ISSN 2063-5346

EVALUATION OF COMPUTER NETWORK SECURITY USING ATTACK UNDIRECTED GEOGRAPHY

Madhumita Ghosh

Article History: Received: 01.02.2023 **Revised:** 07.03.2023 **Accepted:** 10.04.2023

Abstract

To secure a wealth of data traversing the computer network at your fingertips is compulsory. But when attack arises at various parts of the network it is difficult to protect, especially when each incident is investigated separately. Geography is a necessary construct in computer networks. The analytics of geography algorithms and metrics to curate insight from a security problem are a critical method of analysis for computer systems. A geography-based representation is employed to highlight aspects (on a local and global level) of a security problem which are Eigenvalue, eccentricity, clustering coefficient and cliques. Network security model based on attack undirected geography (AUG) is familiarized. First, analysis based upon association rules is presented then the attack threshold value is set from AUG. The probability of an individual attack edge and associated network nodes are computed in order to quantify the security threat. The simulation is exploited to validate that results are effective

Assistant Professor, Department of Geography, Kalinga University, Raipur, Chhattisgarh

Email – madhumita.ghosh@kalingauniversity.ac.in

DOI: 10.48047/ecb/2023.12.s1.081

INTRODUCTION

Security maneuver is primarily a data curation problemin which incident data in concurrence with human operations to develop infrastructure robustness over time is led. Geography in the digital form of *gml* file, in mathematics, is the concept of graph study which is designed to structure associations between nodes, connection lines, and vertices. In computer network security, a method based on geography focuses on the context of security incidences by graphing network components and data stream. To extract security context based upon geography concept helps renovate the mentality of incident responders from regular process- driven operation to progressive data analytics. Not to mention it can improve efficiency and help secure day- to-day operations by inaugurating an intelligent system to prevent future attacks. A system with more context to individual well-known attack contributes analysts an informal association of how current's attack relates to historical incidences or the upcoming one. It is appropriate to audit the security system and swap outdated ones with advanced analytics. Data security using biometric authentication approach over cloud computing network has been recommended in. Recently, the analysis of security alerts using network coding in wireless communication. With the increasing demand on the use of technology, it develops more and more important to protect online information. Network security has steadily become one of the critical tools for leveraging the computer systems. Analysis by incident experts is time-consuming and it is difficult to store up-to-date security information for network nodes. A risk assessment model based on attack graph has been introduced in. A model adopts agents and risk association analysis into the design. Attack graph algorithm is used to collect security information dynamically. The graph to assess the overall risk of any networks can be computed. Attack route, risk index, and hostname are attained in order to quantify risk assessment at a particular network node. The experimental results show the effectiveness and validation of the model. Once security warnings are inspected and taken into account as isolated, independent incidences, security analysts encounter how to determine patterns and relations in order to identify the associations and source of the attack. In many problems, incident data analysts collected is unstructured and not warehoused in a fashion that avails for automation network has been presented in. However, the latency reduction, the improved quality of the wireless connection and the increased throughput are main objectives of the research. There have been several types of research based on network coding for the improvement of network efficiency in wireless environments. The network coding reflects the advantage of increased throughput and efficiency as it can handle higher traffic than the conventional network.

Security can be monitoring as a basic requirement for any computer networks as described in. The traffic graph concept has been introduced and used to help identify the network structure. From the point of the adjacency matrix, potential risks are assessed and the attack is allocated. Multiple attacks and steps are also traced in case of the critical situation. The approaches based on a general graph concept [8-12] focus on medical images, human life, network security traffic and transportation. In order to monitor real-time based network traffic, the system needs a reliable scheduling mechanism as mentioned in. The connection analysis and traffic flow of routing mechanism have been proposed by. But the set of connection can only be applied to the static wireless network. The distributed network coding-aware routing which tolerates packets from two directional flows is encrypted as suggested in. In this paper, network security is evaluated by employing the attack associated with the undirected geography. Related to this, the digital geography which is undirected graph is adapted to analyze the attack based on network security metrics. It becomes more effective if security metrics tend to concentrate on individual network nodes but longer latency and queues. Thus, the analysis is not a good application for time-sensitive services like multimedia or big data. Moreover, once an intermediate router gets an acknowledged packet then it has to relay and these results in augmented delay.

The research centers on evaluating the computer network security based on the attack records from undirected geography. All metrics generated by AUG are considered for security issue. First, the computer network has been geographer to compute all relevant parameters. Second, assumptions for the attack model are set, and these variables are used to calculate for the possibility of attacks. Lastly, results and analysis are discussed in order to remark the future research recommendation

DIRECTED AND UNDIRECTED GEOGRAPHY

Directed Geography Model

A digital geography can be mathematically constructed by two components: a set of vertices and linked by edges. In order to model a computer network to a geography representation, it is to consider the network topology and the link (connection) per se. In general, computer nodes are geographer to symbolize devices structured in the network environments while edges represent communication channels for the information flow. Edges also direct the flow of the traffic between nodes. A geography called directed geography consisting of no various edges nor self-loop (diagonally zeroed out in an adjacency matrix).

Undirected Geography Model

The dissimilarity between an undirected and a directed geography is that the undirected geography becomes a strongly connected one. It is more apparent if the road in the city or all streets are not single directions. If the streets are well connected, then from any part of the city to others can be accessible.

Undirected edges are strongly connected but not well-organized pairs of vertices. If all edges are undirected, or bi-directional, then the computer network is called an undirected network (geography).

Attack Analytical Model

Attack geography approach is a basic tool to assess the security of a computer network. It has been used to model the vulnerabilities of the computer systems and their prospective activities. The effective activity directing to minimal loss/damages of the systems is a matter of security concern. The task has been performed in detecting, modeling, analyzing, and facilitating the attacks. But in general, geographies are complicated and hefty to be translated and comprehensive by security analysts. Then in order to determine vulnerabilities in the computer network as such and simplify the representation of a target system, an attack geography corresponding to a target network for analysis and response must be firstly generated. A vulnerability-based attack can be graphed out, where the condition denotes the system's state-space or security-related vulnerability and activities are modeled for analysis. This also helps prioritize the security responses in terms of both repair and integrity.

NETWORK SECURITY MODEL

Usually, no security analyst likes to experience the attack but it extensively comes to life. To lower the damage of attacks cost helps lead to increased productivity. If rapid protection is not provided, the damage cost arises exponentially. Then, specific models and procedures are required to quickly analyze the attack activities. The geography model of a computer network is the common graph concept producing graph structure in the format of geography markup language (*gml*). *GML* models are appropriate for the design of computer networks in the senses of control, traffic management, and processing capacities [19]. The *gml* model used in this research is introduced in this section. It is assumed that the target computer network composes of *n* independent nodes stored in the dataset. The geography dataset is an input of the simulation in which the geography of the corresponding network is drawn out as depicted in Figure 4. The network consists of several components such as computers, servers, network hubs, routers, switches and other

interconnected devices. The simulation is used to measure the network metrics listed in the previous section such as cliques, closeness, degree etc. Thus the attack severity is computed by Equation based on vulnerabilities, attack paths, and network metrics. A surgery application using simulation as a prototype can be found in.

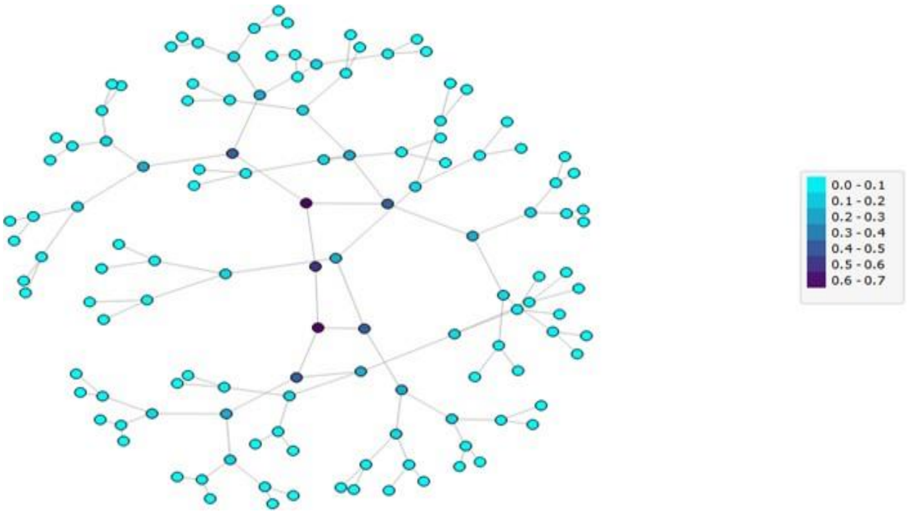

Figure 1. The geography of computer network with hundred nodes

SIMULATION RESULTS AND ANALYSIS

In order to simulate the attack geography, the initial structure of the synthetic *gml* dataset with 62 nodes is generated as shown in Figure 5. The different vulnerabilities based upon VID from the National Vulnerability Database (#7419, #7434 and #9276) are also set up to attack three dissimilar nodes (node 14, 37 and 42). The attack probabilities are assumed to be 0.5, 0.3 and 0.2 for *v1*, *v2* and *v3* respectively. The alert of successful attacks on specific nodes is displayed on the attack geography as depicted in Figure 6. In order to compute for *AS*, normalized parameters from the attack geography in Figure 5 are taken into account as summarized in Table 2. Note that results displayed in Table 2 are only the possible figures for each parameter in the ascending order rather than summarizing them in detail of individual node format. Attack severity is calculated as shown in Table 3. It is apparent node 14 needs to be protected immediately as it exhibits the highest *AS* compared to others.

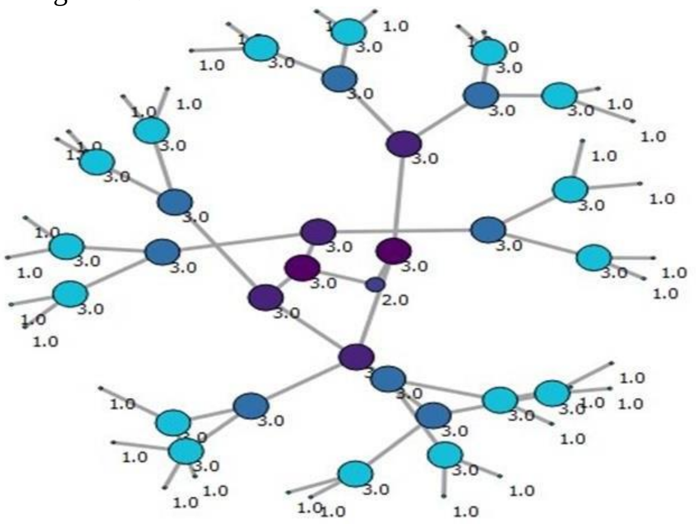

Figure 2. The initial attack geography with 62 network nodes

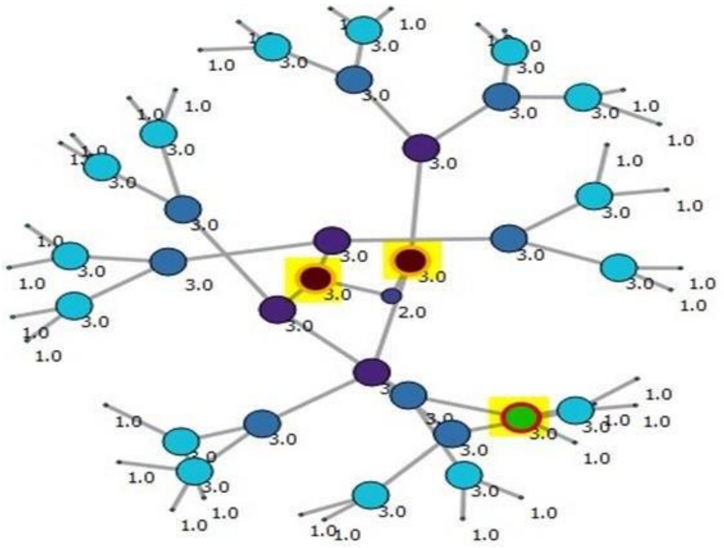

Figure 3. The geography with specific nodes under attack

CONCLUSION

Quantitative evaluation for computer network security [21-25] has critical impacts on the pro-active operation of the network protection. The existing approaches are short of a self-controllable mechanism thus an appropriate security model has been presented in this paper. In this regard, the proposed algorithm to evaluate the security of the computer networks is presented. The main contribution of this research is to help analyze AUG to discover the spotted attack in the geography. In practice, AUG fundamentally is complex and outsized then it is not too easy to comprehend. The proposed algorithm helps streamline the geography and makes it comprehensive for security analysts. The proposed algorithm is to calculate the attack severity of vulnerabilities. The simulation results give the significant immediate response in order to protect the computer networks. Another investigation may include cost-effective analysis for the case of multiple attacks. Assuming the occurrence of vulnerabilities attack follows a Markov chain then the approximation method can be used to reduce the complexity in simulation execution in the next study.

REFERENCES

[1] A. A. M. Bastina and N. Rama, “Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, pp. 408-416, 2017.

[2] Q. Wu, et al., “Evaluation of Network Connection Credibility based on Neural Network,” *Journal of Computers*, vol. 6, pp. 2567-2573, 2011.

[3] L. Xie, et al., “Network Security Risk Assessment Based on Attack Graph,” *Journal of Computers*, vol. 8, pp. 2339- 2347, 2013.

[4] Y. Chen, et al., “Optimizing Large Query by Simulated Annealing Algorithm Based On Graph-Based Approach:, *Journal of Software*, vol. 6, pp. 1655-1663, 2011.

[5] M. Jeong and S. Ahn, “A Network Coding-Aware Routing Mechanism for Time-Sensitive Data Delivery in Multi- Hop Wireless Networks,” *Journal of Information Processing Systems*, vol. 13, pp. 1544-1553, 2017.

[6] J. Chen, et al., “Distributed greedy coding-aware deterministic routing for multi-flow in wireless networks,”*Computer Networks*, vol. 105, pp. 194-206, 2016.

[7] A. S. Cheema, et al., “Network Security Using Graph Theory,” *International Journal of Innovation in Engineering and Technology*, vol. 2, pp. 131-138, 2013.

[8] R. Akshaya and H. P Menon, “A Review on Registration of Medical Images Using Graph Theoretic Approaches,”

Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 12, pp. 974-983, 2018.

[9] J. Webb, et al., “Graph Theory Applications in Network Security,” *SSRN Electronic Journal*, 2015.

[10] S. V. M. Sarma, “Applications of Graph Theory in Human Life,” *International Journal of Computer Application*, vol. 1, pp. 21-30, 2012.

[11] V. Yegnanarayanan and P. Angamuthu, “On Graph Theory Applications-I,” *Applied Research and Development Institute Journal*, vol. 3, pp. 28-42, 2012.

[12] R. Likaj, et al., “Application of graph theory to find optimal paths for the transportation problem,” *International Federation of Automatic Control (IFAC) Proceedings*, vol. 46, pp. 235-240, 2013.

[13] C. Jittawiriyanukoon, “Performance Evaluation of Reliable Data Scheduling for Erlang Multimedia in Cloud Computing,” *IEEE Proceedings of the Ninth International Conference on Digital Information Management*, pp. 39- 44, 2014.

[14] J. Chen, et al., “Dominating set and network coding-based routing in wireless mesh networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 423-433, 2015.

[15] J. B. Jensen and G. Gutin, “Digraphs: Theory, Algorithms and Applications 2nd Edition,” Springer, 2009.

[16] M. Yousefi, et al., “A Novel Approach for Analysis of Attack Graph,” *IEEE International Conference on Intelligence and Security Informatics*, pp. 7-12, 2017.

[17] C. Virmani, et al., “Clustering in Aggregated User Profiles Across Multiple Social Networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, pp. 3692-3699, 2017.

[18] C. Jittawiriyanukoon, “Evaluation of a Multiple Regression Model for Noisy and Missing Data,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 2220-2229, 2018.

[19] A. Daeri and R. Ibsaim, “Case Study: Core Network Design using Graph Theory Method,” *Proceedings of International Conference on Control, Engineering and Information Technology*, pp. 29-135, 2014.

[20] A. B. Sulong, et al., “Jig Prototype for Computer-Assisted Total Knee Replacement and Its Flow Simulation,”*International Journal of Technology*, vol. 7, pp. 132-140, 2016.

[21] B. M. Chandrakala and S. C. L. Reddy, “Secure and Efficient Bi-Directional Proxy Re-Encryption Technique,”*Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 12, pp.1143-1150, 2018.

[22] A. Singh, et al., “Empowering E-governance with E-voting,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 12, pp. 1081-1086, 2018.

[23] A. Satapathy and L. M. J. Livingston, “An Intelligent Framework Prototype for Monitoring Students in Virtual Classroom,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, pp. 1151-1158, 2018.

[24] G. Gür, et al., “Security analysis of computer networks: Key concepts and methodologies,” *Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications*, Elsevier, 2015.

[25] F. Yan, et al., “Computer Network Security and Technology Research,” *Proceedings of International Conference on Measuring Technology and Mechatronics Automation*, pp. 293-296, 2015.