International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Multipath Dynamic Source Routing Protocol using Portfolio Selection

Miss.Sruthi Raju[1], Miss.Rohini M. Muthal[2], Miss.Jyoti R. Gaidhani[3], Miss.Priyanka S. Brahmane[4]

[1] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[2] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[3] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[4] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*

Abstract - Multi-path source routing is widely used networks. This kind of routing allows data to transferred from source to destination with multiple paths. There might be jamming problems in this communication. Many proposed solutions given approaches to provide jamming aware allocation traffic to multiple paths. Explored a different new jamming aware traffic allocation taking the help of the concept of portfolio selection. We can also explore the problem of in network inference. The jamming statistics which are updated and which are made available to the nodes in the network. When the input node sends file to destination node, it will allocates traffic to various paths based on the jamming conscious knowledge and also it portfolio selection for best possible result. The goal of this approach is to use the available paths very efficiently besides reducing the possibility of jamming.

Key Words: *In-network inference, jamming aware traffic allocation, multipath source routing.*

1.INTRODUCTION

In the network jamming disrupts normal communication flow which is causing problems to the data transfer. It also leads various different attacks such as Denial of Service (DoS attack). Jamming occurs at physical layer of model which has its impact on network.

For this is the reason results pertaining to physical layer are to be used to solve this difficulty. Solutions like spread-spectrum and beamforming are some of examples for physical layer solutions. These solution discourage jamming attacks which are made by adversaries. Recent incidents proved that jammers are taking help cross layer protocol knowledge to made attacks and thus it reducing resource requirements for attack. These attacks could decrease the resource consumption to greater extent and thus made process of attacking as feasible as possible.

Confidentiality is created to prevent unauthorized users from accessing the sensitive data as it is subject to unauthorized disclose and accessible after being outsourced. Since the introduction of DAS, the confidentiality of outsourced data has been the initial focus among the various research community. To provide confidentiality to the outsourced data, encryption schemes are deployed.

Integrity can prevent outsourced data files from being changed and modified. Various schemes have been created to prevent the integrity of the outsourced data, such as proof of the retrievability and prov-able data possession. In these schemes, digital signature schemes and the message authentication codes (MAC) are deployed.

Query in data file storage is executed between a receiver and the proxy server. The proxy server can perform some of functions on the outsourced encrypted ciphertexts and convert them to those for the destination. As a result, the receiver can obtain the data file outsourced by the admin without the proxy server knowing the content of the data.

2.OBJECTIVE

In this section, we review the schemes which are related to identity-based secure distributed data storage (IBSDDS) schemes

1.1.1 Data Storage Systems
1.1.2 Outsourcing expanding from a data confidentiality to data utility, and pointed out the important research directions in protection of the externally

stored data. Kher and Kim surveyed the data storage system which are comprehensively and divided them into the three kinds based on their protective services: networked file systems (NFS), a storage-based intrusion detection systems (SBIDS) and cryptographic file systems (CFS).

Networked File Systems

In these systems, the proxy servers are assumed to be trusted. They authenticate the receivers and validate access authorities. The interactions between the proxy servers and a receivers are executed in a secure channel. Therefore, this systems cannot gave us an end-to-end data security, namely they cannot ensure the confidentiality of the data file stored at proxy server. In these schemes, a receiver authenticates himself to the proxy server using his password. Then, the proxy server passes authentication solution to the file owner. The owner will make an access permission according to the received information.

Architecture Diagram

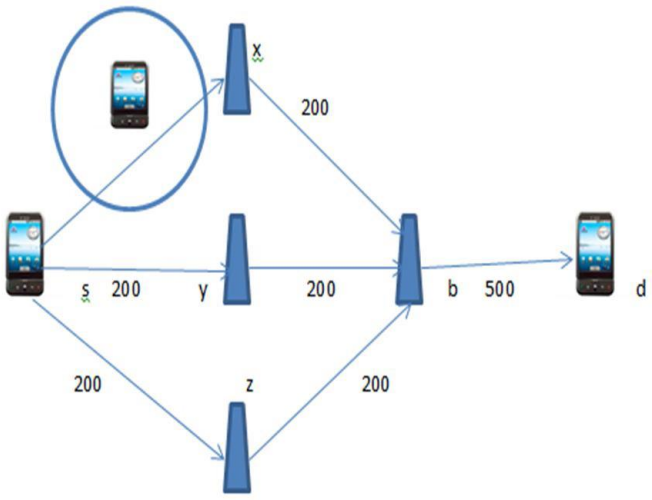

Fig -1: Source and destination with multiple paths

3. CONCLUSIONS AND FUTURE WORK

In this paper we implement multi-path source routing with jamming aware traffic allocation. We consider a network in the presence of jammers. The proposed network is built using NS2 which demonstrate the total traffic allocation among available paths. However, the network considers jamming statistics to make decisions for allocating traffic. Hence it is known as jamming – aware traffic allocation. The proposed solution also makes use of portfolio selection theory which was originally developed for making decisions on financial investments. The portfolio selection theiroy makes the network to be more robust to jamming. While making routing decisions, the source node considers jamming statistics and also portfolio selection approach for efficient traffic allocation which improves throughput and reduces congestion or jamming possibilities. The simulation results reveal that the proposed mechanism is effective can improve the performance of network.

REFERENCES

[1] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., 2001.

[2] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symposium, Washington, DC, Aug. 2003, pp. 15–28.

[4] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06), Washington, DC, Oct. 2006, pp. 1–7. G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs," Wireless Communications and Mobile Computing, vol. 5, no. 3, pp. 273–284, May 2005.

[5] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," IEEE Network, vol. 20, no. 3, pp. 41–47, May/Jun. 2006

[6] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, "MP-DSR: A QoSaware multi-path dynamic source routing protocol for wireless ad-hoc networks," in Proc. 26th Annual IEEE Conference on Local Computer Networks (LCN'01), Tampa, FL, USA, Nov. 2001, pp. 132–141.

[7] Patrick Tague, Sidharth Nabar, James A. Ritcey, and Radha Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 19, NO. 1, FEB 2011.

[8] H. Markowitz, "Portfolio selection," The Journal of Finance, vol. 7, no. 1, pp. 77–92, Mar. 1952.