IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A SURVEY PAPER ON EVIDENCE GRAPHS AND RISK ASSESSMENT METHOD BASED ON AHP

[1]Name of 1st C Srinivas, [2]Name of 2nd Prof P S Avadhani, [3]Name of 3rd Prof P Prapoorna Roja

[1]Designation of 1st Research Scholar, [2]Designation of 2nd Professor, [3]Designation of 3rd Professor
[1]Name of Department of 1st Computer Science and Engineering,
[1]Name of organization of 1st JNTUK, Kakinada, India

Abstract: The Analytic Hierarchy Process (AHP) has been broadly used in the fields of decision-making, operations research, and management. Further extension of the AHP is additionally proposed to deal with the fuzzy environments or crew decision-making trouble via the use of fuzzy or interval numbers. In the AHP, the Consistency Index (CI) or others, e.g., consistency ratio (CR)of the AHP is considered as an index to choose the rationality and consistency of the weights of criteria. However, these indices appear to be disregarded in the Fuzzy / Interval AHP in the previous papers. That is, the end result that we really use the traditional fuzzy/interval AHP may be inconsistent. In this paper, we advocate a steady fuzzy AHP which debates the notion of CI and makes certain the regular end result of the weights in each of the Fuzzy / Interval environments and team decision-making

Index Terms - Analytic Hierarchy process (AHP); Decision-making; consistency index; fuzzy / interval environments; group decision making.

I.INTRODUCTION

Analytic Hierarchy Process (AHP), considering its invention, has been a device in the arms of decision makers and researchers; and it is one of the most widely used a couple of standards decision-making tools. Many excellent works have been posted primarily based on AHP: they encompass applications of AHP in one of a kind fields such as planning, deciding on a great alternative, useful resource allocations etc.,

The AHP [1,2] is a famous technique to locate weights of standards in each person and team decision-making. It is clear that, due to the troubles of incomplete data and subjective uncertainty, even professionals find it hard to quantify unique ratios of weights between criteria. Although the thinking of fuzzy units or interval numbers has been included into the AHP to reflect on consideration on the trouble of uncertainty [3,4,5], few papers talk about the problem of inconsistency in the fuzzy AHP (FAHP) however see [6,7], even though it has been substantially studied in the traditional AHP.

The current article appears in the lookup papers with a view to apprehend the unfolding of the AHP functions in exceptional fields. The papers considered for discussions describe the extensively used AHP as a developed tool. An strive is made to provide an explanation for a few contemporary purposes in a nutshell. Care has been taken to perceive the state-of-the-art references and give an explanation for the findings in every category, and additionally to talk about the paper that have been published in worldwide journals of excessive repute. The coverage, however, is no longer exhaustive, and tries to portray solely the glimpses of AHP purposes In addition, when making use of the FAHP into the team choice making, the troubles of deriving the compromise team weights and keeping the character weights are additionally studied here.

To emphasize that fuzzy weights are very essential in supporting decision-makers to apprehend the uncertainty levels of problems, particularly in areas that contain dynamic selection making or danger evaluation, such as the administration of future investments, monetary portfolio selection, and capital budgeting. However, the inconsistent end result of fuzzy weights can preclude the purposes of the AHP in fuzzy environments and team decision-making. Note that the inconsistent end result of weights in the AHP effects from the inconsistent assessment of weight rations. In FAHP, the difficulty is extra tricky on account that some fuzzy intervals may additionally end in the inconsistent end result of weights however some do not. In this paper, it reflects on consideration of the restrained fuzzy operations to derive the steady fuzzy weights in each character and team FAHP. Note that on account that interval numbers can be regarded as a distinct case of fuzzy numbers, the sole center of attention on FAHP in this paper.

The methods of the proposed approach can be described as follows:

- First, it includes the thought of the consistency index (CI) into our programming to discover the minimal reduction , such that the most CI is much less than the tolerant fee (usually set 0.1 in the traditional AHP).
- Then, add the above statistics of the reduce to the subsequent step of the mathematical programming to derive the fuzzy weights of the criteria. The deriving end result ensures the rationality and consistency of fuzzy weights in the FAHP. Furthermore, prolong the above thinking to deal with the crew selection making situation, i.e., deriving team fuzzy weights.
- Finally, it uses a numerical instance to display the proposed technique and evaluate it with the traditional FANP.

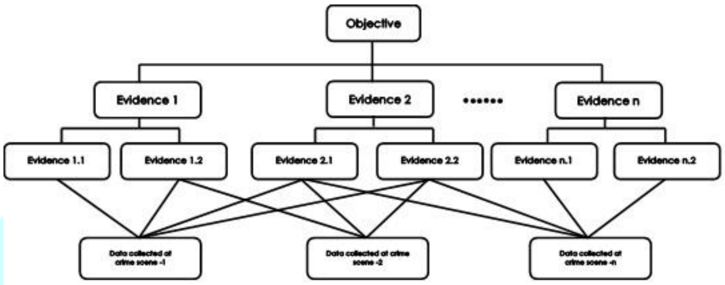


Fig 1 : Cyber Forensics risk Management

It is strongly believed that this work will provide a quick perception for the future work involved with AHP, and assist the working towards engineers get a view of one of a kind sides of AHP.

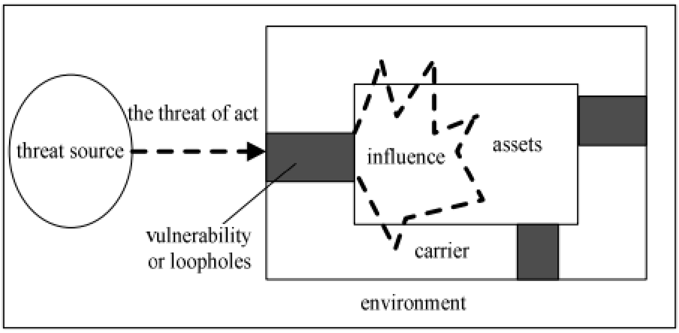
The rest of this paper is geared up as follows. In this, overviews the traditional AHP and the consistency index. The proposed FAHP which is used in both character and team decision-making is introduced. A numerical instance shows the proposed method. A dialogue of the assessment effects and conclusions.

II.NETWORK INFORMATION SYSTEM SECURITY RISK GENERATING MECHANISM:

Network Information system security risk generating mechanism is the premise of the research of information systems security risk assessment. In general, the risk is the uncertainty of the result of actions or incidents. As a result, whether positive opportunities or negative threats, we assess the risk only through the possibility of these uncertainties occurring, as well as the impact of actually happening. Information system security risk is the potential security risk of information systems, or the possible incident that led to the loss of assets of information and information systems. hazard receptor and hazard end result .

Risk foundation is the beginning of the threat, recognized as a risk source. According to their nature, they can be divided into environmental threats and man-made threats. Risk way is the capability via which hazard supply implements threat, referred to as the risk of act. Different danger sources have exclusive chance acts, and in a unique environment, the risk acts have one of a kind potential to attack.

For example, the threat of earthquakes in the earthquake-prone areas is significantly high; the danger of floods in the desolate tract areas is obviously very low. Risk potential is the susceptible hyperlinks which would be used via chance supply to enforce threat, known as the vulnerability or loophole.



The provider and the surroundings of assets have flaws or vulnerable hyperlinks that may want to be used with the aid of risk sources. Vulnerability or loopholes may also exist in the management measures and jogging links, and technology. Risk receptor is the risk to endure side, that is, assets. Asset is valuable, and it will lead to hazard as lengthy as there is value. As a result, assets are the root of danger which exists in a range of forms. Risk outcome is the loss of the implementation of hazard of the chance source, known as influence. In general, the effect of asset impairment is immediately proportional to the fee of the assets. The relationship between them can be expressed as, one or more risk origins of the danger do injury to one or extra hazard receptors, the usage of one or greater risk ways, through one or extra hazard means, resulting in poor hazard consequences. Figure II depicts the facts gadget protection dangers producing mechanism. It can be expressed as, risk supply uses the vulnerability to enforce hazard to the assets, resulting in negative impact. Dotted line on the map capacity that the danger or influence is potential, it should take the vicinity with possible way.

III.THEORETICAL RISK FACTORS:

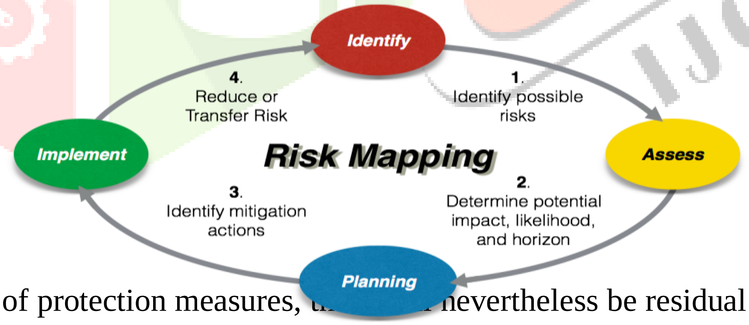
Network device protection chance evaluation is the contrast procedure on statistics safety attributes such as confidentiality, integrity and availability, what is prompted in records structures and its processing, storage and transmission, on the groundwork of statistics safety technological know-how and administration standards. To elevate out threat assessments, one has to pick out a variety of the most integral interrelated elements primarily based on the extraordinary nature of the evaluation object itself, to advance the techniques and capability of hazard assessment.

In the statistics structures protection hazard evaluation studies, the creator thinks that assets, threats, vulnerabilities, such as protection measures are at the same time referred to as threat factors. The members of the family between them can be summed up as follows: Assets are valuable, and the organization's enterprise method relies upon assets.

The greater the dependence, the larger the cost of the assets, and the large its influence on organizations, the increased the risk;

- Risk prompted through threat, the extra the threats of asset and the larger the risk;
- The larger the vulnerability of assets, the larger the opportunity of protection occasions brought on through hazard the usage of the vulnerability of assets;
- Threat do harm to property with the aid of the use of the vulnerability, and this lead to risk;

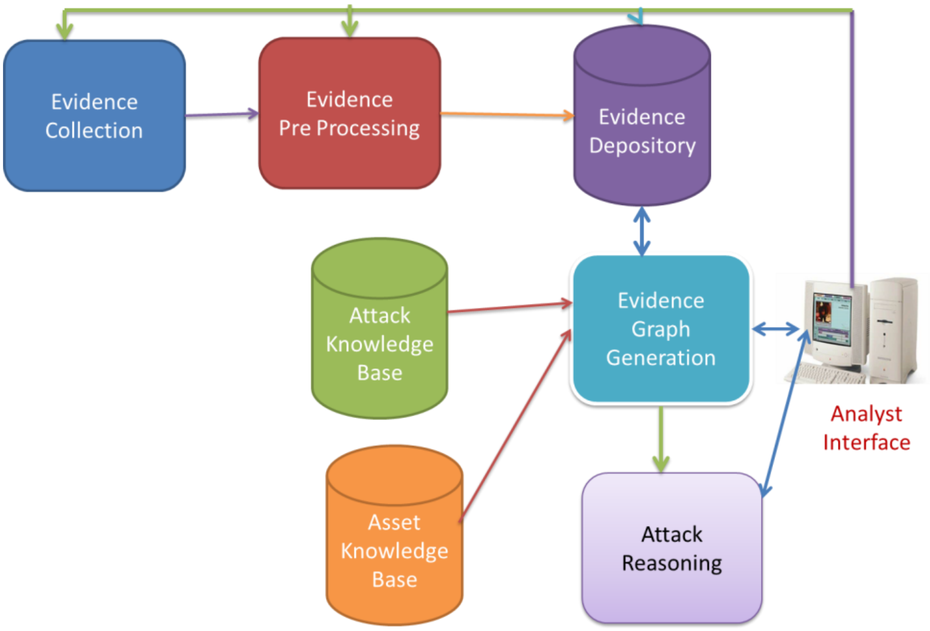
Safety measures can in opposition to threats and limit the danger of the risk via the usage of the vulnerability;



After the implementation of protection measures, th nevertheless be residual risk. Some residual dangers come from the safety measures that had been inappropriate or ineffective, so want to proceed to control [11]. Some residual chance is uncontrolled after taking the fee of safety and advantages into account and these dangers are acceptable. Residual danger has to be carefully monitored, due to the fact it may also motivate new security-induced occasions in the future.

IV.NETWORK FORENSICS ANALYSIS MECHANISM:

In this section, presents the components that support our approach in network forensics analysis. The architecture of our network forensics analysis mechanism



Architecture of Analysis Mechanism

V.EVIDENCE PREPROCESSING:

Primary evidence and secondary evidence are the two types of evidence used in network forensics investigations. Primary evidence is data that clearly demonstrates assaults or security protocol violations. Information that does not directly relate to an assault but could add to the investigation's knowledge base is referred to as secondary evidence. Secondary evidence comes from numerous sources and is significantly more plentiful [21].

Typically, primary evidence forms the basis of secondary evidence searches and serves as the starting point of a forensic inquiry. Searching the secondary evidence often has two goals: finding concealed suspicious events and assessing the reliability of the primary evidence. Our present prototype uses network IDS alarms as the main proof, with raw network flow logs and host logs serving as backup.

VI.EVIDENCE GRAPH CONSTRUCTION AND SNORT AS THE NETWORK:

IDS alerts are the key source of evidence in our prototype. To capture key intrusion alarm attributes, we define a condensed template derived from IDMEF [12]. Raw alert is used to describe the outcome. Raw alerts have the following formatting: AlertID, Classification, SrcIP, DesIP, DetectTime, and HyperID.[23]

It is challenging to effectively examine the underlying threats due to the significant repetition in raw warnings.

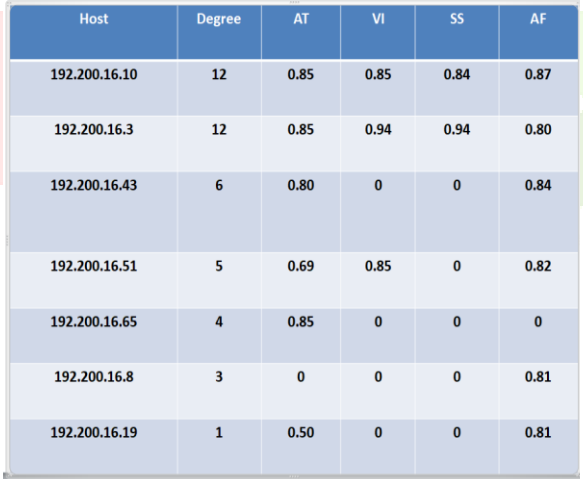
For instance, a single incident frequently produces a large number of duplicate notifications quickly. To combine unprocessed alerts into hyper alerts, we employ alert aggregation based on similarity of properties and context criteria. HyperID, Classification, SrcIP, DesIP, StartTime, EndTime, and Count are the components of a hyper alert's format.

The practice of aggregating alerts tries to eliminate duplicates.

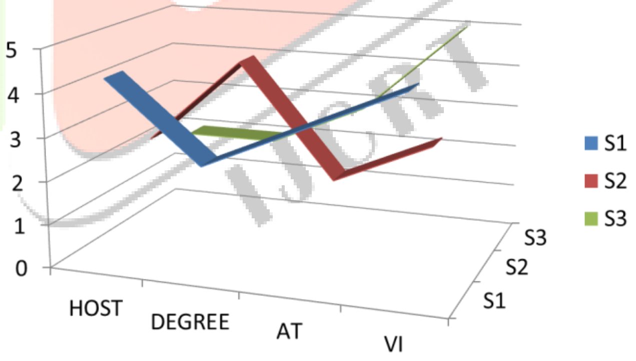
```
input  : A set of raw alerts $r_1 \dots r_n$, time limit T
output: A set of hyper alerts $h_1 \dots h_m$
begin
    $h_1 \leftarrow r_1$;
    $m \leftarrow 1$;
    for $i \leftarrow 2$ to $n$ do
        $merged \leftarrow 0$;
        for $j \leftarrow 1$ to $m$ do
            if $r_i.sourceaddr = h_j.sourceaddr$ &&
            $h_j.destaddr = r_i.destaddr$ &&
            $h_j.class = r_i.class$ &&
            $h_j.starttime - T \leqslant r_i.detecttime \leqslant$
            $h_j.endtime + T$ then
                $h_j.starttime \leftarrow$
                $min(h_j.starttime, r_i.detecttime)$;
                $h_j.endtime \leftarrow$
                $max(h_j.endtime, r_i.detecttime)$;
                $r_i.hyperid \leftarrow h_j.id$;
                $h_j.count \leftarrow h_j.count + 1$;
                $merged \leftarrow 1$;
                $break$;
            end
        end
        if $merged = 0$ then
            $m \leftarrow m + 1$;
            $h_m \leftarrow r_i$;
            $h_m.count \leftarrow 1, h_m.HyperID \leftarrow m$;
        end
```

VII.EXPERIMENTS & RESULTS

We evaluate the proposed method through several multi-stage attack scenarios. It uses Snort as an IDS network sensor to generate intrusion alerts and uses TcpDump to collect raw network traffic from the test bench.



Host	Degree	AT	VI	SS	AF
192.200.16.10	12	0.85	0.85	0.84	0.87
192.200.16.3	12	0.85	0.94	0.94	0.80
192.200.16.43	6	0.80	0	0	0.84
192.200.16.51	5	0.69	0.85	0	0.82
192.200.16.65	4	0.85	0	0	0
192.200.16.8	3	0	0	0	0.81
192.200.16.19	1	0.50	0	0	0.81



Collected evidence is stored in a MySQL database. Implemented a set of Perl scripts to aggregate intrusion alerts, extract flow information, and automatically incorporate previous knowledge into the inference process. We are developing an application based on LEDA[27] to manage proof graphs and inference results.

VIII.CONCLUSIONS AND FUTURE WORK :

In this paper, we have developed a network forensic analysis mechanism. We have proposed the proof graph as a new graph model for the presentation and manipulation of intrusion evidence. Based on the evidence graph, we have proposed to add a hierarchical reasoning framework for automated evidence analysis. Through local reasoning with RBFCM, we learned the possible role of suspicious hosts in the local view. In global inference, we identify the set of highly correlated hosts in the attack cluster and refine the roles in the local inference results to match the scenario context. The combination of local and global argument results provides the analyst with a high-level picture of attacks represented by observable intrusion evidence. We have developed a prototype tool and the first test results demonstrate the potential of using our proposed methods. This work is just the starting point in our efforts towards forensic analysis of the network. In future work, we will refine current approaches to local and global reasoning. We will also explore methods for automating the process of hypothesizing missing evidence and validating hypotheses. In the next step, we will work with government and industry agencies to evaluate our techniques with more real-world tests.

IX. *REFERENCES:*

1. S.L. Ahire, D.S. Rana, Selection of TQM pilot projects using an MCDM approach, International Journal of Quality & Reliability Management 12 (1) (1995) 61–81.
2. Saaty, T.L. (1980). The Analytic Hierarchy Process, McGraw-Hill, NY.
3. Saaty, T. L. & Vargas, L.G. (1998). Diagnosis with dependent symptoms: Bayes theorem and the analytic hierarchy process, Operations Research 46 (4), 491-502.
4. Buckley, J. M. (1985). Fuzzy hierarchical analysis, Fuzzy Sets and Systems 17 (3), 233-247.
5. van Laarhoven, P. J. & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority method, Fuzzy Sets and Systems 11 (1), 199-227.
6. Wagenknecht, M. & Hartmann, K. (1983). On fuzzy rank-ordering in poly optimization, Fuzzy Sets and Systems 11 (1-3), 243-251.
7. Leung, L. C., & Cao, D. (2000). On consistency and ranking of alternatives in fuzzy AHP. European Journal of Operational Research, 124(1), 102-113.
8. Ghazanfari, M., & Nojavan, M. (2004). Educing inconsistency in fuzzy AHP by mathematical programming models. Asia-Pacific Journal of Operational Research, 21(03), 379-391.
9. Mikhailov, L. & Singh, M. G. (2003). Fuzzy analytic network process and its application to the development of decision support systems, IEEE Transactions on Systems, Man, and Cybernetics 33 (1), 33-41.
10. Mikhailov, L. (2003). Deriving priorities from fuzzy pairwise comparison judgments, Fuzzy Sets and Systems 134 (3), 365-385.
11. Chang, P. T. & Lee, E. S. (1995). The estimation of normalized fuzzy weights, Computers & Mathematics with Applications, 29 (5), 21-42.
12. Csutora, R. & Buckley, J. (2001). Fuzzy hierarchical analysis: the Lambda-max method, Fuzzy Sets and Systems 120 (2), 181-195.
13. Entani, T., & Inuiguchi, M. (2010). Group decisions in interval AHP based on interval regression analysis. In Integrated Uncertainty Management and Applications (pp. 269-280). Springer Berlin Heidelberg.
14. Entani, T. (2015). Group interval weights based on conjunction approximation of individual interval weights, 7 (3), 427-439.
15. J. P. Carvalho and J. A. B. Tome. Rule Based Fuzzy Cognitive Maps and Fuzzy Cognitive Maps - A Comparative
16. Study. In Proceedings of the 18th International Conference of the North American Fuzzy Information Processing Society(NAFIPS99), New York, 1999.
17. J. P. Carvalho and J. A. B. Tome. Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations. In Proceedings of the 8th International Fuzzy Systems Association World Congress(IFSA99), Taiwan, 1999.
18. F. Cuppens and A. Miege. Alert Correlation in a Cooperative Intrusion Detection Framework. In Proceedings of the 2002 IEEE Symposium on Security and Privacy, May 2002.
19. O. Dain and R. Cunningham. Building scenarios from a heterogeneous alert stream. In Proceedings of the 2001 IEEE workshop on Information Assurance and Security, pages 231–235, 2001.
20. O. Dain and R. Cunningham. Fusing a heterogeneous alertworkshop on Data Mining for Security Applications, pages 231–235, 2001.
21. T. E. Daniels. Reference Models for the Concealment and Observation of Origin Identity in Store-andForward Networks. PhD thesis, Purdue University, West Lafayette,Indiana, 2002.
22. H. Debar, M. Dacer, and A. Wespi. A revised taxonomy for intrusion-detection systems. In IBM Research Report, 1999.
23. H. Debar and A. Wespi. Aggregation and Correlation of Intrusion-Detection Alerts. In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection(RAID), October 2001.
24. EnCase Forensic Tool. Available at http://www.guidancesoftware.com.
25. Intrusion Detection Message Exchange Format. Internet draft available at http://www.ietf.org/internet-drafts/draftietf-idwg-idmef-xml-14.txt.
26. Institute for Security Technology Studies. Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report. http://www.ists.dartmouth.edu, February 2004.
27. LEDA graph library. Algorithmic Solutions Software, http://www.algorithmic-solutions.com/enleda.htm.
28. S. M. Bellovin. Internet draft: ICMP traceback messages. Available at http://www.ietf.org/internet-drafts/draftbellovin-itrace-00.txt, March 2000.
29. C. Kruegel and W. Robertson. Alert Verification: Determing the success of intrusion attempts. In Proceedings of the 1st Workshop on the Detection of Intrusions and Malware Vulnerability Assessment (DIMVA), Dortmund, Germany, July. 2004.

30. B. Morin, L. Me, H. Debar, and M. Ducasse. M2D2: A Formal Data Model for IDS Alert Correlation. In Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection, pages 115–137, 2002. [16] P. Ning, Y. Cui, and D. S. Reeves. Constructing attack scenarios through correlation of intrusion alerts. In the 9th ACM Conference on Computer and Communications Security, November 2002.
31. SafeBack Bit Stream Backup Software. Available at http://www.forensics-intl.com/safeback.html.
32. K. Shanmugasundaram, N. Memon, A. Savant, and H. Bronnimann. ForNet: A Distributed Forensics Network. In Proceedings of the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, St. Petersburg, Russia, 2003.
33. A. Siraj, S. M.Bridges, and R. B.Vaughn. Fuzzy cognitive maps for decision support in an intelligent intrusion detection system. Technical report, Department of Computer Science, Mississippi State University, 2001.
34. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer. Single-packet ip traceback. IEEE/ACM Trans. Netw., 10(6):721–734, 2002.
35. A. Valdes and K. Skinner. Probabilistic alert correlation. In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection(RAID), October 2001.
36. K. Yoda and H. Etoh. Finding a connection chain for tracing intruders. In Proceedings of the 6th European Symposium on Research in Computer Security (ESORICS 2000), Toulouse, France, Oct. 2000.
37. Y. Zhang and V. Paxson. Detecting stepping stones. In Proceedings of the 9th USENIX Security Symposium, pages 171–184, Denver, USA, Aug. 2000.

.