, (2015).

2. http://www.social-iot.org/

3. J. Shafi, A. Waheed and P. V. Krishna, Investigating Recommender Systems in OSNs. In: Social Network Forensics, Cyber Security, and Machine Learning. SpringerBriefs in Applied Sciences and Technology. Springer, Singapore, (2019).

4. A. Ciortea, O. Boissier, A. Zimmermann and A. M. Florea, "Reconsidering the social web of things," position paper. In Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication (UbiComp '13 Adjunct), (2013).

5. A. Kamilaris, D. Papadiomidous and A. Pitsillides, "Lessons Learned from Online Social Networking of Physical Things," 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp.128,135, 26-28 Oct.2011

6. T. Y. Chung, I. Mashal, O. Alsaryrah, V. Huy, W.-H. Kuo and D. P. Agrawal, Social Web of Things: A Survey, 19th IEEE International Conference on Parallel and Distributed Systems, DOI:10.1109/icpads.2013.102, (2013).

7. D. Vargör and P. Dundar, The medium domination number of a graph, International Journal of Pure and Applied Mathematics, 70(3), 297–306, (2011).

8. L. Atzori, A. Iera and G. Morabito, $SIoT$: Giving a Social Structure to the Internet of Things, IEEE Communications Letters, 15(11), 1193–1195, (2011).

9. J. Shafi and A. Waheed, "$SIoT$: A new platform for Online Social Networks Using IoT," 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, 2018, pp. 1–6. doi: 10.1109/CAIS.2018.8441970

10. N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of Computer Mediated Communication, 13(1), 210–230, (2007).

11. K. Musia and P. Kazienko, "Social networks on the internet," World Wide Web 16.1, 31–72, (2013).

12. F. Buckley and F. Harary, Distance in Graphs, Addison Wesley Pub. California, (1990).

13. P. Dündar and N. Tackın, Domination and Total Domination Number of Graphs, Master Thesis, Faculty of Science, Ege University (2006).

Aaysha Khan
Department of Mathematics,
Prince Sattam bin Abdulaziz University,
Alkharj, KSA.
E-mail address: a.aysha@psau.edu.sa

and

Jana Shafi (Corresponding Author)
Department of Computer Science,
Prince Sattam bin Abdulaziz University,
Alkharj, KSA.
E-mail address: j.jana@psau.edu.sa