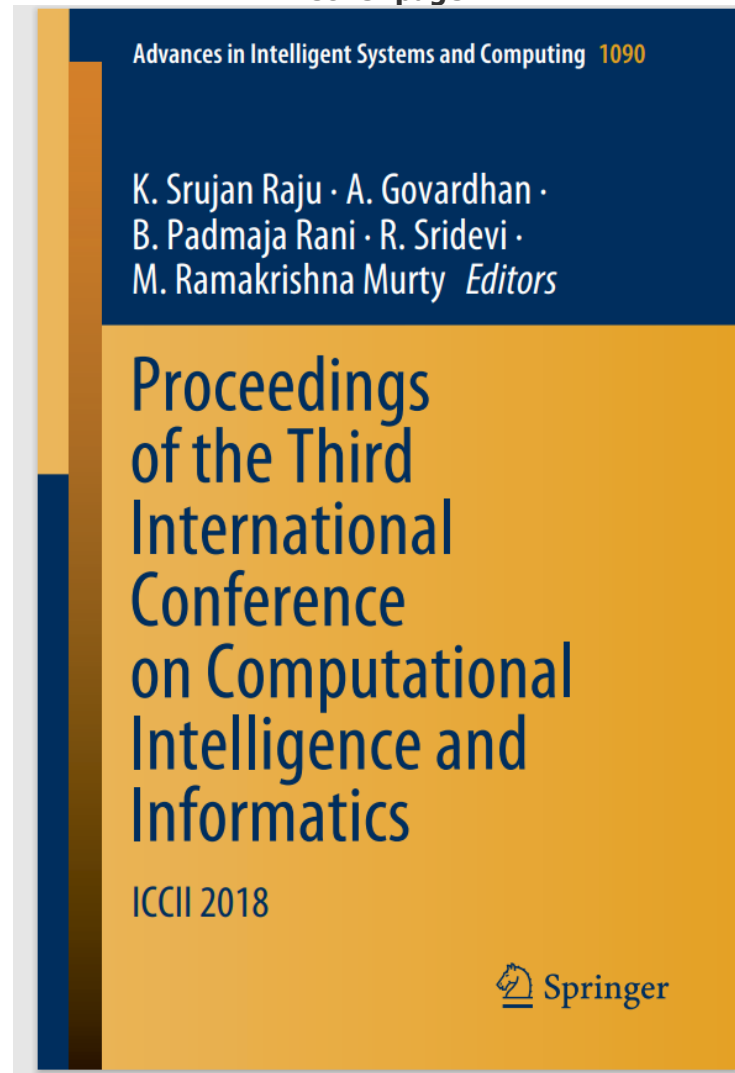


Cover page



Content page

x

Contents

A Survey on Deceptive Phishing Attacks in Social Networking Environments	443
Mohammed Mahmood Ali, Mohd S. Qaseem and Md Ateeq Ur Rahman	
Implementation of Spatial Images Using Rough Set-Based Classification Techniques	453
D. N. Vasundhara and M. Seetha	
Multi-objective Optimization of Composing Tasks from Distributed Workflows in Cloud Computing Networks	467
V. Murali Mohan and K. V. V. Satyanarayana	
IP Traceback Through Modified Probabilistic Packet Marking Algorithm Using Record Route	481
Y. Bhavani, V. Janaki and R. Sridevi	
Necessity of Fourth Factor Authentication with Multiple Variations as Enhanced User Authentication Technique	491
K. Sharmila and V. Janaki	
Performance Analysis of Feature Extraction Methods Based on Genetic Expression for Clustering Video Dataset	501
D. Manju, M. Seetha and P. Sammulal	
Identification of Cryptographic Algorithms Using Clustering Techniques	513
Vikas Tiwari, K. V. Pradeepthi and Ashutosh Saxena	
A Framework for Evaluating the Quality of Academic Websites	523
Sairam Vakkalanka, Reddi Prasadu, V. V. S. Sasank and A. Surekha	
A Survey on Analysis of User Behavior on Digital Market by Mining Clickstream Data	535
Praveen Kumar Padigela and R. Suguna	
Optimal Resource Allocation in OFDMA-LTE System to Mitigate Interference Using GA rule-based Mostly HBCCS Technique	547
Kethavath Narendra and C. Puttamadappa	
Review of Techniques for Automatic Text Summarization	557
B. Shiva Prakash, K. V. Sanjeev, Ramesh Prakash, K. Chandrasekaran, M. V. Rathamma and V. Venkata Ramana	
Data Mining Task Optimization with Soft Computing Approach	567
Lokesh Gagnani and Kalpesh Wandra	
Dog Breed Classification Using Transfer Learning	579
Rishabh Jain, Arjeeta Singh, Rishabh Jain and Praveen Kumar	



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, Vengal Rao 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.

© 2014 Faculty of Engineering, Ain Shams University. Production and hosting by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

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: ybhavani@ymail.com (Y. Bhavani), janakiv@yahoo.com (V. Janaki), sridevins@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.

This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).