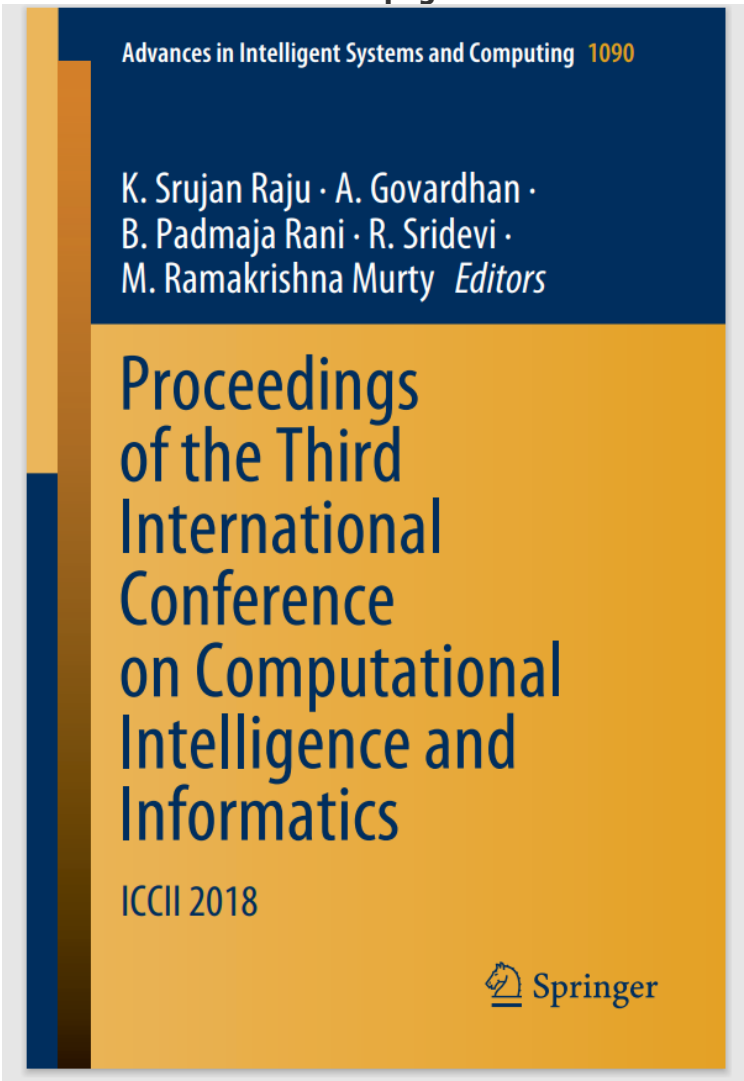
Cover page


Advances in Intelligent Systems and Computing 1090
K. Srujan Raju · A. Govardhan ·
B. Padmaja Rani · R. Sridevi ·
M. Ramakrishna Murty Editors
Proceedings of the Third International Conference on Computational Intelligence and Informatics
ICCII 2018
Springer

Content page

First page

Ain Shams Engineering Journal (2015) 6, 715–722

Ain Shams University

Ain Shams Engineering Journal

www.elsevier.com/locate/asej
www.sciencedirect.com

ENGINEERING PHYSICS AND MATHEMATICS

IP Traceback through modified Probabilistic Packet Marking algorithm using Chinese Remainder Theorem

Y. Bhavani [a,*], V. Janaki [b], R. Sridevi [c]

[a] Dept of Information Technology, Kakatiya Institute of Technology and Science, Warangal, India
[b] Dept of Computer Science, Vaagdevi College of Engineering, Warangal, India
[c] Dept of Computer Science, Jawaharlal Nehru Technological University, Hyderabad, India

Received 14 September 2014; revised 9 November 2014; accepted 2 December 2014
Available online 20 January 2015

KEYWORDS
DOS attack;
IP Traceback;
Chinese Remainder Theorem;
Modified Probabilistic Packet Marking algorithm

Abstract Probabilistic Packet Marking algorithm suggests a methodology to identify all the participated routers of the attack path by probabilistically marking the packets. In this approach, these marked packets contain partial information regarding the routers of the attack path. At receiver, to get the complete information of every router, it requires more number of marked packets and hence more combinations and more fake positives. To overcome this drawback we have presented a novel idea in finding the exact IP address of the routers in the attack path by applying Chinese Remainder Theorem. The result of our implementation reveals that our idea requires less number of marked packets and takes no time in constructing the attack path. The same idea is true even in the case of multiple attackers.

1. Introduction

Information transfer became very easy due to the invention of Internet. The speed of transmission has been tremendously increased and along with this, the attack rate has also grown exponentially. An "attack" is defined as a method of creating obstruction during the transmission of information. Due to the attacks all authorized persons are unable to retrieve the information while unauthorized people are successful in getting the information.

These attacks are broadly categorized as passive and active attacks. Generally passive attacks are difficult to detect but to some extent easy to prevent. Active attacks are difficult to prevent and simple to detect. In the active attacks, one of the most upsetting and very difficult task is to trace the adversary, called DOS attack, in which the legitimate people are unable to access the information. This is due to the intense logging of redundant packets sent by the attacker. This problem can be solved by finding the IP address of the attacker, but the IP

* Corresponding author.
E-mail addresses: yarram.bh@gmail.com (Y. Bhavani), janakicse@yahoo.com (V. Janaki), sridevirgm@yahoo.com (R. Sridevi).
Peer review under responsibility of Ain Shams University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.asej.2014.12.004
2090-4479 © 2014 Faculty of Engineering, Ain Shams University. Production and hosting by Elsevier B.V.