HIERARCHICAL ROUTING WITH SECURITY AND FLOW CONTROL

Ajay Kumar V[1], Manjunath S S[2], Bhaskar Rao N[3]
[1]Department of Computer Science Engineering, DSCE, Bangalore, India
[2&3]Associate Professor, Department of Computer Science Engg., DSCE, Bangalore, India

ABSTRACT

For existing hierarchical network, the network is partitioned into smaller networks where each level is responsible for its own routing but no security and flow control mechanisms has been provided while routing the information, i.e. there is no investigation of ensuring security for hierarchical network routing. Hierarchical routing is used in internet routing such as OSPF. This paper proposes a method of providing both Security, Flow control and Routing analysis for Hierarchical Network Routing using Private Key Encryption and flow control mechanism to minimize packet loss. Joint analysis of Security, Flow control and Routing is used as it reveals the weaknesses in the network that remain undetected, when Security, Flow control mechanisms and Routing protocols are analyzed independently. A simulation result demonstrates the effectiveness of the proposed method in terms of delay, throughput.

KEYWORDS: *Authentication, Delay, Hierarchical Routing, Network Security, Flow Control, Packet Loss and Network Congestion.*

I. INTRODUCTION

HIERARCHICAL NETWORK ROUTING is a promising approach for point to point routing in networks based on hierarchical addressing. Hierarchical Routing was mainly devised to reduce memory requirements over large topologies. This topology is broken down into several Layers, thus downsizing the load on the routers. The router consists of routing table, the length of the routing table must be as small as possible and also the information that these routing table contains must be confidential from other routers. Hence, routers must ensure security. Private Key encryption is Symmetric Encryption. In symmetric encryption, a secret-key is used for providing security and for authenticating the user. A secret-key must be same at both sender and the receiver. Flow control is the process of managing the amount of data sent between two nodes to prevent a fast sender from outrunning the receiver. Classical flow control techniques depend on buffer size. This also involves a lot of message transmission from the receiver to the sender. Considerable overhead occurs under normal operation. If the receiver's buffer outruns, packet loss occurs. Packet loss can also occur due to network congestion, distance between sender and receiver. It is not possible to remove packet loss altogether. The fraction of lost packets increases as the traffic intensity increases. Of particular importance in understanding the dynamics of packet loss behaviour since it can have significant impact on TCP and UDP applications. Although sliding window based flow control is relatively simple, it has several conflicting objectives. The problem is finding an optimal value for the sliding window that provides good throughput, yet does not overwhelm the network and the receiver [7]. Packet Loss ratio is among the most important metrics for identifying poor network conditions, since it affects data throughput performance and the overall end-to-end data transfer quality. In our method, information will be sent to different router in a hierarchical manner when secret-key is matched and packet loss percentage is calculated and this information is used to control the next set of data to be

sent. The rest of the paper is organized as follows: Section 2 provides literature survey on hierarchical routing, flow control and hierarchical security. Section 3 introduces the proposed method of providing security, packet loss issues and authenticating the nodes for Hierarchical Network Routing using Symmetric Encryption. Section 4 shows the simulation results. This paper is finalized in section 5. This is followed by the Acknowledgement and References.

II. LITERATURE SURVEY

2.1. Hierarchical Routing

Hierarchical routing is the procedure of arranging routers in a hierarchical manner. The complex problem of routing on large networks can be simplified by breaking a network into a hierarchy of smaller networks, where each level is responsible for its own routing [5]. The advantages of hierarchical routing are as follows: It decreases the complexity of network topology, increases routing efficiency, causes much less congestion, and a reduction of topology information for minor nodes. The representation of hierarchical routing is shown in Figure 1 [4].

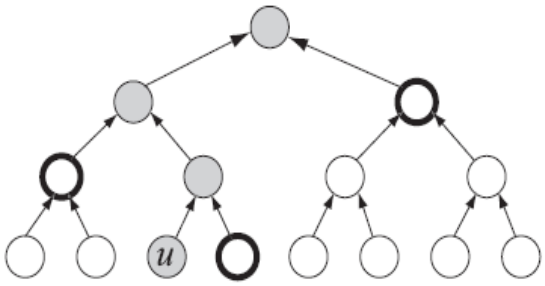

Figure 1. Hierarchical Routing

2.2. Security

Hierarchical Security allows security to be applied collectively to all the nodes in a hierarchy, without having to be defined redundantly for each node. Security goals guarantee the confidentiality, integrity, authenticity, availability and freshness of data [4].

2.3. Flow Control

Flow control enhances the rate at which the packets are sent to the neighbouring nodes in a hierarchical manner, by using packet loss data, hence minimising future packet loss and congestion control. The representation is shown in Figure 2.

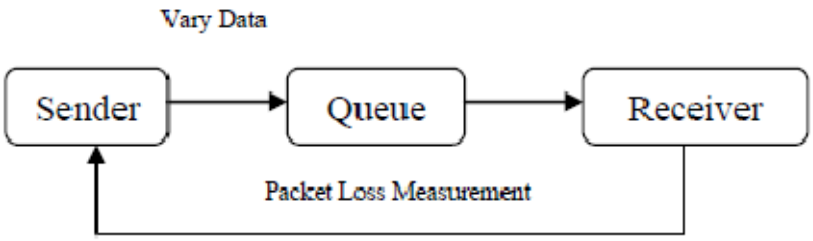

Figure 2. Packet Loss Measurement

III. PROPOSED METHOD

The purpose of this paper is to provide security in hierarchical network routing and flow control mechanism to minimize packet loss thus enhancing throughput of the packets. Many previous Hierarchical routing protocols assume a safe and secure environment where all nodes cooperate with no attack present. But the real world environment is totally opposite; there are many attacks that affect

the performance of routing protocol. To overcome this we ensure security and authenticity using Symmetric encryption. In our method every node is provided with a Secret-key. Every time the exchange of information takes place between the nodes, a secret-key should be matched. i.e., when a root node has to send information to its lower nodes then a secret key should be matched. Only then the information will go the respective lower nodes. The receiver follows the hierarchical routing protocol. When a data is received from a sender, a secret-key is asked for security purpose and for authenticating the node user, based on this information provided, the data is actually received to the main root node. For this information to be further sent to the lower nodes, a secret-key is asked by the root node to continue sending to the lower nodes and also for authentication. Now the information is sent to the lower nodes. Further if they want to send to their respective nodes, the same procedures will take place. Hence, both security and routing is achieved together in a hierarchy. Fig 3 shows the block representation of the work undertaken.

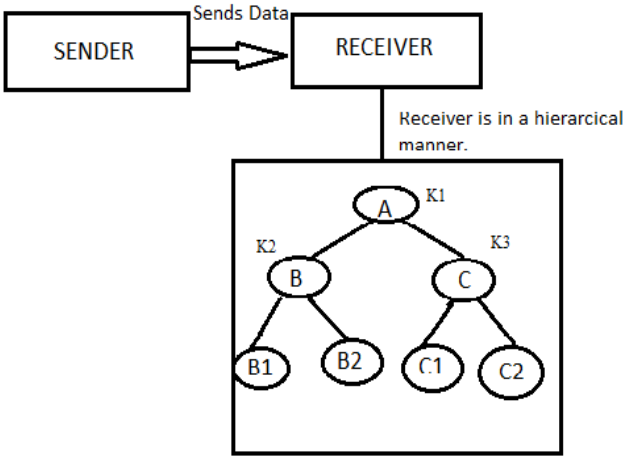

Figure 3. Block Representation of proposed method.

In the proposed method, between two nodes we calculate end to end packet loss and utilize this to transmit the next set of data. Input data is broken down into packets. The input data in this case is considered to be a file. These packets are sent to the Queue. Packet loss is created here in the Queue. The remaining packets are sent to the receiver. Packet Loss Measurement module first computes the amount of packets lost. When data is asked in the next session, amount of data to be sent then depends on the historical /previous transaction's estimation of packet loss. For the current data set, packet loss percentage is calculated. For the next data set, the amount of packets that would be lost is estimated. These many packets would then be deducted from the data set to be sent , thus enabling the sender to send only as much the receiver can receive. The remaining amount of data can be sent after an optimum amount of times.

IV. SIMULATION

4.1. Performance Metric

The performance of the proposed algorithm is evaluated through Delay, Throughput and Memory utilization. The delay is the expression of how much time it takes for a packet of data to get from one designated point to another. Latency in a packet-switched network is measured either one-way (the time from the source sending a packet to the destination receiving it), or round-trip (the one-way latency from source to destination plus the one-way latency from the destination back to the source). Throughput or network throughput is an average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bits/or bps), and sometimes in data packets per second or data packets per time slot. Bandwidth-Delay product refers to the product of a data link's capacity (in bits per second) and its end-to-end delay (in seconds). The result, an amount of data measured in bits (or bytes), is equivalent to the maximum amount of data on

the network circuit at any given time. Memory Utilization is the amount of memory consumed for the implementation of the method.

4.2. Simulation Setup

We compare the proposed method with existing Hierarchical Routing .We use MATLAB to evaluate the performance of the proposed method. Results are shown using line graphs.

4.3. Simulation Results

Figure 4 shows the delay estimate in the proposed method as well as the existing method. It can be easily seen that the delay in the proposed method is much lesser than that of the existing Hierarchical method. Figure 5 shows the throughput in proposed method as well as the existing method. The throughput is seen to be more than the existing method since the delay is found to be less. Figure 6 shows the memory utilization .The proposed method uses more memory than the existing system. This needs to be optimized and is seen as a future work.

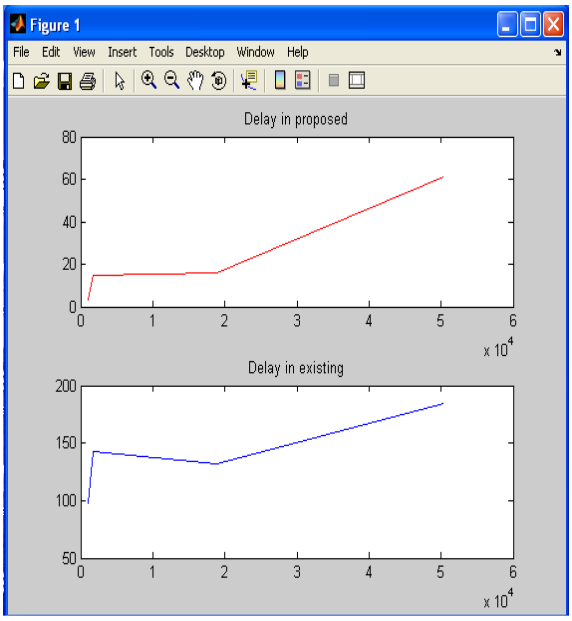

Figure 4. Delay

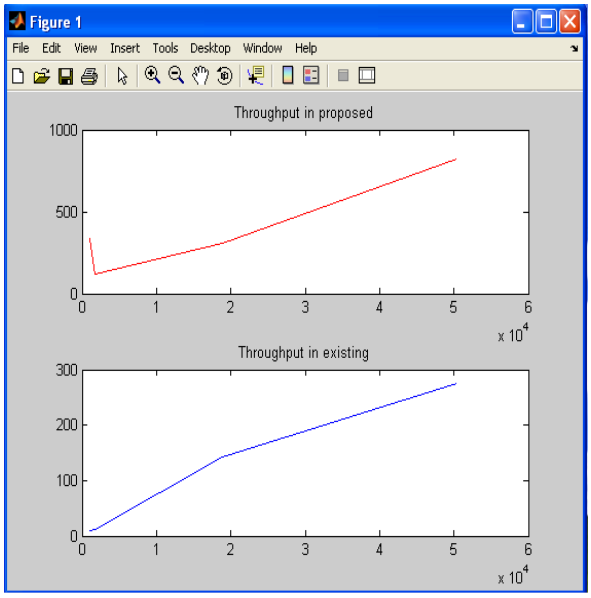

Figure 5. Throughput

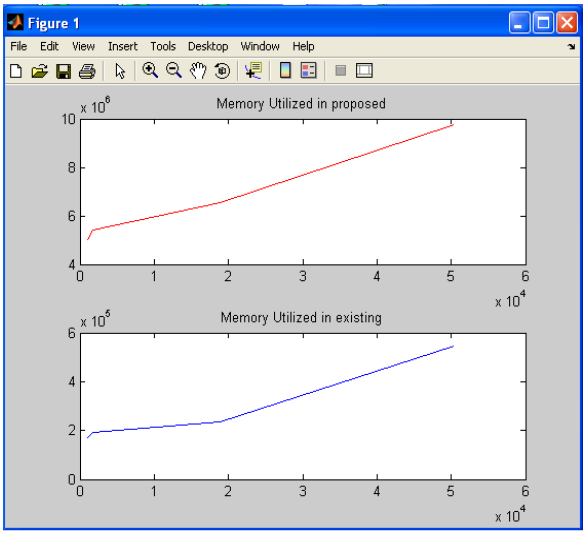

Figure 6. Memory Utilization

V. CONCLUSIONS

In this paper, flow control mechanism and security has been provided to the hierarchical routing, hence achieving security, flow control and routing in the hierarchical network. The main advantage of this approach is securing, minimizing packet loss and authenticating the individual node in the hierarchical network. Other advantage is to reduce the packet loss and topology information to the minor node, thus increasing the performance.

ACKNOWLEDGEMENTS

This paper would not have existed without my guide Professor Bhaskar Rao N. I also would like to thank our head of the department Dr. Ramesh Babu D.R, Associate Prof. Manjunath.S.S and my colleague Pranav Kurbet.

REFERENCES

[1]. Chris Karlof David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, F33615-01-C-1895.
[2]. Y. Zhang, N. Duffield, V. Paxson., and S. Shenker, "On the constancy of internet path properties," Proc. ACM SIGCOM Internet Measurement Workshop '01, San Francisco, CA, Nov. 2001.
[3]. Joel Sommers, Paul Barford, Nick Duffield, Amos Ron, "Improving Accuracy in End to end Packet Loss Measurement" ,SIGCOMM'05., Conference paper Digital Identifier No. ACM 1595930094/05/0008., Philadelphia, Pennsylvania, USA, Aug. 21–26, 2005.
[4]. Haowen Chan, Adrian Perrig and Dawn Song, "Secure Hierarchical In Network Aggregation in Sensor Networks.", *CCS'06,* October 30–November 3, 2006, Alexandria, Virginia, USA.
[5]. Leonard Kleinrock and Farouk kamoun, "Hierarchical Routing for Large Network", Computer Science Department, Univerisity of California, North-Holland publishing Company, Computer Networks 1(1997).
[6]. Leonardo B. Oliveira, Hao Chi Wong, Antonio A. Loureiro, Daniel M. Barbosa, "A Security Protocol for Hierarchical Sensor Networks", CNPq – process number 55.2111/2002-3.
[7]. Alexander Afanasyev, Neil Tilley, Peter Reiher, and Leonard Kleinrock, "Host-to-Host Congestion Control for TCP " , Manuscript received 15 December 2009; revised 15 March 2010.Digital Object Identifier 10.1109/SURV.2010.042710.00114.
[8]. B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad-hoc networks," Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.
[9]. Soufiene Djahel, Farid Nait Abdesselam and Ashfaq Khokhar, " A Cross Layer Framework to Mitigate a joint MAC and Routing Attack in Multihop Wireless Networks" 978-1-4244-4487-8/09/$25.00 2009 IEEE.
[10].Patrick Tague, David Slater, Jason Rogers, and Radha Poovendran, "Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis" , 1545-5971/09/$25.00 2009 IEEE.
[11].Chao Lv, Maode Ma, Hui Li and Jianfeng Ma, "A Security Enhanced Authentication and Key Distribution Protocol for Wireless Networks, 2010", 978-1-4244-8865-0/10/$26.00 ©2010 IEEE.
[12].Suraj Sharma and Sanjay Kumar Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks, 2011", Copyright_© 2011 ACM 978-1-4503-0464-1/11/02, *ICCCS'11* February 12-14, 2011, Rourkela, Odisha, India.

Authors

Ajay Kumar V has received B.E degree from VTU University, Belgaum and currently pursuing M.Tech degree in VTU University, Belgaum, Karnataka, India. His area of interest include routing, security, flow control in wired and wireless network.

Manjunath S.S has received B.E degree from Mysore University, Mysore and M.Tech degree from VTU University, Belgaum, Karnataka India. Currently he is working as a Associate Professor at Dayananda Sagar College of Engineering, Karnataka, India. Currently he is pursuing PhD in Mysore University. His areas of interests include microarray image processing, medical image segmentation and clustering algorithms.

Bhaskar Rao N has received B.E degree UVCE, Bangalore, M.Tech degree from IIS. Currently he is working as a Associate Professor at Dayananda Sagar College of Engineering, Karnataka, India. His area of interest includes teaching and research.