Journal of Ambient Intelligence and Humanized Computing (2022) 13:3765–3770
https://doi.org/10.1007/s12652-022-03730-2

ORIGINAL RESEARCH

Application of graph domination to defend medical information networks against cyber threats

D. Angel[1]

Received: 31 March 2020 / Accepted: 19 January 2022 / Published online: 7 February 2022

Abstract
The principal and supreme concern in medical information systems is the issue of safe guarding the electronic health records of patients. Defending a health care industry's computer network against attacks on its nodes and links requires placing mobile guards on the nodes of a network. Bloom graph topologies are attractive networks that are potential structures for massively parallel computers. This article focuses on the computation of exact value of the parameters which gives the minimum number of guards required to protect the bloom networks with a linear time algorithm. This research highlights the benefits of locating domination sets in locating the minimum number of detection devices or cyber security employees (mobile guards) to be deployed on the significant servers (nodes) of the bloom's topology (healthcare network) which is essential for securing the network to fight against cyber threats.

Keywords Graph theory · Locating domination · Edge cover · Bloom networks

1 Introduction and background

The health care industry is often the most targeted and attacked hosts by cyber criminals. On March 13, the Brno University Hospital which is a key Covid-19 testing site in the Czech Republic, immediately shutdown all computers as a cyberattack took hold. Czech hospital is not the only medical institution to be targeted by cybercriminals as the novel coronavirus has spread around the world. As the total number of global cases of Covid-19 has swelled above 250,000, hackers have increased their activity as they look to capitalise on the crisis (Burgess 2020). The huge need for e -records of health of patients in the illegal market is intensifying the number of cyber attacks that have destroyed the prestige and funds of health care institutions. Consequently, it is fundamental to curb medical cyber piracy and secure the network infrastructure that supports them (Fernández-Alemán et al. 2013).

Cyberspace can be expressed mathematically using graph theory since the basic structure of a graph is applicable to the interconnected world of computer networks. Nodes can be associated with various types of hardware or virtual systems as well as routers and other internet infrastructure, and edges can represent connections or information flow between nodes (Mahapatra et al. 2020; Dawood 2014). In cybersecurity, a graph-based approach can benefit security operations teams to increase performance and capability by establishing a system of record and intelligence used to inform future threats (Maida 2018).

Strategies for protection of a graph $G = (V, E)$ by placing one or more guards at every vertex of a subset S of V, where a guard at v can protect any vertex in its closed neighborhood have resulted in the study of several graphs domination parameters such as location and secure domination. concept of locating dominating set was introduced and first studied by Slater and secure domination was initiated by Cockayne et al. Various aspects of location and secure domination problems and properties of a graph have been studied in the literature and is shown to be not polynomially solvable (Cockayne et al. 2005). Secure dominating sets can be considered as processors (nodes) from which the information of the patient can be passed on securely to all other processors (nodes) of the system which could be accessed by medical practitioner remotely and the patient and their family but not by hackers (see Fig. 2). This can be accompolished by just monitoring the nodes present in the minimum secure dominating set. Another protection strategy called the locating

✉ D. Angel
angel.zara1001@gmail.com

[1] Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, India

domination problem which also non-polynomially solvable, is concerned with the protection of vertices of G, using one guard per vertex and require the set of guarded vertices to be a locating domination and this is essential to locate the position of the faulty vertices (Weigt and Zhou 2006; Angel et al. 2021).

Most hospitals do not have the resources to monitor threats to their systems, and many might not even be aware that they are something to be concerned about (Coventry and Branley 2018). Compounding the issue, the vast majority of hospitals don't have full-time cybersecurity employees. Small, rural hospitals in underserved communities, probably don't have the money to hire staff or update their systems. Without security staff, they might not be aware of or able to implement security updates announced by a device company (Wetsman 2019). The lack of awareness and lack of resources is the motivation to build robust cybersecurity programs having the ability to detect network activity and pointing to an intrusion attempt on the server so that the system administrator can take appropriate measures in time.

Most malware protection and detection hardware or software is equipped with logging capability used to identify suspicious activity. These softwares monitors the firewall logs to detect a scan or attack on the server, and then can alert administrators or take proactive steps to contain the threat. One can also consider hiring a cybersecurity professional to review the logs for any red-flag trends, such as high frequency of viruses consistently found on a single computer.

A worm is a malware which is transmitted through insecure networks, e-mail attachments, software downloads, and social media links. The combinatorial topology of routing may have a huge impact on the worm propagation and thus some servers play a more essential and significant role than others. Identifying these nodes (servers) are essential to greatly hinder worm propagation. The idea is to find a minimum vertex cover in the graph whose vertices are the routing servers and whose edges are the connections between routing servers. This is the best solution for worm propagation and an exact solution for designing the network defense strategy (Armbruster et al. 2007).

Security and privacy in e-records can be seriously threatened by hackers, viruses, and worms (Fernández-Alemán et al. 2013) (see Fig. 1). If the networks are not rightly monitored at the organizational level, it can undoubtedly jeopardize the kind of care, given to patients. Because of the risks that accompany poorly monitored healthcare IT networks it is essential that healthcare industries should be assisted with a extensible network monitoring solution.

Bloom networks can be considered as healthcare systems (data structures), are interesting in and of themselves as they are both planar and regular which make them particularly attractive as potential structures for massively parallel computers (see Fig. 2). Motivated by the grid, cylinder and torus networks, Antony et al. (2016), introduced the definition of bloom graph. The bloom graphs are very reliable networks as their vertex connectivity equals the degree of regularity.

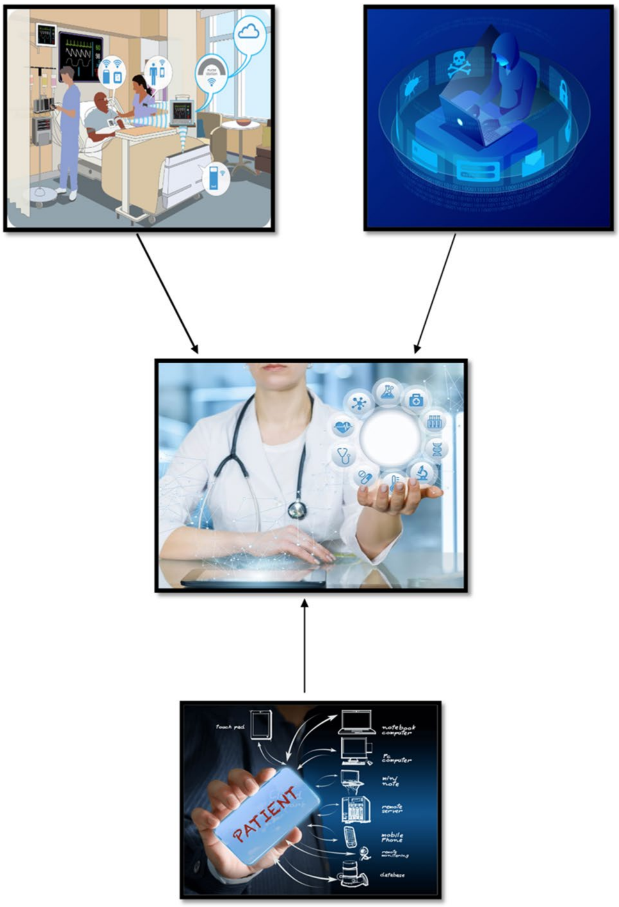

Fig. 1 Accessing and hacking health care system

Fig. 2 Bloom's architecture representing healthcare system

In this paper, the problem of using mobile guards to defend the nodes of a graph $G = (V, E)$ (network) against a single attack on its vertices (nodes) and edges (links) is studied. This study is beneficial in locating the minimum number of detection devices or cyber security employees (mobile guards) to be deployed on the significant servers (nodes) of the bloom's architecture (health centres) which is essential for defending the network against a single malware attack.

2 Preliminaries

A graph $G = (V, E)$ consists of nonempty set of vertices (or nodes) and E, a set of edges. Each edge has either one or two vertices associated with it, called its endpoints. An edge is said to connect its endpoints. In a graph G, a set $S \subseteq V$ is secure in G if every attack on S is defendable. The set $S \subseteq V$ is a dominating set in G if every vertex in G not in S has a neighbor in S. The domination number of G denoted by $\gamma(G) = min\{|S| : S$is a dominating set of G$\}$. A secure dominating set in G is a set $S \subseteq V$ that is both a secure set in G and also a dominating set inG. The secure domination number of G is $\gamma s(G) = min\{|S| : S$is secure dominating set$\}$. For a graph in Fig. 3, $\gamma s(G) = 3$. This protection strategy defends the vertices of a graph against a single attack on its vertices.

A set of edges of G is called an edge cover if that set covers all the vertices in G. The cardinality of the minimum edge cover set is called the edge covering number denoted by $\beta'(G)$. Finding the minimum edge cover is called the edge covering problem (Eze et al. 2020). Edge covers can be applied in network analysis. Another area where the edge covering number plays a role is the traffic phasing problem. A perfect matching M in G is a maximum number of non-adjacent edges with the property that every vertex is incident with an edge of the matching. M is always a minimum edge cover. For the graph in Fig. 7, the minimum edge cover set is given by S where, S is the set containing the thicker edges.

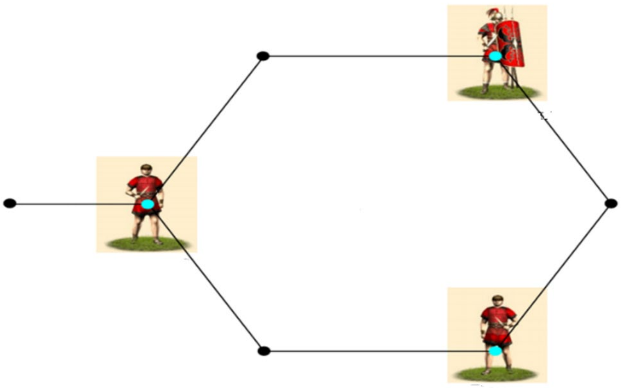

Fig. 3 A graph with $\gamma_L(G) = \gamma s(G) = 3$

A locating dominating (LD) set of a graph G is a dominating set S of G such that for every two vertices u and v in $V(G) - S$ such that $N(u) \cap S \neq N(v) \cap S$. The locating domination number γ_L(G) is the lowest cardinality of a LD set of G (Angel et al. 2021). For a graph in Fig. 3, γ_L(G) = 3. As seen from the example below in Fig. 3, secure domination and locating domination sets mitigates the security issues in any health care system infra structure or topology.

3 The bloom architecture

The bloom network denoted by $B_{m,n}$, where $m, n > 2$ is defined in [1]. For example, the grid view of bloom networks $B_{3,6}$ and the flower view of $B_{3,6}$ are shown in Figs. 4 and 5 respectively and the flower view of bloom network $B_{4,6}$ is shown in Fig. 6. Antony et al. (2016) identified these new topological representation for bloom networks showed that these representations are isomorphic.

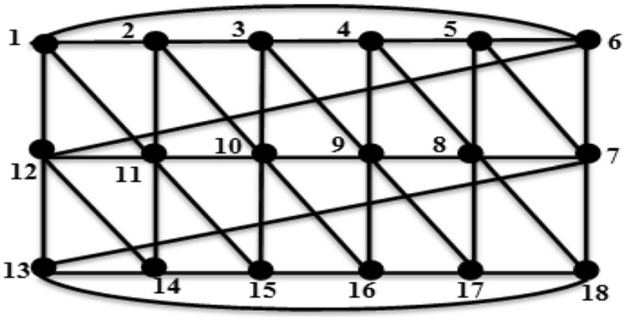

Fig. 4 Grid view of $B_{3,6}$

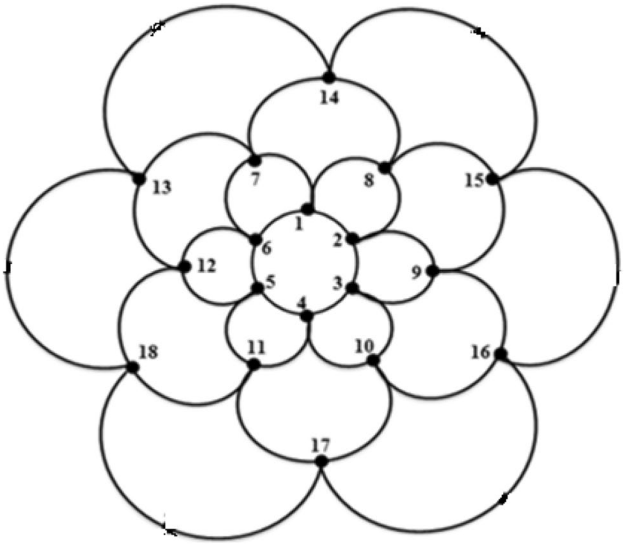

Fig. 5 Flower view of $B_{3,6}$

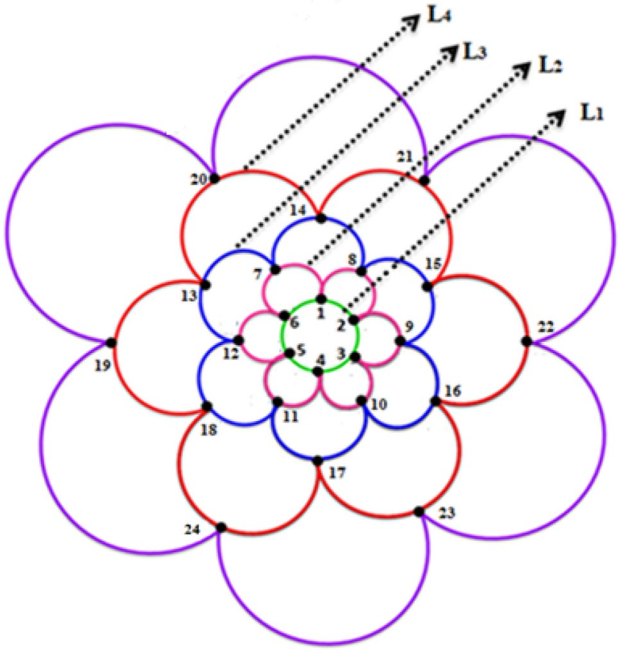

Fig. 6 Flower view of $B_{4,6}$

First and foremost an algorithm for solving the locating dominating set problem for bloom networks is constructed which works on the flower-like structure. To explain the flower structure of bloom networks, $B_{4,6}$ is considered as an example. From Fig. 6, the inner most cycle which is at the center of $B_{4,6}$ colored in green is a cycle of length 6 denoted by C_6. Call all those cliques of length 3 on top of C_6 colored pink, as petals. These n petals together with the center C_6 is called a floret (pink and green colored edges and the vertices on them) and is denoted by f_6 (see Fig. 6). All the vertices in level i, where $1 \le i \le m$ are denoted by L_i.

3.1 Locating domination for bloom $B_{m,n}$

In this section a linear time algorithm for finding the locating dominating set of bloom graph is presented. Denote by L_i, the vertices in level i, where $1 \le i \le m$. Let S_1 denote $\lceil \frac{n}{2} \rceil$ number of alternate vertices in the level L_1 and v_j denotes any vertex in the level L_j.

3.1.1 Algorithm LD-$B_{m,n}$

To find a locating dominating set of a bloom graph.
Input: A bloom graph $G = B_{m,n}$ where $m > 2, n > 2$.
Output: A LD set S of G.

```
Initialization: $S = \phi; i = 1$
while $(i < m)$ do
$S = S \cup v_j$
$i = i + 1$
end while
$S = S \cup S_1$
Stop
```

The proof of correctness of the algorithm is given by the following theorem.

Theorem 3.1.2 *If* $B_{m,n}$ *is a bloom graph then*, $\gamma_L(B_{m,n}) = \lceil \frac{n}{2} \rceil + (m-1)$.

Proof Let G be the bloom graph $B_{m,n}$ and let S be a locating dominating set of G.

Let the value of m be even or odd. To cover vertices on floret f_n, $\lceil \frac{n}{2} \rceil$ vertices on C_n are chosen. That is, $\lceil \frac{n}{2} \rceil$ number of L_1 vertices are required to cover all the vertices of f_n. Since all L_2 vertices are already dominated by L_1 vertices, we choose one vertex from each level. Since there are m levels, we choose one vertex from each of the $m-1$ levels except L_1, as $\lceil \frac{n}{2} \rceil$ vertices are already chosen from the first level. Thus the set S will contain the vertices on levels $L_1, L_2, L_3, \ldots, L_m$. Adding all the vertices in S, the LD number is $\lceil \frac{n}{2} \rceil + (m-1)$.

Suppose if S is not minimum. Then there exists a LD set D which is minimum. If this is the case, then leaving out a single vertex in any level L_i from the set S will contradict the LD set property and so S will not be a LD set. Therefore, S should to be minimum.

Location problems examine the ability to pinpoint the origin of an event. The nodes in a γ_L- set can be used for safe gaurding the nodes of the network and to locate defective nodes in that network (Majeed et al. 2019). Now, if the minimum edges, covers(domninates) all the nodes then it becomes edge covering. In the following section an edge covering set which covers nodes of a graph, is obtained for the bloom networks.

Theorem 3.1.3 *If* $B_{m,n}$ *be a bloom graph, then*,

$$\beta'(B_{m,n}) = \begin{cases} \frac{mn}{2}, \textit{if either m or n is even} \\ \lceil \frac{mn}{2} \rceil, \textit{if m and n are odd} \end{cases}$$

Proof Let $B_{m,n}$ be a bloom graph. Case (i): If either m or n is even. Then mn is even. Since G contains even number of vertices, we conclude that G has a perfect matching. This perfect matching is a minimum edge cover for G. Hence $\beta'(B_{m,n}) = \frac{mn}{2}$. Case (ii): If both m and n are odd. Then mn is odd. Since G contains odd number of vertices, we conclude that G has a near perfect matching (Fig. 7). Therefore, $\beta'(B_{m,n}) = \frac{mn+1}{2} = \lceil \frac{mn}{2} \rceil$.

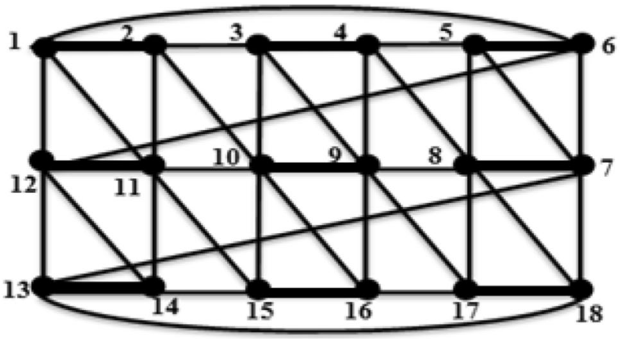

Fig. 7 Thick edges represent the edge cover of $B_{3,6}$

3.2 Secure domination for bloom $B_{m,n}$

In this section a linear time algorithm for finding the minimum secure dominating set of bloom graph is given. Denote by L_i, the n number of vertices present in level i, where $1 \le i \le m$. Let S denote secure dominating set (SDS) of $B_{m,n}$ (Fig. 8).

3.2.1 Algorithm SDS-$B_{m,n}$

To find a minimum secure dominating set of a bloom graph.

Input: A bloom graph $G = B_{m,n}$ where $m > 2$, $n > 2$.

Output: A SDS set S of G.

```
1.  Initialization: $S = \phi$; $i = 1$
2.  If $mn$ is even then
3.      while ($i = m$) do
4.          $S = S \cup L_i$
5.          $i = i + 1$
6.      end while
7.  end if
8.  goto step 15
9.  If $mn$ is odd then
10.     while ($i \le m$) do
11.         $S = S \cup L_i$
12.         $i = i + 1$
13.     end while
14. endif
15. stop
```

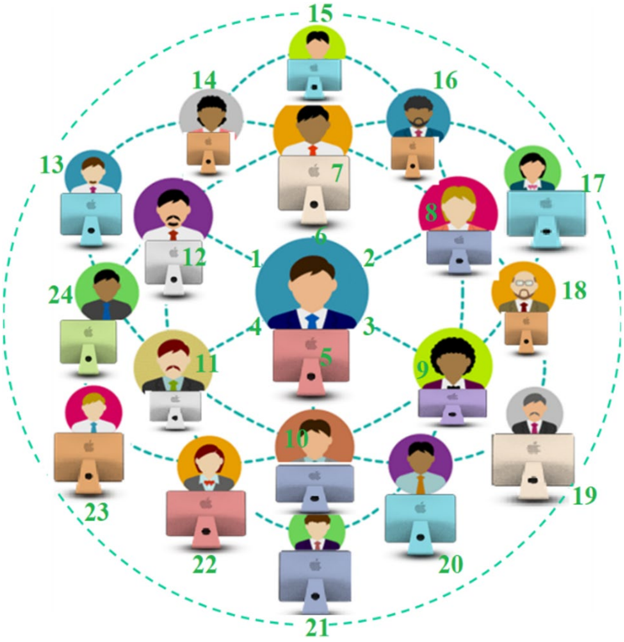

Fig. 8 $\gamma s(B_{4,6}) = 12$

The proof of correctness of the algorithm is given by the following theorem.

Theorem 3.2.2 *If* $B_{m,n}$ *is a bloom graph then,* $\gamma s(B_{m,n}) = \begin{cases} \frac{mn}{2} & \text{if } mn \text{ is even} \\ n\lceil \frac{m}{2} \rceil & \text{if } mn \text{ is odd.} \end{cases}$

Proof Let $G = B_{m,n}$ be a bloom graph and S be a minimum secure dominating set of G.

Case 1: mn is even.

In level 1, all the n vertices are selected. These n vertices will securely dominate both level 1 and level 2 vertices. In level 3, n vertices are chosen. These n vertices will securely dominate both level 3 and level 4 vertices. Similarly proceeding for $\frac{m}{2}$ number of alternate levels, that is, selecting n from alternate levels till the level m, $\gamma s(B_{m,n}) = \frac{mn}{2}$.

Case 2: mn is odd.

In this case, m and n both should be odd. In each level select n vertices. There are $\lceil \frac{m}{2} \rceil$ number of alternate levels. Therefore, selecting n number of vertices from $\lceil \frac{m}{2} \rceil$ alternate levels, $\gamma s(B_{m,n}) = n\lceil \frac{m}{2} \rceil$.

Suppose if S is not minimum then, there exists another secure dominating set S which is minimum. If this is the case, then leaving out a single vertex in any level L_i from the set S will leave the vertices unsecured and so S will not be a secure dominating set. Therefore, S should be of mimimum cardinality.

4 An application of the proposed algorithm

Graphical structures like bloom graphs $G = (V, E)$ are significant to model a health care centre network with each vertex in V representing an area in the health care centre hub in a computer network, or processor in a computer system. Each edge in E denotes connections such as adjacent hubs or rooms in a health care centre network or adjacent processors in a system. Consider an example of $B_{4,6}$ as shown in Fig. 8. Each vertex in the graph or hubs in the health care network is a potential location for a hacker or a cyber-criminal to attack the health care computer network.

Mobile guards or detection sensors are to be positioned at certain vertices or locations, provided by the proposed algorithm to defend the health care centres from hackers (intruders). Placing the mobile guards at the locations given by the secure dominating set S defends the network for a single attack and this is accomplished with the minimum number of twelve guards or sensors for this twenty four vertices network (refer Fig. 8).

A detection sensor at a vertex v given by the LD set can detect intruders in adjacent areas and as well as vertex v. Therefore, if a mobile guard is positioned at vertex v, then that guard or the sensor can detect an attacker or intruder in $N[v]$. To have some fault-tolerance in the system, it is also assumed that only detection devices that are in the closed neighbourhood of the intruder vertex can report, so there can be no false alarms. Placing the mobile guards at the locations given by the location dominating set S defends the network for a single attack and this is accomplished with the minimum resources.

5 Conclusion

The primary purpose of this paper is to propose that graph theory can be significantly applied in cyber security. In today's healthcare world, most patient's medical records are electronic, and those systems need to be monitored and maintained. But if a hospital's network is not being well monitored then they impact patient care or confidentiality and can lead to lackluster healthcare. This article promotes the novel idea of applying graph theory for network monitoring in maintaining the security of patient information. The location domination, secure domination and edge cover problems in graphs are solved for blooms architecture and is shown that this research is beneficial in the security of health care systems. This research will also help minimize problems which frustrate and compromise the efficiency of overworked cyber security staff whose time is so valuable. This study can be extended to evaluate several other domination parameters such as roman domination, secure vertex cover domination and double domination for bloom networks and for topologies which are similar to bloom architecures.

Acknowledgements The authors are highly grateful to all the reviewers for their valuable comments and suggestions to improve the quality of the article.

References

Angel D, Arputhamary IA, Ezhilarasi K (2021) Location domination for generalized friendship graphs analytics. In: Proceedings of the 5th international conference on computing methodologies and communication, ICCMC 2021, pp 865–868, 9418258

Antony XD, Rosary M, Thomas E, Arokiaraj A (2016) Broadcasting in bloom graph. Int J Math Soft Comput 6(2):57–64

Armbruster B, Cole Smith J, Park K (2007) A packet filter placement problem with application to defense against spoofed denial of service attacks. Eur J Oper Res 176(2):1283–1292

Burgess M (2020) Hackers are targeting hospitals crippled by coronavirus, Security, Hackers are targeting hospitals crippled by coronavirus, WIRED UK

Cockayne EJ, Gründlingh WR, Grobler P, Munganga J (2005) Protection of a graph. Utilitas Mathematica 67:1–15

Coventry L, Branley D (2018) Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113:48–52

Dawood Harith A (2014) Graph theory and cyber security. In: 3rd international conference on advanced computer science applications and technologies

Eze B, Kuziemsky C, Peyton L (2020) A configurable identity matching algorithm for community care management. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-019-01252-y

Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A (2013) Security and privacy in electronic health records: a systematic literature review. J Biomed Inform 46:541–562

Mahapatra T, Ghorai G, Pal M (2020) Fuzzy fractional coloring of fuzzy graph with its application. J Ambient Intell Humaniz Comput 11:5771–5784

Maida L (2018) How graph theory makes sense of overwhelming security data, Uplevel Security

Majeed A, urRasool R, Ahmad F, Alam M, Javaid N (2019) Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-018-0936-7

Weigt M, Zhou H (2006) Message passing for vertex covers. Phys Rev E. https://doi.org/10.1103/PhysRevE.74.046110

Wetsman N (2019) Health Care's Huge Cybersecurity Problem, Science