iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3173

www.ijraset.com

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

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Centralized Server Controlled Secure Packet Transmission in Military Network

D. Monica Lakshmi[1], M. Yuvalalitha[2], M. Dhivya[3]
[3]*Assistant Professor, Dept. of Computer Science & Engineering*
Panimalar Institute of Technology, Chennai, Tamilnadu, India

Abstract: ***The development of a novel wide-area centralized damping controller to improve the time consuming in presence of time-varying delay and packet dropout in the communication network. Two different strategies have been adopted to deal with the input and the output delays. In the first strategy, the system output delay has been compensated by predicting the packet drop. In the second strategy, a wide-area controller, based on delay-range-dependent stability criteria, has been designed for the time-varying delays in packet loss. In a large network file transfer between two nodes experience lot of challenges. There is minimum safety in file transfer between two source and destination. Malicious users and hackers will steal the data easily, the user may never know the data being transmitted in a secure way. Hence a Centralized Controlled Secure Packet Transmission is introduced. Here centralized server provides packet to the source node (Soldier) for encryption and it provides the key for the destination (Military Chief) for decryption. The centralized server also tells to the source, through which intermediate server, the encrypted file can be transmitted to the destination.***
Keywords: Centralized Server, Centralized Controlled Secure Packet Transmission*.*

I. INTRODUCTION

Social groups and their relationships have long been identified using Social network analysis (SNA). Inspired by SNA, researchers in digital forensic investigation have been employing similar network analysis techniques for identifying criminal communities, their relationships, and their influential leaders. As a result, digital forensic has emerged as an important tool for investigation crimes. Usually, forensic investigators study and analyze communication records for the purpose of identifying criminal communities and their leaders. So the information is secured.

II. LITERATURE SURVEY

Taimur Bhakhshi,Bogdan[1] proposes the control data plane Open Flow protocol, offering centralized authentic-time programmability and monitoring of network contrivances. Efficacious SDN predicated traffic engineering utilizing Open Flow, concretely in campus networking requires sophisticated authentic-time utilizer traffic visualization solution having minimum management overhead. To address the intuitive monitoring gaps in subsisting campus predicated SDN, the present paper proposes profiling campus utilizer traffic to visualize authentic-time network workload and accurately provision resources. The design solely utilizes subsisting Open Flow traffic quantifications, subjected to k-designates clustering to segregate users into different traffic classes (profiles) predicated on their application trends. The derived profiles represented consequential discrimination among utilizer application trends and were further benchmarked for high stability (96.1-99.1%),to as certain their viability for monitoring purposes. Adscititious simulation tests at varying utilizer loads attributed minimum computational cost and low Open Flow control overhead (4.02-4.96%) to the proposed approach, offering high scalability for authentic-time network monitoring and resource provisioning in the paper. Michihiro Koibuchi, Hiroki Matsutani, Hideharu Amano, Timothy Mark Pinkston[2] proposes that Survival capability is becoming a crucial factor in designing multicore processors built with on-chip packet networks, or networks on chip (NoCs). The mechanism provides default paths as backup between certain router ports which accommodate as alternative datapaths to circumvent failed components within a faulty router. Evaluation results show that, for a 2-D mesh wormhole NoC, only 12.6% adscititious hardware resources are needed to implement the proposed DBP mechanism in order to provide graceful performance degradation without chip-wide failure as the number of faults increases to the maximum needed to compose ring. Niels L. M. van Adrichem, Christian Doerr and Fernando A. Kuipers[3] proposes that ISPs over-provision capacity in order to meet QoS demands from customers. Software-Defined Networking and OpenFlow sanction for better network control and flexibility in the pursuit of operating networks as efficiently as possible. OpenNetMon polls edge switches, switches with flow end-points annexed, at an adaptive rate that increments when flow rates differ between samples and decreases when flows stabilize to minimize

the number of queries. The adaptive rate reduces network and switch CPU overhead while optimizing quantification precision. throughput, delay and packet loss quantifications for bursty scenarios in our experiment tested in the paper.

III. EXISTING SYSTEM

In existing system the file can be accessed easily by the hackers in the intermediate servers. The file will not be encrypted so the hackers can easily access the data. If the intermediated servers are busy in transmitting the file there will be packet loss and there will be increased traffic. We can't find which intermediate server is free.

A. Disadvantages

Takes extra time for packet delivery. Don't have the client side encryption. Security is less. Finding the free intermediate server is difficult.

IV. PROPOSED SYSTEM

In proposed system, centralized server controlled packet transmission is introduced. The centralized server takes care of secure file transmission and also finds through which intermediate server the file can be transmitted. The centralized server finds the busy intermediate server so that the file can be sent securely through the free intermediate server. The source node (soldier) gets encrypted key from centralized server and send the encrypted file to the destination(Chief) through the available free intermediate server and the destination node(chief) decrypts the file securely through the key received from the centralized server

A. Advantages

1) Files can be transmitted securely through encryption.
2) Low traffic since the file can be transmitted through the free intermediate server.
3) Busy intermediate server can be found.
4) Only the destination node can decrypt the file.
5) Hackers can't access the file in-between since it's in encrypted format.
6) RSA algorithm is used.

V. ARCHITECTURE DIAGRAM

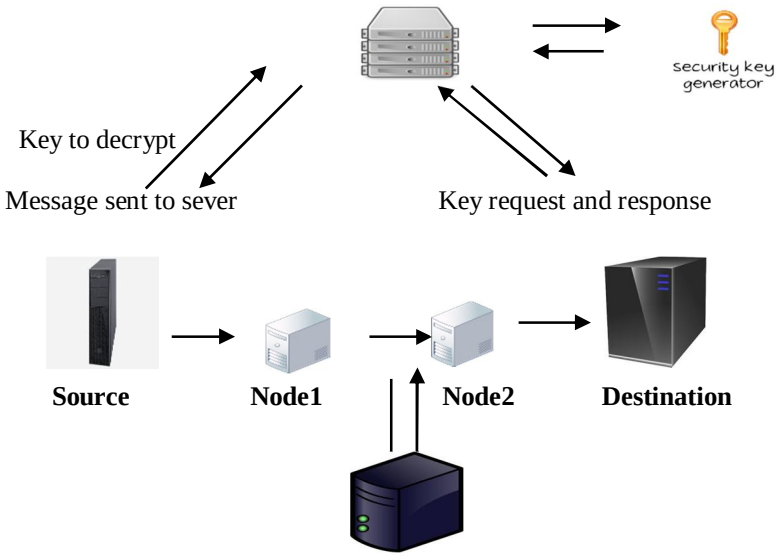


Fig -1: Block diagram of our proposed method

A. Finding Shortestpath

In this module, the shortestpath is found to transmit the messages. Centralized server controls the Packet transmission. The source to send the message will request the centralized server then the server provides the encryption key to encrypt the information and

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

decryption key will be generated to the destination whether received from it to read the message. The server handles shortest path from source to destination. Hence, packets will be transmitted easily from source to destination in a secured way.

B. Packet Encryption

In this module packet encryption occurs . The packets will be encrypted in server before transmitting the message such that there will be no loss of data and hacking is impossible. So in this module the packet is securely encrypted and the malicious nodes cannot steal the information. RSA algorithm is implemented for packet encryption so two level key will be generated (public key and private key). Public key is used for encryption and private key is used for decryption.

C. Key Generator

In this module, key is generated. When the centralized server receives the request to transmit the data through the packet, it generates the packet to the source to transmit the data. Server only sent the packet to source and the key will be kept by the server. When a hacker tries to access the packet it will be in the cipher text format. Thus the details of the packet is hidden from malicious persons.

D. Key Request

In this module, key request is done by the destination to decrypt the data. Once destination receives the packet, to decrypt the packet it requires the key. The destination send's request to the server then the server will check destination details after that server provide private key to the destination. Sometimes, if a hacker requests for the key to decrypt, the server does not send the key since that node will not be registered on the server side.

VI. RESULT AND DISCUSSION

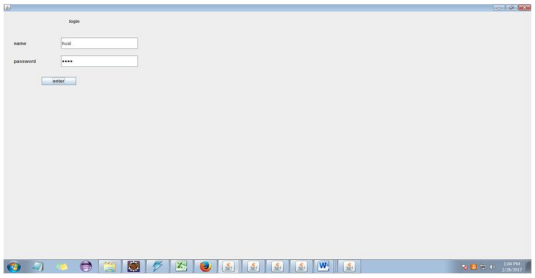


Fig.1 represent the user login to the page

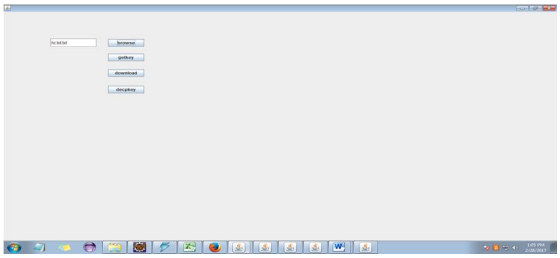


Fig 2.represent the main page

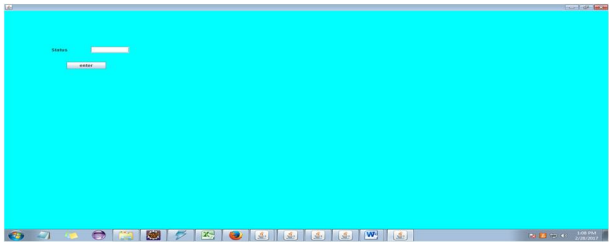


Fig 3.represent the Iteration1

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

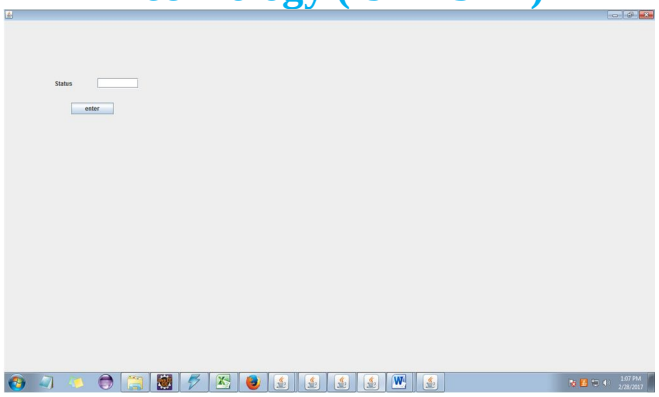


Fig 4.represent the Iteration2

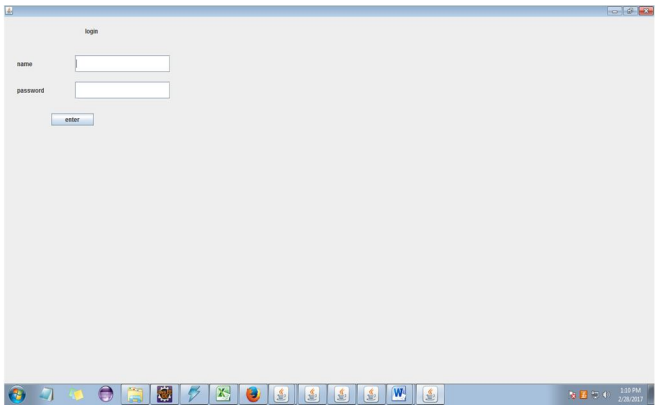


Fig 5.represent the Destination

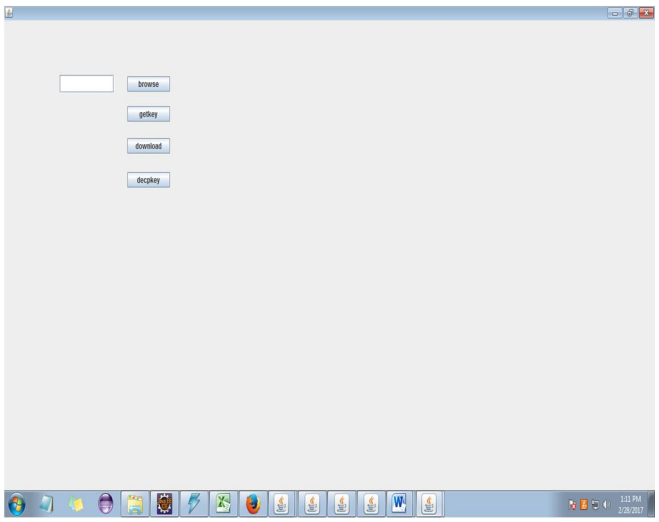


Fig 6.represent the Destination Page

VII. CONCLUSION

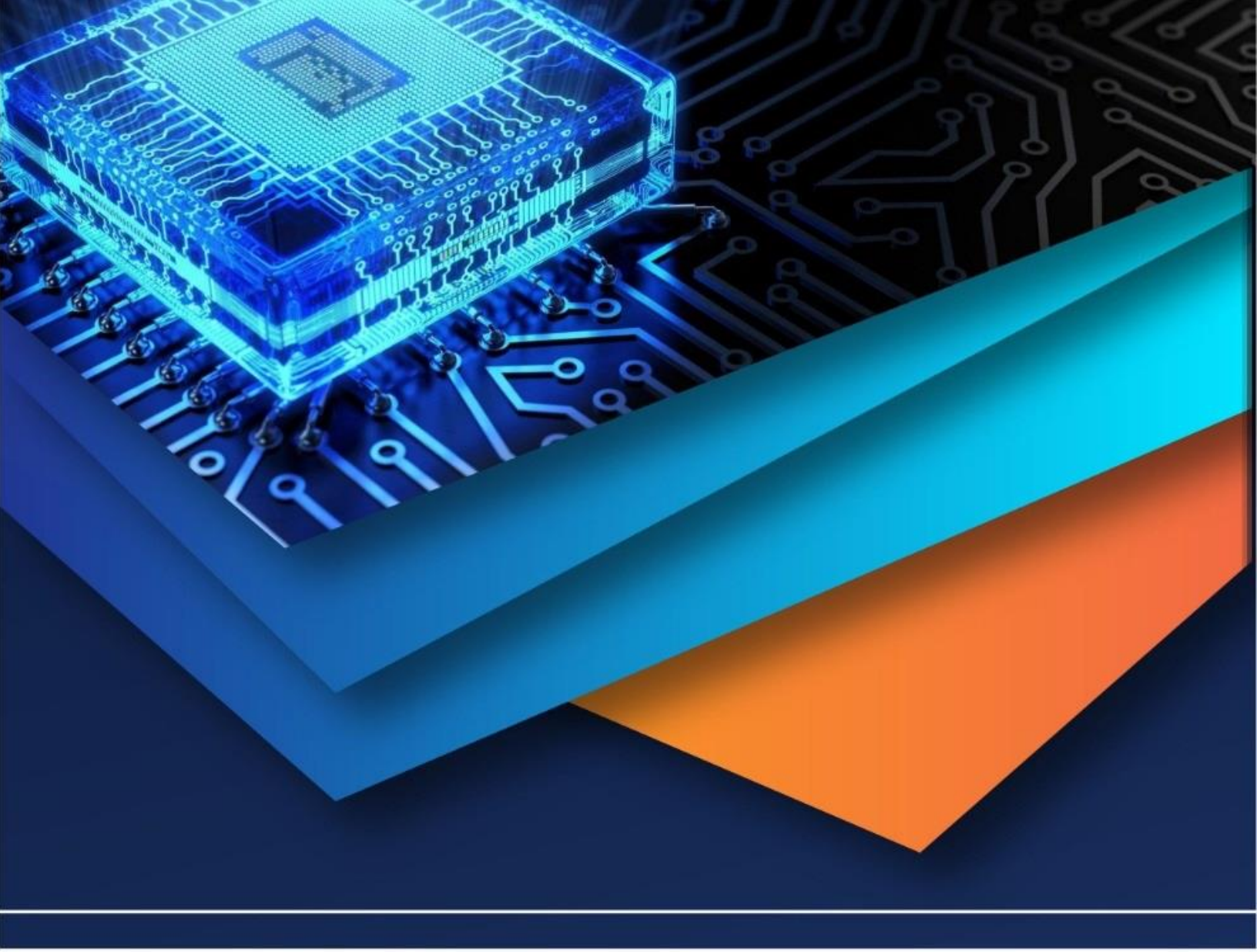
Thus, centralized server controlled secure packet transmission is introduced to transmit the file securely between source and destination by determining the free intermediate server and using the encryption process.

VIII. ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1] Open Flow-enabled user traffic profiling in campus software defined networks" , Taimur Bhakhshi and Bogdan, IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2016.
[2] A Lightweight Fault-Tolerant Mechanism for Network-On-Chip", Michihiro Koibuchi, Hiroki Matsutani, Hideharu Amano, Timothy Mark Pinkston , IEEE International Symposium on Networks-On-Chip2008.
[3] OpenNetMon: Network Monitoring in OpenFlow Software-Defined Networks.", Niels L. M. van Adrichem, Christian Doerr and Fernando A. Kuipers, 2014 IEEE 12th International Conference .



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY