iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XII **Month of publication:** December 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Defeating DOS Attacks in Low Rate Networks Using Network Multifractal

Shraddha C. Belsare[1], Anjali B. Raut[2]
Department of Computer Science & Engineering, HVPM, COET, Amravati & SGBAU, Maharashtra, India

Abstract— Nowadays, distributed denial of service (DDoS) attacks pose one of the most serious security threats to the Internet. DDoS attacks can result in a great damage to the network service. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defense technologies in the wireless networks. There are number of algorithms existing to counter Low rate DoS attacks but their performance and efficiency vary from one algorithm to another. In this paper we discuss how MFDFA algorithm works and also overcome the drawbacks of previous system and compare it.
Keywords: Low-rate denial of service (LDoS), multifractal detrended fluctuation analysis (MF-DFA), simulation.

I. INTRODUCTION

Distributed denial-of-service is a serious problem and many defenses have been proposed to handle this threat. A common evaluation platform is needed to comparatively evaluate these solutions. The fractal characteristic of network traffic is verified by MF-DFA (Multifractal Detrended Fluctuation Analysis) algorithm . The DFA algorithm is widely used in verifying the scale characteristic of monofractal and in detecting the long-range correlation of noisy nonstationary sequences. By using the MF-DFA algorithm researchers can achieve the multifractal spectrum easily and analyze the multifractal characteristic ofnonstationary sequences effectively. MF-DFA algorithm are as follows

Step 1: Computing the “profile”
Step 2: Dividing into non-overlapping segment.
Step 3: Fitting local trend polynomial by using least-square method for each segment.
Step 4: Calculating the qth order fluctuation function by averaging over all segments.
Step 5: Analyzing log-log plots.
Step 6: detecting the DOS attack in low rate network.

II. PROPOSED METHODOLOGY

In propose a method by which DDOS attacks IN low rate network can be detected and removed in wireless environments. This approach will be based on a time frame based tracking system, which will check the number of packets arriving in a particular time frame, and then take an action based on the packets and their signature from all the nodes. If the nodes are sending packets in a particular signature, then decide that the particular set of nodes is performing DDOS attack and can remove them from the network. This will help to improve the efficiency of the network, by reducing the overall delay and energy consumption needed to transfer a packet successfully from source to destination. In propsed methodology also used the MFDFA algorithm but in previous work of this MFDFA algorithm can only detect tddos attack but in proposed work algo can detect and remove the ddos attack in low rate network.

Following steps are used in MFDFA algorithm

Step 1: Computing the “profile”
Step 2: Dividing into non-overlapping segment.
Step 3: Fitting local trend polynomial by using least-square method for each segment.
Step 4: Calculating the qth order fluctuation function by averaging over all segments.
Step 5: Analyzing log-log plots.
Step 6: detecting the DOS attack in low rate network.
Step 7: If a particular node does not follow the fitting local trend polynomial step then remove the node from any communication in the network.

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. ADVANTAGES

A. It is useful for reducing Delay and energy

B. It improved the packet delivery over the communication channel. This system perform well even when traffic is occur over the network and produced maximum throughput

IV. RESULTS AND DISCUSSION

When ddos attack does not be generated following graph will be generated.

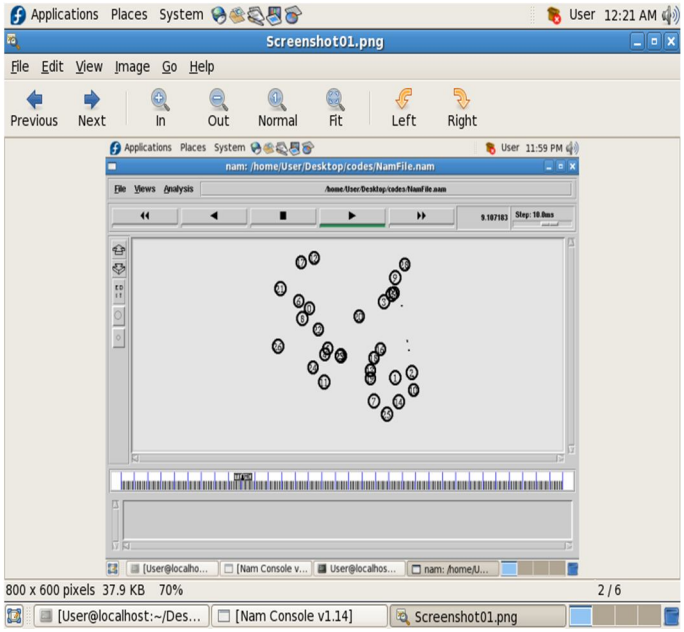


Fig1. ddos attack not generated

When ddos attack is perform on environment but not remove the ddos attack then generate the following graph.

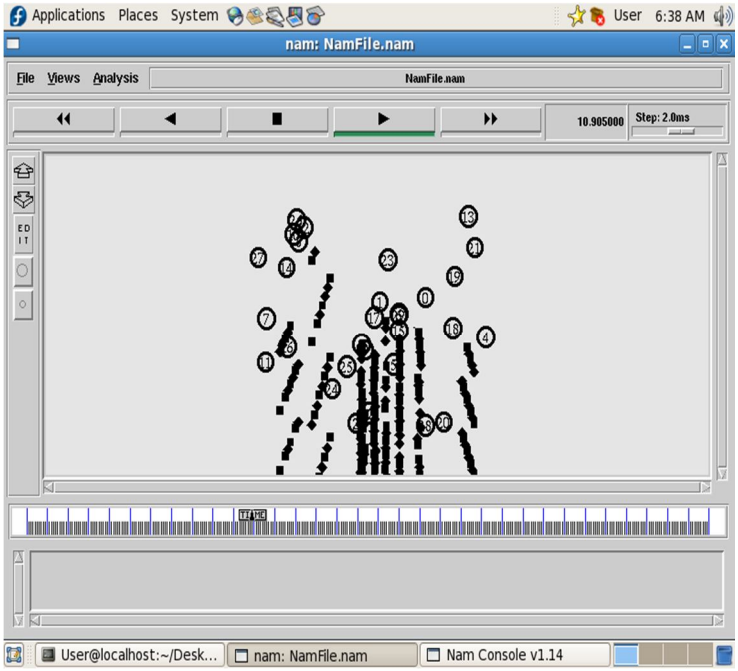


Fig2. Generate Ddos attack

When ddos attack is perform on environment and remove the ddos attack then generate the following simulation

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

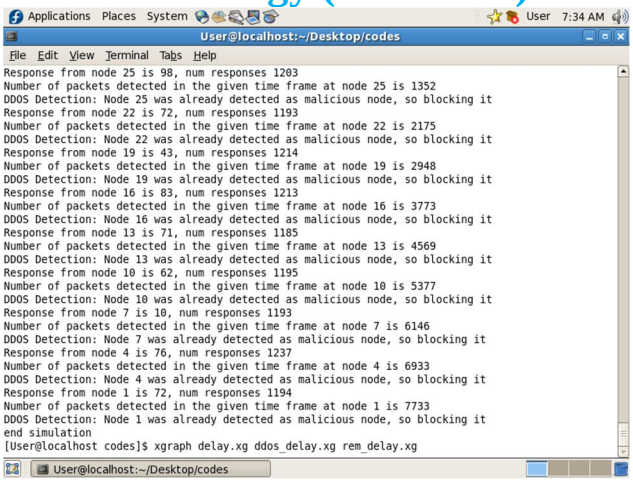


Fig3. Generate simulation when remove Ddos attack

And then generate the following graph to remove the ddos attack.

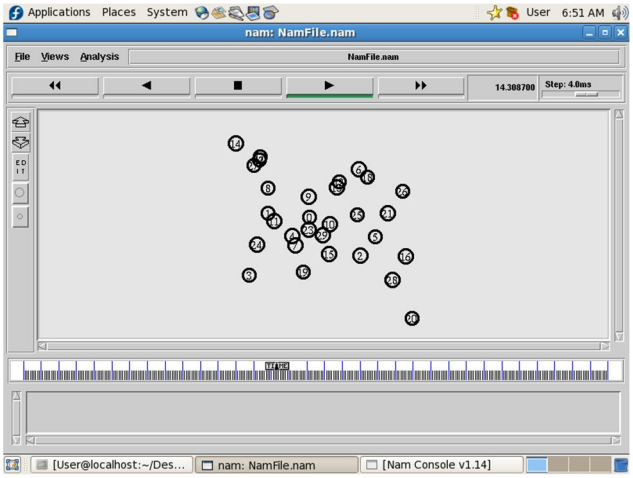


Fig4. Remove Ddos attack

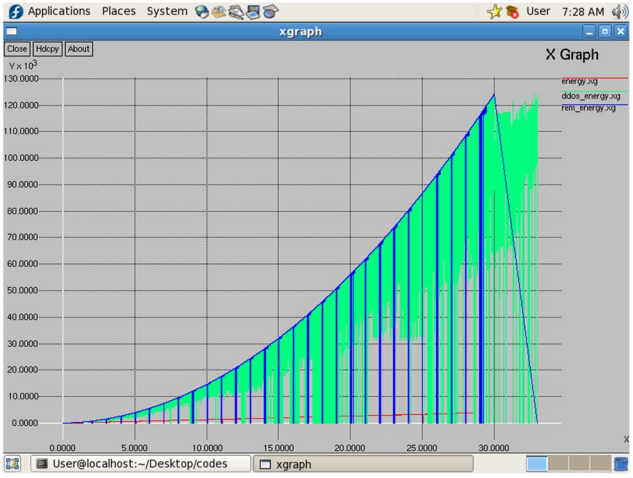


Fig 5. Comparison of energy metric

between previous methods and proposed system This graph shows energy consumed by proposed system is less than that of existing system. Green color shows energy consumed by proposed system when without removing ddos attack and red color

Volume 4 Issue XII, December 2016
ISSN: 2321-9653

shows energy consumed by existing system and blue color shows energy consumed by proposed system when ddos attack is remove.

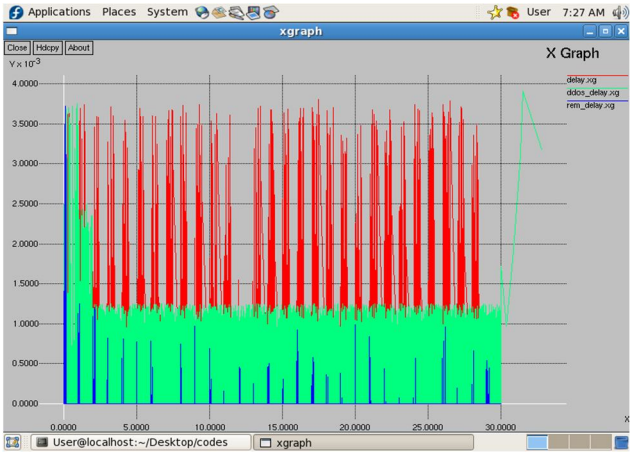


Fig 6. Comparison of delay metric

between previous methods and proposed system Above graph shows that metric delay is minimum using our proposed system as compared to existing system.

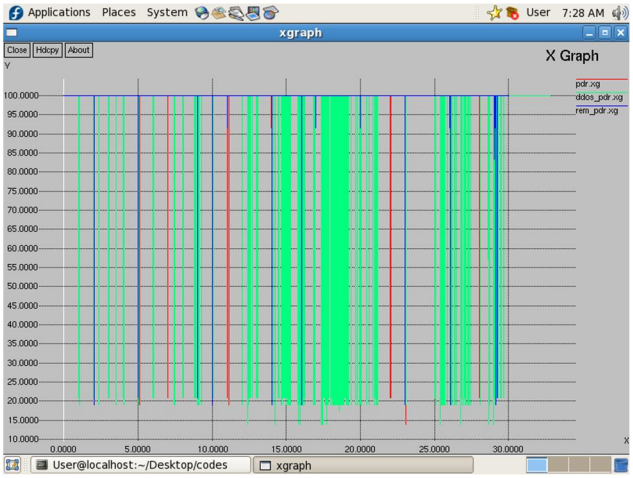


Fig 7. Comparison of packet delivery ratio(pdr)

between previous methods and proposed system Above graph shows that packet delivery ratio(pdr)is maximum in our proposed system as compared to existing system.

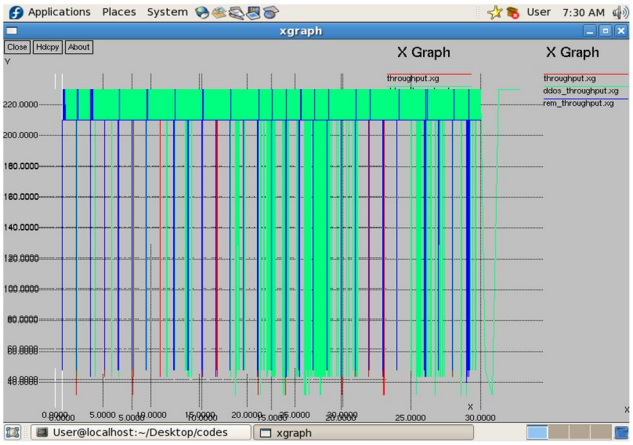


Fig 8. Comparison of throughput metric

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

between previous methods and proposed system This graph shows that throughput is high ,using our proposed system as compared to the existing system.

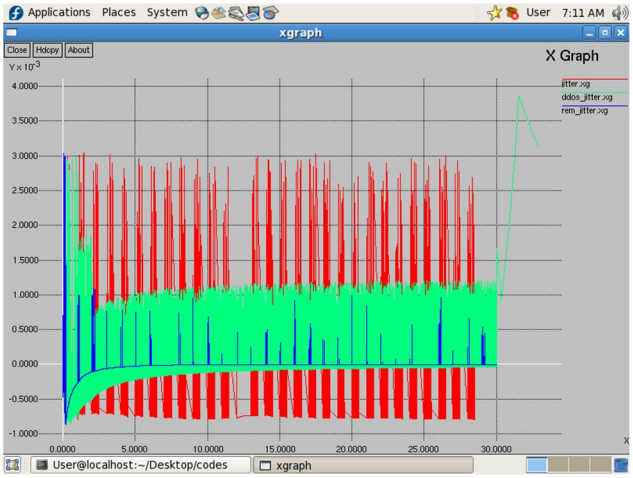


Fig 9. Comparison of jitter metric

between previous methods and proposed system Above graph shows that metric jitter is good in our proposed system as compared to existing system.

V. CONCLUSION

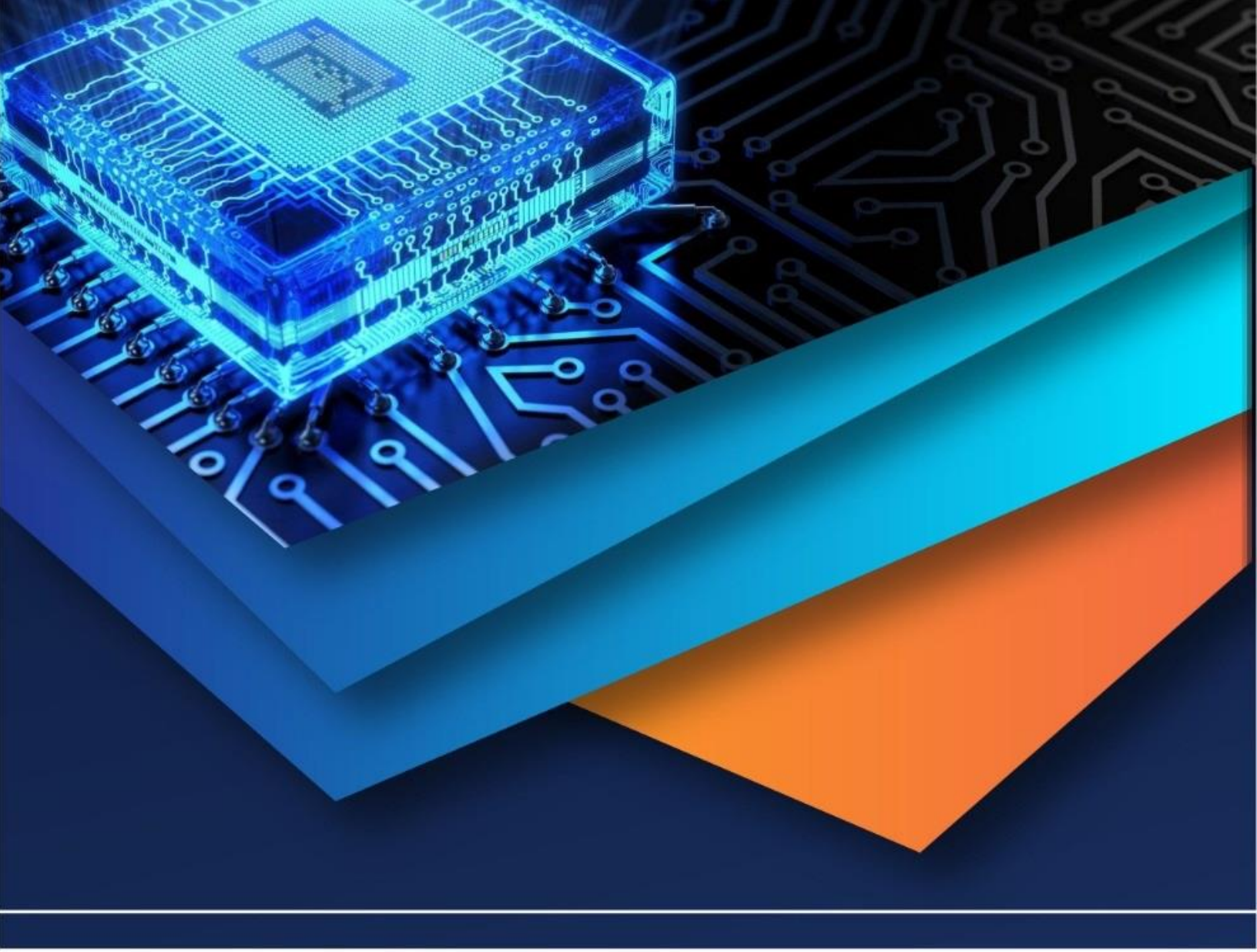
There are number of LDoS detection and prevention algorithms exist to tackle LDoS problem and their performance vary from one algorithm to another.. We believe that all of the algorithms surveyed in this paper are effective , but the advantages favors more time frame based tracking system which is help to improve the efficiency of the network, by reducing the overall delay, energy consumption and get maximam throughput matrix and get efficient result.

VI. FUTURE SCOPE

Future work, aims to investigate the use of DDOS (Distributed Denial of Service) attack in low rate network and extend DOS (Denial of Service) attack detection with multifractal technique using MFDFA algorithm and detecting and removing DOS attack in low rate network.

REFERENCES

[1] WU Zhi-jun, ZHANG Liyuan, YUE Meng, “Low-Rate DoS Attacks Detection Based on Network Multifractal” IEEE Transactions on Dependable and Secure Computing (Volume: 13, Issue: 5, Sept.-Oct. 1 2016)
[2] Liberious Vokorokos, Pvol Drienik, Olympia fortotira, “Abusing mobile devices for Denial of Service” IEEE 13th International Symposium on Applied Machine Intelligence and Informatics January 22-24, 2015 , Herl’any, Slovakia.
[3] ALlesso Merio, Mauro Migliard, Nicola, Franscesco palmerie and castigilione “A Denial of Service Attack to Umts Networks Using Sim-less Device” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014.
[4] Mojtaba Ayoybi Mobarhan,Moastafa Ayoubi Mobarhan “EVALUATION OF SECURITY ATTACKS ON UMTS AUTHENTICATION MECHANISM” International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012.
[5] Kazi walli ullah “Denial Of Service Attack On Umts Network” Computer Communications 34 (2011) 226–235.
[6] Georgios Kambourakis, Constantinos Kolias, Stefanos Gritzalis, Jong Hyuk Park “DoS attacks exploiting signaling in UMTS and IMS” Computer Communications 34 (2011) 226–235.
[7] Patrick P. C. Lee, Tian Bu, and Thomas Woo “On Detection of Signaling Dos Attack on 3G Wireless Network” P.P.C. Lee et al. / Computer Networks 53 (2009)2601–2616
[8] Rakesh Matam, Somanath tripathi “Denial of service attack on low rate wireless personal area networks” Communication (NCC), 2016 Twenty Second National Conference on
[9] Honowar H. Bhiyan, D.K bhattyachyarya,J.K.Kalita “Information metrics for low rate ddos attack detection” Contemporary Computing (IC3), 2014 Seventh International Conference on



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY