Congestion Control, Routing and Security in Networks

Suchitha .S [1], Dr. B. G. Prashanthi [2]

[1]*Research Scholar, Bharathiar University and Assistant Professor, DSCE, Bangalore, India*

[2]*Associate Professor, St.Joseph's College, Bangalore, India*

Abstract **-** This paper deals with routing, congestion control and security. When the data is transferred between the source and destination systems, proper routing is required. If the packets are more in number, congestion may occur. So appropriate congestion control algorithm should be considered to reduce the traffic. Security aspects can be considered to transfer data in secure way. Using multipath routing the congestion can be reduced because packets can be transferred using multiple routes. Multipath routing also reduces the security attacks by maximizing the paths.The three important concepts of networks, routing, congestion control and security can be considered to transfer data in optimized and secured way.

Keywords **-** routing, security, congestion control, networks, multipath routing

I. INTRODUCTION

When the data is transferred between the nodes in the network, routing of packets has to be considered . The congestion near the nodes can cause delay in data transfer.

The data has to be sent in safer way, for this security is required.

Routing is the way used to transfer data across the networks. Route selection can be done on the various factors like distance, line cost, efficiency and other parameters. Router is used to transfer data in networks. Routing tables are used to decide on which route to choose to transfer data based on the routing table values. The routing algorithms are classified as adaptive and non-adaptive algorithms. The routing can be shortest path, flooding, link state, distance vector routing.

Congestion means more traffic in networks. It causes packet loss or data transfer delay. It may block the connection also.

Network layer deals with congestion. Congestion can be controlled either by increasing the available resources or by decreasing the load of the network.

Many congestion control algorithms are available. We can use general principles, virtual circuit subnet, load shedding, Jitter control, choke packets or congestion control policies.

Congestion can occur for various reasons. If the data arrives on a fast LAN is passed to a slower WAN, then congestion can occur. Congestion avoidance can be used to handle congestion. The packet loss can occur because of time out. The retransmission of packet has to be used.

Network uses congestion avoidance techniques to avoid congestion collapse. These technique includes the concepts like fair queuing method, CSMA/CA and Ethernet, window reduction in TCP.

There can be attacks like passive and active. In passive attack intruder can read the data and in active attack intruder can read and can also modify the data.

There are many aspects that has to be considered while sending the data packets like confidentiality, data integrity, authentication of the user. The other aspects of network security are access control, non-repudiation and digital signatures.

II. NETWORK SECURITY

When the data is sent between the source and destination system, it should be transferred in a secure way.

The basic aspects of Network Security are

Authentication: It verifies the user identity. It checks for genuine user. Identification of the user can be done by authentication process.

Confidentiality: Confidentiality deals with providing security from unauthorized person or third party. It is one of the basic service for network security.

Data Integrity: Data integrity deals with finding out whether the data is same as the host has sent or it has been changed. If any changes are there in the original data, that is specified. Original data should not be modified by unauthorized person.

Access Control: Access Control deals with controlling or limiting the resource access for security purpose. Only authorized person can use the data.

Digital Signatures: Sender can electronically sign the data using the concept of digital signature.

It is used for the message authentication.

Non-repudiation: When the data is exchanged between the two persons there may be dispute regarding data transfer. To solve this, non-repudiation can be used. In this service the person cannot refuse the previous action which he has done.

To send the data in a secure way encryption and decryption of data can be used.

$$C=E_K(P)$$
$$P=D_K(C)$$

Original message is plain text. It can be converted into cipher text by using encryption key. Cipher text is the output after encryption. Cipher text can be converted back into plain text by decryption key.

If the same keys are used for the purpose of encryption and decryption, this becomes symmetric key. If the different keys are used for the encryption and decryption then it is public key encryption. In public key encryption, we use two keys, private and public key for more security.

Basically there are two types of attacks. They are

- Passive attack
- Active attack

In passive attack intruder can read the data but cannot modify the data. The examples for passive messages are Release of message contents and traffic analysis.

In active attack intruder can read as well modify the data. Intruder can modify the message like deleting some portion of data , adding some extra data etc. Replay, masquerade, modification and Denial of service are active attacks.

III ROUTING, SECURITY AND CONGESTION CONTROL

When we transfer data, route is required between the nodes. Path selection is essential for routing of packets.

Congestion is very common because many packets travel in networks. Congestion may occur because of limited resources. One solution is that using multipath routing congestion problem can be minimized.

Multipath routing system can be used between the source and destination system. Using multipath routing the congestion can be reduced because packets can be transferred quickly using multiple paths or routes.

There is a one more issue in network that is security. Data which transfers through networks are vulnerable to various kinds of security attacks. So security is very essential for data. Always data transfer should be efficient , secure and optimized.

Security is very important when we transfer data in networking system. Multipath routing strategy is used for the purpose of security.

There are many advantages of multipath routing like reduced delay, load balancing, bandwidth aggregation and fault tolerance. In multipath routing path should be selected among many routes. The data has to be distributed between the paths.

Many multipath routing algorithms are present to provide security aspects. The data is divided into different routes to minimize the attacks by unauthorized users. Multipath routing reduces security attacks by maximizing the routes.

Basics of Multipath routing deals with

Route discovery

Route selection

Data distribution

Using multipath routing protocol, failure rate of packet delivery is reduced. In multi path routing, first paths should be discovered, then the appropriate path is selected and packet are distributed. After that path maintenance has to be done.

Multipath routing can be either node disjoint, or link disjoint.

There are various kinds of attacks. In selective forwarding attack the packets are dropped and data loss occurs. Multipath provides the solution to selective forwarding attacks of packets. When the packets are dropped it can be resend using other route. It improves packet delivery ratio in networks.

Distributed Denial of Service (DDoS) attacks are common in networks. There are many approaches to solve distributed denial of service attacks. Multipath routing is also one approach.

In DDoS attack unwanted traffic is created to prevent the usage of service provided by the networks. The disruption of services occurs because of DDoS.

Routing protocols have to be robust to security attacks and node failures. The factors like confidentiality, access control, reliability, authentication, integrity specifies the security level in networks.

The results can be simulated. First, nodes are arranged in a graph with communication lines. Initialization of nodes has to be specified. Data transfer requires routing. If the congestion occurs, using multipath routing data transfer can be done.

For selective forwarding attack and distributed denial of service attack multipath routing strategy can be used.

Packet delivery ratio between the normal routing procedure and multipath routing method has to be compared. The evaluation metric parameters are throughput, delay, packet loss. The multipath routing is an efficient method to deal with congestion and data security in networks.

IV CONCLUSION

This paper combines the concepts of routing, congestion control and security in networks. Routing is used to transfer data from one system to another system. Congestion may occur due to more traffic. This may slow down the packet transfer rate. Congestion control is used to control the load in networks. The data has to be transferred in secure way. Multipath routing provides the security to the data and it reduces the congestion so the data is transferred in optimized way.

V. REFERENCES

[1]. William stallings, “Network security essentials Applications and Standards” , pearson education ,third edition, ISBN 978-81-317-1664-9.

[2]. Eric Cole, Ronald Krutz, James W Conley, “Network Security Bible”, second edition, Wiley-India, ISBN 978-81-265-2331-3.

[3]. Larry L Peterson and Bruce S Davie,“Computer Networks A Systems Approach”, third edition, Elsevier.

[4]. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security PRIVATE communication in a PUBLIC world”, Second edition, Pearson, ISBN 81-7758-415-4.

[5]. William Stallings, “Cryptography and Network Security Principles and Practice” ,Fifth edition, Pearson.

[6]. Joseph Migga Kizza, ”Computer Network Security”, Springer International edition, ISBN 81-8128-558-1.

[7]. Andrew S Tanenbaum,“Computer Networks” , Fourth Edition, Pearson, ISBN 978-81-7758-165-2.

[8]. Behrouz A Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security”, second edition, McGRaw Hill education.

[9]. Srinivas Shakkottai and R. Srikant, Network Optimization and control, Foundations and TrendsR in Networking , Vol. 2, No. 3 (2007) 271–379.

[10]. Route Optimization in IP Networks, Jennifer Rexford

[11]. Ning wang, kin hon ho,George pavlou and michael howarth, University of surrey, “An Overview of routing optimization for internet traffic engineering”, IEEE communications surveys and tutorials,1st quarter 2008.

[12]. ex Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi ,“A Review of Routing Protocols for Mobile Ad- Hoc NETworks(MANET)”,International journal of information and education technology,vol.3,No.1, february 2013

[13]. William Stallings, “High Speed Networks and Internets performance and quality of services,” Second edition ISBN 978-81-7758-569-8.

[14]. Van Jacobson, Modified TCP Congestion Control Avoidance Algorithm,end-2-end-interest mailing list ,april 30,1990.

[15]. Peter Key, Laurent Massoulie and Don Towsley, “Combining Multipath Routing and Congestion Control for Robustness,” Cambridge UK.

[16]. Abu Zafar M. Shahriar, Mohammed Atiquzzaman, Senior Member, IEEE, and William Ivancic,“Route Optimization in Network Mobility: Solutions, Classification, Comparison, and Future Research Directions” , IEEE communications surveys and tutorials, vol.12, No.1,first quarter 2010.

[17]. Patrick Jaillet, Jin Qi,Melvyn Sim,”Routing optimization with deadlines under uncertainty”.

[18]. Raj Jain, “Congestion Control in Computer Networks : Issues and Trends,” IEEE Network Magazine,May 1990, pp. 24-30.

[19]. W. Stevens, TCP Slow Start, Congestion Avoidance, Fast Retransmit and Fast Recovery Algorithms, January 1997,RFC 2001.

[20]. Peter Dempsey and Alfons Schuster,”Swarm intelligence for network routing optimization” , Journal of telecommunications and information technology,2005.

[21]. Ratul Mahajan, Sally Floyd and David Weatherall , “Controlling High-Bandwidth Flows at the Congested Router,” AT&T Center for Internet Research at ICSI(ACIRI), Berkeley,CA.

[22]. Raj Jain, “ Congestion Control and Traffic Management in ATM Networks: Recent Advances and A Survey,” The Ohio State University, Columbus, October 15,1995.

[23]. Jiayue He, Ma’ayan Bresler, Mung Chiang and Jennifer Rexford, “ Towards Robust Multi-layer Traffic Engineering: Optimization of Congestion Control and Routing,” Princess University, USA, IEEE Globecom 2006.

[24]. Huaizhong Han,Srinivas Shakkottai,C.V.Hollot,R.Srikant,Don Towsley, ” Multi-path TCP: A Joint Congestion Control and Routing Scheme to Exploit Path Diversity in the Internet”,IEEE/ACM Transactions on Networking, Vol.14,No.6,December 2006.

[25]. Luca Muscariello, Diego Perino,”Evaluating the performance of multi-path routing and congestion control in presence of network resource management”,Orange Labs Paris,France Telecom R&D,INRIA Project Team ,France

[26]. Kari Visala,”Multipath Routing, Congestion Avoidance and DDoS Resistance”, Helsinki Institute for Information Technology HIIT/Aalto University School of Science and Technology

[27]. Jia Liu, Ness B.Shroff, Cathy H.Xia, Hanif D.Sherali, “Joint Congestion Control and Routing Optimization: An Efficient Second-Order Distributed Approach”,The Ohio state university

[28]. Wael Y.Alghamdi, Hui Wu, Jingjing Fei,Salil S.Kanhere, “Randomised Multipath Routing for secure Data Collection”,2014 IEEE Ninth international conference intelligent on sensors networks and information processing symposium on security,privacy and trust for cyber-physical systems,Singapore 21-24 april 2014.

[29]. Jiayue He and Jennifer Rexford, “Towards Internet-wide Multipath Routing” ,Princeton University,USA