INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Polandwith IC Value of 5.09 &number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2592 Cities in 161 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

IP TRACEBACK OF DOS ATTACKS

S.THILAGAVATHI.
RESEARCH SCHOLAR
DEPARTMENT OF COMPUTER SCIENCE
BHARATHIAR UNIVERSITY
COIMBATORE

DR. A. SARADHA
HEAD
DEPARTMENT OF CSE
IRTT COLLEGE OF ENGINEERING
ERODE

ABSTRACT

IP trace back means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, It may not be able to find the actual hackers at present. In fact, IP trace back schemes are considered successful if it identify the zombies from which the DDoS attack packets entered the Internet. The efforts on IP trace back are limited. This System proposes a IP trace back using information theoretical parameters, and there is no packet marking in the proposed strategy; therefore, can avoid the inherited shortcomings of the packet marking mechanisms. The packets are categorized; that are passing through a router into flows, which are defined by the upstream router where a packet came from, and the destination address of the packet. During non attack periods, routers are required to observe and record entropy variations of local flows. In this paper flow entropy variation or entropy variation is used interchangeably.

KEYWORDS
Distributed Denial-of-Service, Entropy Variation, Forwarding packets from sender to receiver, Measuring link loss rate.

1. INTRODUCTION

IP trace back methods should be independent of packet pollution and various attack patterns. The new approach compares the packet number distributions of packet flows, which are out of the control of attackers once the attack is launched, and it is found that the similarity of attack flows is much higher than the similarity among legitimate flows, e.g., flash crowds.

Once a DDoS attack has been identified, the victim initiates the following pushback process to identify the locations of zombies: the victim first identifies which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated, and then submits requests to the related immediate upstream routers. The upstream routers identify where the attack flows came from based on their local entropy variations have monitored.[2][3]

2. DISTRIBUTED –DENIAL OF SERVICE ATTACK

A distributed denial of service attack (DDOS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack[1]

3. DRAWBACK OF EXISTING SYSTEM

The existing system has following disadvantages,

- Priority Inference is applied based on packet types.
- Port based load sharing is not discussed.
- Speed reduction in high speed packet sending application is not possible.
- Theoretical discussion only available and lack of implementation.

4. SCOPE OF THE SYSTEM

- Minimize the packet loss rate.
- To create a topology that sends the packets between two nodes without failure.
- Create a communication method that updates the failure nodes offline status to all the dependent nodes immediately.
- To improve the routing table configuration information to network administrators.
- To update the upcoming nodes status to all the nodes in the network immediately so as to make automatic routing configuration
- Assists in regulation of malicious packet sending nodes.
- Alert sending to affecting router.
- The proposed strategy can trace back fast in larger scale attack networks

4.1. FORWARDING PACKETS FROM SENDER TO RECEIVER

The router metric such as incoming bit rate of normal TCP nodes, high speed torrent like application's port's incoming bit rate and time to live in queue are stored first. The client application sends packets to server application which acts as router, The packets if arrived has reached the maximum limit of router then it will be added in queue. The packets remain there up to their time to live. If the traffic is less enough, then the packets are routed to destination nodes otherwise if time exceeds it will be simply dropped.[4]

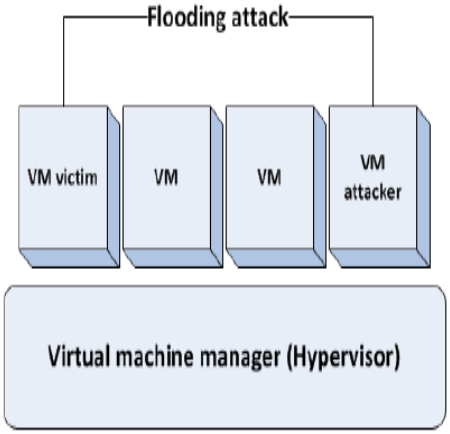
4.2. MEASURING LINK LOSS RATE

The packets lost details are logged in a database table to measure the loss rate. The details are analyzed whether the high speed port applications cause the more loss rate. Packet dropping start time and end time are kept in log so as to measure the loss rate.

4.3 CHANGE QUEUE PRIORITY BASED ON PORT BASED LOAD SHARING

The packets lost details are measured and queue priority is maintained between normal queue and high speed port's queue. Details are gathered such that the incoming packets arrived quickly from high speed port's application are responsible for packet loss in normal traffic.

FIGURE 1: CHANGE QUEUE PRIORITY BASED ON PORT BASED LOAD SHARING



4.4 ALERTING NODES WHICH SEND MORE PACKETS

The link loss rate is measured and decided whether the high speed ports are responsible for that loss. If the condition is met, then the loss amount as well as rate is calculated and nodes that containing high speed torrent applications are notified to reduce the packet sending speed.

The new approach includes maximum throughput algorithm to serve the nodes better. Maximum throughput scheduling is a procedure for scheduling data packets in a packet-switched best-effort communications network, typically a wireless network, in view to maximize the total throughput of the network, or the system spectral efficiency in a wireless network. This is achieved by giving scheduling priority to the least "expensive" data flows in terms of consumed network resources per transferred amount of information.

4.5 ENTROPY PROCESS

Network traffic for a router may dynamically change a lot from peak to off-peak service times. However, this kind of change lasts for a relatively long time interval, e.g., at least at the level of minutes.

If it break down these changes into seconds, the change of traffic is quite smooth in the context. The number of attack packets is at least an order of magnitude higher than that of normal flows[6][11]

5. PROPOSED SYSTEM

The proposed system is required to analyze the loss rate and change queue priority. Hence a system with efficient algorithm is required to minimize the loss rate by normal nodes. An effective and efficient IP trace back scheme against DDoS attacks based on entropy variations. It is a fundamentally different trace back mechanism from the currently adopted packet marking strategies. Many of the available work on IP trace back depend on packet marking, either probabilistic packet marking or deterministic packet marking.

The proposed system keeps log the packet queues and drop details. The continuous packet drops are easily notified and alerting procedure is invoked to reduce the loss rate. The new approach helps in efficient packet forwarding in the router. The new system uses maximum throughput scheduling algorithm so as to serve high speed as well as normal TCP packets to flow efficiently. In proposed system it contains the several algorithms as such local flow monitoring algorithm mainly contribute the trace out the path while transferring the data with less degradation of data loss. In entropy variation during the specified time period client send the data from one system to another system. Ingress and outgress router of the path tracing can be carried out in a less period time. Capturing router can prevent packet loss with the respective known able IP address.

On the other hand, the proposed method can work independently as an additional module on routers for monitoring and recording flow information, and communicating with its upstream and downstream routers when the pushback procedure is carried out.

6. ADVANTAGES OF THE PROPOSED SYSTEM

The proposed system has following advantages,

- Statistical analysis of packets received, queued and dropped are possible with more information.
- Less time consuming in analyzing the packets.
- Minimize the packet loss rate.
- Assists in regulation of malicious packet sending nodes.
- Alert sending to affecting router.
- The proposed strategy can trace back fast in larger scale attack networks

7. FURTHER ENHANCEMENTS

Trace back mechanism from the currently adopted packet marking strategies. Many of the available work on IP trace back depend on packet marking, either probabilistic packet marking or deterministic packet marking. Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extra ordinary challenge on storage space at victims or intermediate routers. On the other hand, the proposed method needs no marking on packets, and therefore, avoids the inherent shortcomings of packet marking mechanisms. It employs the features that are out of the control of hackers to conduct IP trace back.

Some of the further enhancements that can be made in this system are as follows:

- The metric for DDoS attack flows could be further explored. The proposed method deals with the packet flooding type of attacks perfectly. However, for the attacks with small number attack packet rates, e.g., if the attack strength is less than seven times of the strength of non attack flows, then the current metric cannot discriminate it. Therefore, a metric of finer granularity is required to deal with such situations.
- Location estimation of attackers with partial information when the attack strength is less than seven times of the normal flow packet rate, the proposed method cannot succeed at the moment. However, it can detect the attack with the information that have accumulated so far using traditional methods.
- Differentiation of the DDoS attacks and flash crowds
- In this system, it did not consider this issue the proposed method may treat flash crowd as a DDoS attack, and therefore, resulting in false positive alarms

8. CONCLUSION

In this proposed an effective and efficient IP trace back scheme against DDoS attacks based on entropy variations. It is a fundamentally different trace back mechanism from the currently adopted packet marking strategies. Many of the available work on IP trace back depend on packet marking, either probabilistic packet marking or deterministic packet marking.

Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on storage space at victims or intermediate routers.

On the other hand, the proposed method needs no marking on packets, and therefore, avoids the inherent shortcomings of packet marking mechanisms. It employs the features that are out of the control of hackers to conduct IP trace back. It observes and store short-term information of flow entropy variations at routers. Once a DDoS attack has been identified by the victim via detection algorithms, the victim then initiates the pushback tracing procedure.

The trace back algorithm first identifies its upstream routers where the attack lows came from, and then submits the trace back requests to the related upstream routers. This procedure continues until the most far away zombies are identified or when it reaches the discrimination limitation of DDoS attack flows.

REFERENCES

1. Anubama Mishra, B.B.Gupta, R.C. Joshi " A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation technique".
2. T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems,” ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.
3. CLARK, D. D. 1988 “The design philosophy of the DARPA Internet protocols”. In Proceedings of SIGCOMM (Stanford, CA). 106–114.
4. GLIGOR, V. D. 1984. “A note on denial-of-service in operating systems”. IEEE Trans. Softw. Eng. 10, 3, 320–324.
5. N, R. M. 1994. “Denial of service: an example” Commun. ACM 37, 11, 42–46.
6. Carnegie Mellon Univ., Pittsburgh, PA Perrig,A. ; DawnSong 24,,Issue:10
7. GARBER, L. 2000. “Denial-of-service attacks rip the Internet” IEEE Comput. 33, 4 (Apr.), 12–17.
8. CHANG, R. K. C. 2002. “ Defending against flooding-based distributed denial of- service attacks: A tutorial”. IEEE Commun. Mag. 40, 10 (Oct.), 42–51.
9. MIRKOVIC,J. AND REIHER, P. 2004. “A taxonomy of DDoS attack and DDoS defense mechanisms”. ACM SIG-COMM Comput. Commun. Rev. 34, 2, 39–53.
10. Y. Kim et al., “PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks,” IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 141-155, Apr.-June 2006.
11. D. Moore, G.M. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” Proc. 10th USENIX Security Symp., Aug. 2001.
12. L. Garber, “Denial-of-Service Attacks Rip the Internet,” Computer, pp. 12-17, Apr. 2000.
13. P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing,” RFC 2827, 2000.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail i.e. **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals