ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Detecting Critical Link and Critical Node Vulnerability for Network Vulnerability Assessment

Savita R. Dhurde, Prof .A.Deshpande

Master of Engineering (Computer Network) Student, Department of Computer Engineering, G.H.Raisoni College of Engineering & Management, Wagholi, Pune, Pune University, India

Assistant Professor , Department of Computer Engineering (Network), G.H.Raisoni College of Engineering & Management, Wagholi, Pune, India

ABSTRACT: The vulnerability assessment is the pro-active step to secure network organization. The network vulnerability is very important in today's world for critical link and for critical node. The CLD (critical link disruptor) & CND (critical node disruptor) are always NP complete on the unit disk graph and power law graph and for the general graph we are analyze the CLD & CND. Finding the solution for CLD & CND problem by using HILPR algorithm, HILPR algorithm is linear programming algorithm. . In this paper we are proposed one of the novel methods is belief propagation used for critical link and critical node vulnerability for network vulnerability assessment and weight of the network.

KEYWORDS: Network vulnerability, critical node, critical link vulnerability assessment

I. INTRODUCTION

Now a day's we are study about the network security that is important in today's world. Firewalls and IDS are independent layers of security. Firewalls merely examine network packets to determine whether or not to forward them on to their end destination. Firewalls screen data based on domain names or IP addresses and can screen for low-level attacks. They are not designed to protect networks from vulnerabilities and improper system configurations. Nor can they protect from malicious internal activity or rogue assets inside the firewall. Vulnerability assessment takes a wide-range of network issues into consideration and identifies weaknesses that need correction. Vulnerability assessment solutions test systems and services such as NetBIOS, HTTP, CGI and WinCGI, FTP, DNS, DoS vulnerabilities, POP3, SMTP, LDAP, TCP/IP, UDP, Registry, Services, Users and Accounts, password vulnerabilities, publishing extensions, detection and audit wireless networks, and much more.

Vulnerability analysis aims to provide decision support regarding preventive and restorative actions, ideally as an integrated part of the planning process. [10]Vulnerability assessment usually focuses mainly on the technology aspects of vulnerability scanning. The vulnerability scanner works with a proactive approach, it finds vulnerabilities, hopefully, before they have been used. There is however a possibility that a, to the public, unknown vulnerability is present in the system vulnerability has two types. Tangible is something which can be measured/ assessed (real) e.g. Computers, book etc. Intangible are something which cannot be measured (imaginary). In this paper we study about the intangible vulnerability. [11]Vulnerability is the measuring weakness of the system or the any network such as ad-hoc network, World Wide Web, enterprise network. Network vulnerability assessment is study the natural disaster, unexpected failures of element and also studies the performance of the network reduces in different cases. After studying the vulnerability of critical links and critical nodes also we are study the vulnerability of network. [1] Identifying the critical link and critical node for the natural disaster and unexpected failure of network because in the natural disaster such an earthquake and in the unexpected failure of network. Destroy many important power lines and a large area blackout.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

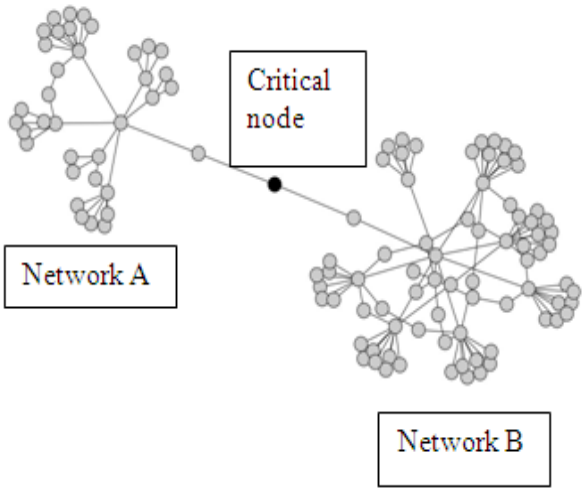

FIG: 1: Detecting Critical Node between Network A&B

Vulnerability scanning consists of using a computer program to identify vulnerabilities in networks, computer infrastructure or applications [8]. Vulnerability assessment is the process surrounding vulnerability scanning, also taking into account other aspects such as risk acceptance, remediation etc. A vulnerability assessment process should be part of an organization's effort to control information security risks. This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. [9]Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information many organizations do not frequently perform vulnerability scans in their environment. They perform scans on a quarterly or annual basis which only provides a snapshot at that point in time. The figure below shows a possible vulnerability lifecycle with annual scanning in place

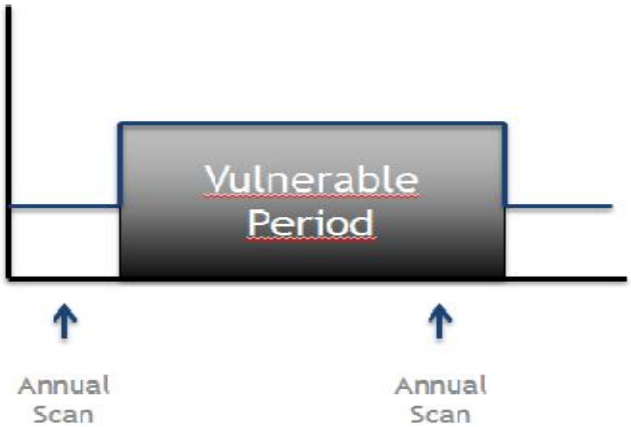

FIG: 2: Annual Vulnerability scanning

Any vulnerability not detected after a schedule scan takes place, will only be detected at the next scheduled scan. This could leave systems vulnerable for a long period of time. When implementing a vulnerability management process, regular scans should be scheduled to reduce the exposure time. The above situation will then look like this:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

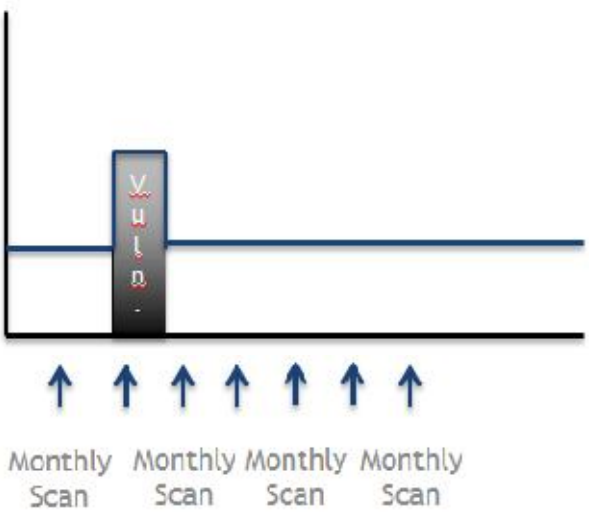

FIG: 3: Continuous vulnerability assessment

Regular scanning ensures new vulnerabilities are detected in a timely manner; allow them to be remediated faster. Having this process in place greatly reduces the risks an organization is facing. When building a vulnerability assessment process, the following roles should be identified within the organization:
1) Security Officer:
2) Vulnerability Engineer:
3) Asset Owner:
4) IT System Engineer

Suppose taking example of MANET[13] for definition of a critical node is a node whose failure or malicious behaviour disconnects or significantly degrades the performance of the network. Once identified, a critical node can be the focus of more resource intensive monitoring or other diagnostic measures. If a node is not considered critical, this metric can be used to help decide if the application or the risk environment warrant the expenditure of the additional resources required to monitor, diagnose, and alert other nodes about the problem. In order to detect a critical node we look towards a graph theoretic approach to detect a vertex-cut and an edge-cut. A vertex-cut is a set of vertices whose removal produces a sub graph with more components than the original graph. A cut-vertex, or articulation point, is a vertex cut consisting of a single vertex. An edge-cut is a set of edges whose removal produces a sub graph with more components than the original graph. A cut-edge, or bridge, is an edge-cut consisting of a single edge. Although the cut-vertex or cut-edge of a graph G can be determined by applying a straight forward algorithm [12], finding a cut-vertex in the graphical representation of an ad hoc network is not as straightforward, since the nodes cannot be assumed to be stationary. A network discovery algorithm can give an approximation of the network topology, but the value of such an approximation in performing any kind of network diagnosis or intrusion detection depends on the degree of mobility of the nodes.

II. RELATED WORK

We study about the framework and its components for measuring the vulnerability [5]. Either connectivity or capacity is needed to network reliability analysis .In the area of distributed computing network reliability is an important issue. For measuring the graph vulnerability use the neighbor-scattering number [6]. In the world software, vulnerability is increased in the fast way. In the information security the focusing point is software vulnerability .for the similarity calculation the national vulnerability database and ontology of vulnerability management provide the needed information. In many area of vulnerability management the similarity measurement can be used. in software security , data mining , software testing the similarity measurement model of program execution is used. reducing the quality of software testing method because of the lacking of measurement. by using the data types the measurements are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

categorized. For optimization process the similarity graph is used. Categorization scheme of the standard vulnerability lacking in the assessment of the information system security, lack of vulnerability is problem in the information system security. For the information system security assessment and measurement of the software tools and services necessary thing is standard vulnerability taxonomy [7].

Quality of the services is more important in the discovery of topologies because the real time internet application developed rapidly in the world. So, for assessment the vulnerability of general network topologies we used the quality of service aware measurement. Many existing works on network vulnerability assessment mainly focus on the centrality measurements, including degree, between's and closeness centralities, average shortest path length [6], global clustering coefficients. Due to the failures to assess the network vulnerability using above measurements, Sun et al. First proposed the total pair wise connectivity as an effective measurement and empirically evaluate the vulnerability of wireless multichip networks using this metric. Arulselvan et al. [3] showed the challenge of CND problem by proving its NP-completeness. Later on, the _-disruptor problem was defined by Dinh et al. [2] to find a minimum set of links or nodes whose removal degrades the total pair wise connectivity to a desired degree. They proved the NP-completeness of this problem with respect to both links and nodes and the corresponding in approximability results. Even for the tree topology, Di Summa et al. [4] found that the discovery of critical nodes also remains NP-complete using this metric. In this paper, we further investigate the theoretical hardness of both CLD and CND on UDGs and PLGs. In addition, there are a few effective solutions in the literature of the network vulnerability assessment based on the pair wise connectivity. Arulselvan et al. [3] designed a heuristic (CNLS) to detect critical nodes, which is however still far away from the optimal solution in large-scale and dense networks. In [2], Dinh et al. proposed pseudo-approximation algorithms to solve the _-disruptor problem. However, this problem is defined differently than ours and hard to use its solution when we only know the available cost to destroy or protect these critical links or nodes.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- Initially taking nodes & links for drawing graph
- Select starting and ending point for finding shortest path.
- Solve and find critical node and link
- Solve graph for as a general graph ,power law graph and unit disk graph
- Lastly solve the belief propagation algorithm for network vulnerability

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to find the critical node vulnerability& critical link vulnerability and find network vulnerability & weight of network. The proposed algorithm is consists of three main steps.

Belief propagation Algorithm:

Step: 1

Every node $n_i$computes vulnerability metric of all its neighboring nodes to which it transmits packets this node n_i calculates vulnerability belief over time Δt duration.

Step: 2

Node n_i periodically calculates vulnerability belief of all its neighbors.

Step: 3

Similarly node n_i also gets assessed by its neighbouring nodes for belief value

Step: 4

The total vulnerability belief of node n_i over Δt

$$= \frac{\sum_{i=1}^{Dn_i} V_{n_i}^{\Delta t}}{D_{ni}}$$

Step: 5

The total vulnerability belief of network is calculated as

$$= \frac{vulnerability\ belief\ of\ node\ n_i}{total\ no.of\ nodes\ N}$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

IV. SIMULATION RESULTS

Suppose the following graph G1 show the network structure of any lab (L)

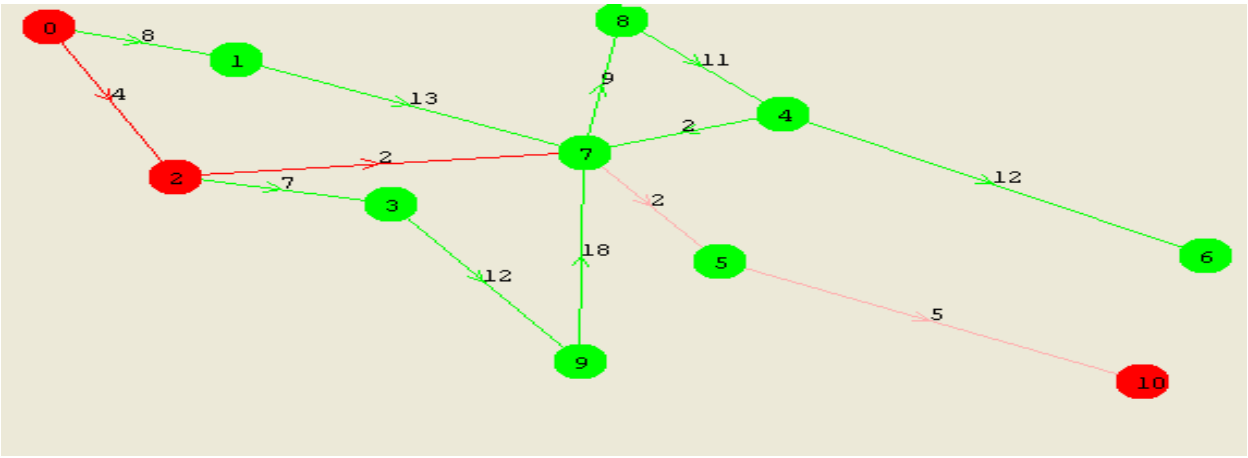

Fig: 4: The Network of Lab (L)

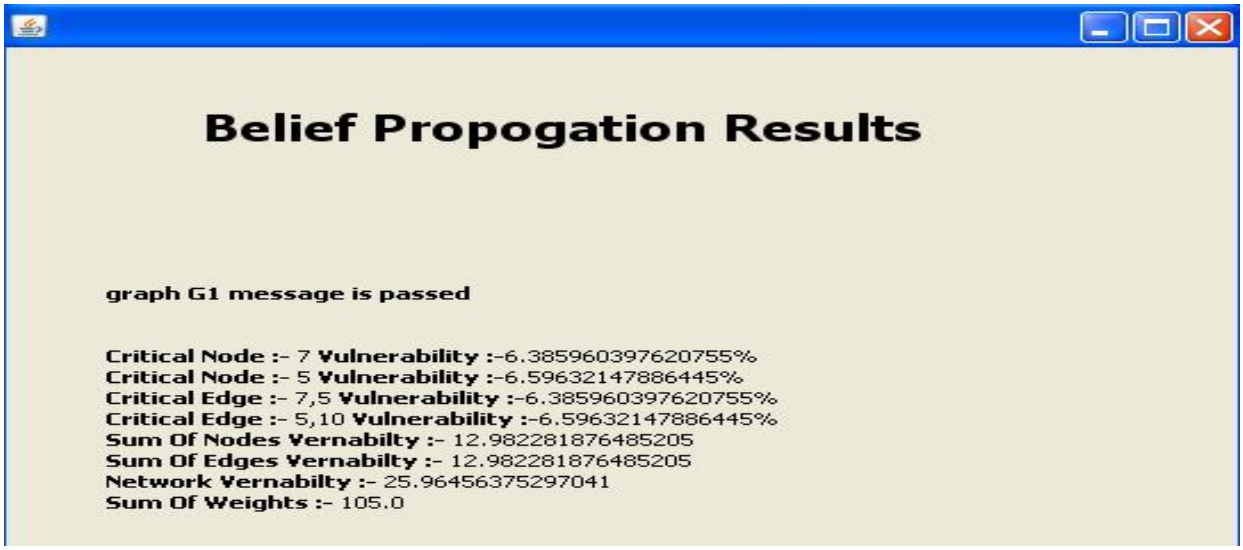

FIG: 5: Show the Result for Above Graph (Network of L)

V. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better in this paper using Vulnerability Belief propagation we are study the novel method for Network Vulnerability Assessment about the given graph of network. We are first find out the shortest path in the network by using Dijkstra algorithm and then find vulnerability of CLD & CND .For finding the network vulnerability we are use belief propagation algorithm this vulnerability is in percentage. Also we are finding the weight of the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

REFERENCES

1. Anjum R. Albert, I. Albert, and G. L. Nakarado. "Structural vulnerability of the North American power grid." Phys. Rev. E, 69(2), Feb 2004.
2. T. Dinh, Y. Xuan, M. Thai, P. Pardalos, and T. Znati. "On new approaches of assessing network vulnerability: Hardness and approximation". Networking, IEEE/ACM Transactions on, 20(2):609 –619, April 2012.
3. A. Arulselvan, C. W. Commander, L. Elefteriadou, and P. M. Pardalos. "Detecting critical nodes in sparse graphs" Comput. Oper. Res., 36:2193–2200, July 2009
4. M. D. Summa, A. Grosso, and M. Locatelli. "Complexity of the critical node problem over trees".Computers & OR, 38(12):1766–1774, 2011
5. Scarfone, K.; Grance, T. Nat. Inst. of Stand. & Technol., Washington, DC. "A framework for measuring the vulnerability of hosts". Information Technology IT 2008.1st International Conference on,52(1):1-4 May 2008
6. Fengwei Li; Qingfang Ye; Shuhua Wang. "Neighbor-scattering number in regular graphs", Multimedia Technology (ICMT), International Conference on . 2209 – 2214, 2011
7. Dept. of Inf. Technol., Mahakal Inst. of Technol., Ujjain, India Computer Technology and Development (ICCTD)."Towards standardization of vulnerability taxonomy.Towards standardization of vulnerability taxonomy", 2nd International Conference on.379-384,2010
8. http://en.wikipedia.org/wiki/Vulnerability_management
9. Williams, A and Nicollet, M: "Improve IT Security With Vulnerability Management", Gartner ID Number: G00127481, May 2005
10. Y. Shen, N. P. Nguyen, and M. T. Thai. "Exploiting the robustness on power-law networks". In COCOON, pages 379–390, 2011.
11. F. Yamaguchi, M. Lottmann, and K. Rieck. "Generalized vulnerability extrapolation using abstract syntax trees". In Proc. of Annual Computer Security Applications Conference (ACSAC), pages 359–368, Dec. 2012.
12. de Bruijn, H.; de Bruijne, M.; Steenhuisen, B. Delft Univ. of Technol., "Delft Managing infrastructure vulnerability: An empirical study on the use of performance management systems that seek to reduce vulnerability of network industries Technology and Society", IEEE International Symposium on, 1-7,2007
13. Daisuke Kasamatsu, Norihiko Shinomiya and Tadashi Ohta, "A Broadcasting Method considering Battery Lifetime and Distance between Nodes in MANET", IEICE Transactions on Information and Systems, Vol. J91-B, No.4, pp.364-372, 2008
14. A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, "Detecting Critical Nodes for MANET Intrusion Detection Systems", In Proceedings of IEEE Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.7-15, 2006

BIOGRAPHY

Savita R.Dhurde & Prof Aarti Deshpande is a Research in the Computer Department, College of G.H.Raisoni College Of Engg.&Mgmt, PuneUniversity. Savita Dhurde is the student of ME (Computer Network) in Computer Department. Assistant Professor Aarti Deshpande is MTECH (mobile computing); her research interests are Computer Networks (Networks Security), Vulnerability Assessment.