Protection of Medical Information Systems Against Cyber Attacks: A Graph Theoretical Approach

D. Angel

Accepted: 29 May 2022 / Published online: 21 June 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Securing electronic health records of patients is the paramount concern in medical information systems which faces unique set of challenges. Safeguarding a health care’s computer network against attacks on its nodes and links requires placing mobile guards on the nodes of a network. Bloom topologies are attractive networks that are potential structures for massively parallel computers. This paper focuses on the evaluation of exact value of the parameters which gives the minimum number of guards required to protect the bloom networks. A linear time algorithm is proposed for finding these parameters. 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 (healthcare system) which is essential for defending the network against a single malware attack by network monitoring.

Keywords Secure domination · Vertex cover · Bloom’s topology · Healthcare

1 Introduction and Background

Cyber criminals contemporaneously have been putting a bullseye on the health care industry especially after the pandemic covid-19. The virtual violation catastrophe has become a very serious threat to the health care that many of hospitals in West Virginia and Ohio have revoked medical procedures and diverted ambulances following a ransomware attack that laid out staff access to information systems [3]. These are not the only health care institutions which were focussed by the hackers during the pandemic. Since the number of world wide occurrence of covid-19 has raised above 250,000, cyber criminals have expanded their endeavour as they seek to take advantage on the crisis [17].

The extensive demand in the illegal market for electronic health records of a patient is aggravating the number of virtual attacks and this has resulted in the destruction of the reputation and wealth of the medical institutions. Therefore, it is vital to suppress health care cyber piracy and protect the network infrastructure that supports them [9].

* D. Angel
angel.zara1001@gmail.com

1 Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, India
Mathematically, graph theory can be used to represent cyberspace, because the unde-
lying structure of a graph is pertinent to the global interconnected network of comput-
ers. Vertices are related with different kinds of hardware or virtual systems, routers and
other internet infrastructure and edges are used to express connections or information flow
between vertices [14]. In cybersecurity, a graph-based approach is significant for security
operation groups to improve the performance and capability by establishing a system of
record and intelligence to avoid forthcoming hazards. [15].

The procedure to secure a graph $G = (V, E)$ by placing one or more guards at every node
of a subset $S$ of $V$, where a guard at $v$ can secure any node in its closed neighborhood have
resulted in the study of several graphs domination parameters such as secure domination
and vertex cover. The concept of secure domination was initiated by Cockayne et al. Various
aspects of secure domination problem and properties of the secure domination number
of a graph have been studied in the literature and is shown to be not polynomially solvable
[11]. Secure dominating sets can be considered as processors (vertices) from which the
information of the patient can be passed on securely to all other processors (vertices) of the
system which could be accessed by medical practitioner remotely and the patient and their
family but not by hackers (see Fig. 1). This can be accomplished by just monitoring the
nodes present in the minimum secure dominating set. Another protection strategy called
the vertex cover problem which also non-polynomially solvable, is concerned with the pro-
tection of edges of $G$, using one guard per vertex and require the set of guarded vertices to
be a vertex cover [5, 12, 6.

Many health care institutions do not possess the support system to monitor the dangers
to their systems, and the worst part is that they are not even aware that these are things to
be bothered about [8]. The real problem is that, many hospitals are not possessing cyberse-
curity employees who work in full-time. The hospitals in rural communities, mostly suffer
because of shortage of funds to update their systems and recruit full time labourers. The
lack of awareness and shortage of resources is the inspiration to create potent cybersecurity
schemes with the tendency to detect network activity and an intrusion endeavor on the
server so that the system administrator can take pertinent preventive actions quickly.

A malware called worm has the possibility to get transferred through not protected
networks, e-mail attachments, software downloads, and social media links. The com-
binatorial topology of routing may have a big bang on the worm propagation and thus
some servers possess a more vital and significant role than others. Identifying these
nodes(servers) are important to vastly impede 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 [10].
Security and privacy in EHRs can be seriously threatened by hackers, viruses, and worms [9] (see Fig. 2). 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 information systems, it is essential that healthcare industries should be assisted with an 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 especially fascinating as potential structures for massively parallel computers (see Fig. 1). Antony Xavier et al. in 2014, first studied bloom graph from the motivation from the grid, cylinder and torus networks [16]. Since the bloom graphs satisfy the property that their vertex connectivity equals the degree of regularity, these are found to be very reliable networks.

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.

Fig. 2 Bloom’s architecture representing healthcare system
2 Preliminaries

A graph $G = (V, E)$ consists of non-empty set of nodes (or vertices) and $E$, a set of links (or edges) where the edges are ordered pairs of vertices. 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 $\gamma(G) = \min\{|S| : S\text{ is a dominating set of } G\}$. A secure dominating set in $G$ is a set $S \subseteq V$ which is both a secure set and also a dominating set in $G$. The secure domination number of $G$ is $\gamma_s(G) = \min\{|S| : S\text{ is secure dominating set}\}$ [2, 4]. 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 vertex cover of a graph $G$ is a set $S \subseteq V$ such that for each edge $uv \in E$, at least one of $u$ or $v$ is in $S$ [1, 6, 7]. The minimum vertex cover is the minimum cardinality of a subset $S$ of vertices such that all the edges are covered by those vertices in the set $S$ called the covering number of $G$ denoted by $\beta(G)$. For a graph in Fig. 3, $\beta(G) = 3$.

As seen from the example below in Fig. 3, secure domination and vertex cover sets mitigates the security issues in any health care system infra structure or topology.
3 Bloom Topology

The Bloom Graph $B_{m,n}$, where $m, n > 2$ is defined in [1]. For example, the grid view of bloom graphs $B_{4,8}$ and the flower view of $B_{4,86}$ are shown in Figs. 4 and 5 respectively.
and the flower view of bloom graph $B_{4,6}$ is shown in Fig. 6. Antony Xavier et al. identified these new topological representation for bloom graphs showed that these representations are isomorphic [16].

First and foremost an algorithm for solving the minimum vertex cover set problem for bloom graphs 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 innermost 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 $1 \leq i \leq m$ are denoted by $L_i$.

### 3.1 Vertex Cover for Bloom $B_{m,n}$

In this section a linear time algorithm for finding the minimum vertex cover set of bloom graph is presented. Denote by $L_i$, the vertices in level $i$, where $1 \leq i \leq m$. Let $S_1$ denote $\frac{n}{2}$ number of alternate vertices in the level $L_m$.

#### 3.1.1 Algorithm MVC-$B_{m,n}$

To find a minimum vertex cover set of a bloom graph.

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

**Output:** A MVC set $S$ of $G$.

1. Initialization: $S = \phi$; $i = 1$
2. If $m$ is even then
3. while ($i < m$) do
4. $S = S \cup L_i$
5. $i = i + 2$
6. end while
7. end if
8. goto step 16
9. If $m$ is odd then
10. while ($i < m$ ) do
11. $S = S \cup L_i$
12. $i = i + 2$
13. $S = S \cup S_1$
14. end while
15. endif
16. 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, $\beta(B_{m,n}) = \begin{cases} n \lfloor \frac{m}{2} \rfloor + \lfloor \frac{n}{2} \rfloor, & \text{if } m \text{ is odd.} \\ n \lfloor \frac{m}{2} + 1 \rfloor, & \text{if } m \text{ is even.} \end{cases}$

**Proof** Let $G$ be the bloom graph $B_{m,n}$ and let $S$ be a minimum vertex covering set of $G$. 

© Springer
Case (i): If \( m \) is odd. To cover vertices and edges on floret \( f_n \), \( n \) vertices on \( C_n \) are chosen. That is, \( n \) number of \( L_1 \) vertices are required to cover all the edges of \( f_n \). Since all \( L_2 \) edges are already covered by \( L_1 \) vertices, choose all \( n \) number of \( L_3 \) vertices which covers all \( L_3 \) and \( L_4 \) edges. Proceeding in this way, up to \( \left\lfloor \frac{m}{2} \right\rfloor \) times, all edges except the level \( L_{m+2} \) edges are covered. Now, to cover \( L_{m+2} \) edges, \( \left\lfloor \frac{n}{2} \right\rfloor \) vertices are required. So clearly the set \( S \) will contain the vertices on levels \( L_1, L_3, L_5, \ldots, \left\lfloor \frac{m}{2} \right\rfloor \) and \( \left\lfloor \frac{n}{2} \right\rfloor \) number of \( L_{m+2} \) vertices. Adding all the vertices in \( S \), the covering number as \( n \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor \).

Case (ii): If \( m \) is even. To cover vertices and edges on floret \( f_n \), \( n \) vertices on \( C_n \) are chosen. That is, \( n \) number of \( L_1 \) vertices, are required to cover all the edges of \( f_n \). Since all \( L_2 \) edges are already covered by \( L_1 \) vertices, all \( n \) number of \( L_3 \) vertices are chosen to cover all \( L_3 \) and \( L_4 \) edges. Proceeding in this way, up to \( \frac{m}{2} + 1 \) times, all edges of the graph covered. Thus the set \( S \) will contain the vertices on levels \( L_1, L_3, L_5, \ldots, \left\lfloor \frac{m}{2} \right\rfloor \). Adding all the vertices in \( S \), the covering number as \( n \left( \frac{m}{2} + 1 \right) \).

Suppose if \( S \) is not minimum. Then there exists a covering 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 leave the edges uncovered and so \( S \) will not be a covering set. Therefore, \( S \) should to be the MVC set.

The vertices in a \( \beta - \) set can be used for protecting the links of the network, since every communication link will be under the coverage of one or more nodes. Thus the monitoring of these minimum number of nodes is the backbone to secure all the links of the health care system [13]. It is seen that, vertex cover sets are those nodes which cover(dominate) all the links in a network. Now, if the minimum nodes, covers(dominates) all the nodes instead of links in a network, then it becomes domination. In the following section, a variation in the domination parameter of a network, that is, dominating set with an additional condition, is obtained for the bloom networks.

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 \( 1 \leq i \leq m \). Let \( S \) denote secure dominating set (SDS) of \( B_{m,n} \).

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: \( S = \emptyset \); \( i = 1 \)
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 \((i \leq m)\) do
11. \(S = S \cup L_i\)
12. \(i = i + 1\)
13. end while
14. endif
15. stop

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, \(\gamma_s(B_{m,n}) = \begin{cases} \frac{mn}{2} & \text{if } mn \text{ is even} \\ \left\lfloor \frac{m}{2} \right\rfloor n & \text{if } mn \text{ is odd}. \end{cases}\)

**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 \(\left\lfloor \frac{m}{2} \right\rfloor\) number of alternate levels. Therefore, selecting \(n\) number of vertices from \(\left\lfloor \frac{m}{2} \right\rfloor\) alternate levels, \(\gamma_s(B_{m,n}) = n\left\lfloor \frac{m}{2} \right\rfloor\).

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 minimum cardinality.

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 resources.

**4 Limitations**

The algorithm proposed in this article for solving the problems of secure domination and vertex cover runs in polynomial time and is therefore significant as there are no existing algorithms in literature to obtain the exact solution for a Bloom’s network. However, if the structure of the network is arbitrary then the proposed algorithm may not be successful. This is because of the fact that these problems are NP Complete for any arbitrary network. Hence, this approach can be useful to solve these problems on specific graph classes.

**5 Conclusion**

The main intention of this paper is to propose that graph theory can be significantly applied in cyber security. In today’s healthcare world, most patient’s hospital 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 secure domination and vertex 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.

Funding  This study was not funded by anyone.

Declarations

Conflict of interest  On behalf of all authors, the corresponding author states that there is no conflict of interest.

Ethical approval  This article does not contain any studies with human participants performed by any of the authors.

References

1. Quan, C., & Guo, P. (2021). A local search method based on edge age strategy for minimum vertex cover problem in massive graphs. *Expert Systems with Applications, 182*, 115185.

2. Hernández-Ortiz, R., Montejano, L. P., & Rodríguez-Velázquez, J. A. (2021). Secure domination in rooted product graphs. *Journal of Combinatorial Optimization, 41*, 401–413. https://doi.org/10.1007/s10878-020-00679-w

3. Bilyeau, N. (2021). Newest Target of Cyber Attacks: America’s Hospitals The Crime Report, [https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/](https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/).

4. Chithra, M. R., & Menon, M. K. (2020). Secure domination of honeycomb networks. *Journal of Combinatorial Optimization, 40*, 98–109.

5. Hasudungan, R., Pangestuty, D. M., Latifah, A. J., & Rudiman, (2019). Solving minimum vertex cover problem using DNA computing. *Journal of Physics: Conference Series, 1361*, 012038. https://doi.org/10.1088/1742-6596/1361/1/012038

6. Angel, D. (2019). A graph theoretical approach for node covering in tree based architectures and its application to bioinformatics. *Network Modeling Analysis in Health Informatics and Bioinformatics, Springer*. [https://doi.org/10.1007/s13721-019-0193-5](https://doi.org/10.1007/s13721-019-0193-5)

7. Angel, D., & Amutha, A. (2017). On covering the nodes of circulant networks and its applications. *Wireless Personal Communications, Springer, 94*, 2163–2172.

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

9. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*, 541–562.

10. Benjamin Armbruster, J., Smith, C., & Park, K. (2007). A packet filter placement problem with application to defense against spoofed denial of service attacks. *European Journal of Operational Research, 176*(2), 1283–1292.

11. Cockayne, E. J., Gründlingh, W. R., Grobler, P., & Munganga, J. (2005). Protection of a graph. *Utilitas Mathematica, 67*, 1–15.

12. Weigt, M., & Zhou, H. (2006). Message passing for vertex covers. *Physical Review E*. [https://doi.org/10.1103/PhysRevE.74.046110](https://doi.org/10.1103/PhysRevE.74.046110)

13. Majeed, A., Rasool, R. U., Ahmad, F., Alam, M., & Javaid, N. (2019). Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. *Journal of Ambient Intelligence and Humanized Computing*. [https://doi.org/10.1007/s12652-018-0936-7](https://doi.org/10.1007/s12652-018-0936-7)

14. Harith A. Dawood (2014). Graph Theory and Cyber Security. In: 3rd International Conference on Advanced Computer Science Applications and Technologies.
15. Angel, D. (2022). Application of graph domination to defend medical information networks against cyber threats. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-022-03730-2

16. Antony, X. D., Rosary, M., Thomas, E., & Arokiaraj, A. (2016). Broadcasting in Bloom Graph. *International Journal of Mathematics and Soft Computing*, 6(2), 57–64.

17. Matt, B. (2020) Hackers are targeting hospitals crippled by coronavirus, Security. *Hackers are targeting hospitals crippled by coronavirus, WIRED UK*.

**Publisher’s Note**  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

---

**D. Angel** is an Assistant Professor in the department of Mathematics, Sathyabama Institute of Science and Technology, Chennai. She has received her doctorate degree from Sathyabama Institute of Science and Technology, Chennai in 2019. She received her M.Sc., M.Phil. degree in Mathematics from Madras Christian College, Chennai in 2005. She is currently guiding two research scholars in Graph Theory. She has presented papers in International Conferences held in Indonesia and China and so far 20 publications are indexed in Scopus and Web of Science. Her research area includes Graph Theory and Networks.