SRI BALAJI CHOCKALINGAM ENGINEERING COLLEGE
NBA Accredited and ISO 9001:2008 Certified Institution
Arni-632 317.
Thiruvannamalai District, Tamilnadu.
Visit us @ : www.sbcecarni.org
2nd NATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION ENGINEERING 2014

SECURITY AWARE SCHEDULER

D.Santhosh Kumari
Research Scholar
Department of Electronics & Communication Engineering
St. Peter's College of Engineering & Technology
Avadi, Chennai

Dr.K.Thirunadana Sikamani
Professor & Head
Department of Computer Science & Engineering
St. Peter's College of Engineering & Technology
Avadi, Chennai

***Abstract*-The Internet has become a commercial entity that need to provide its customers with quality-of-service (QoS) guarantees. Real-time network applications have been congesting the Internet. To provide the real-time network applications with the QoS guarantees, network technologies were developed by applying a scheduling algorithm. Conventional schedulers focus on the timing constraints but are much less effective in satisfying the security requirements. In this paper, an adaptive security-aware scheduling system for packet switched network is used. The system combines scheduling with security service enhancement (authentication security service). The scheduling unit uses the Diff-EDF scheduler and the security enhancement scheme adopts a congestion control mechanism. This approach helps meet both QoS and security requirements for data flows.**

***Keywords*- Quality of service, multi agent system, Security enhancement, Congestion control.**

I.INTRODUCTION

Internet has become a commercial entity that need to provide better services to its customers through QoS guarantees. Scheduling algorithm can be implemented to guarantee the required QoS for different data packets in the network. The QoS can be in the form of average total packet delay, miss ratio, reliability, jitter and throughput [1]. Different data streams in the real time network have been congesting the Internet.

Nowadays these data packets are required to be made robust against different security threats [2]. Therefore network has to keep a balance between providing the required security services and overall performances of the network by using scheduling algorithm [3]. The network performances can be measured by various network parameters as delay, miss ratio of packets, jitter and throughput. The factor that affects the network performance is the network buffer system utilization. This regulates the total data packets in the network and limits the network performance. In order to analyze the heterogeneous environment with QoS guarantees and security aspects multi agent system is used [4]. That provides security aware scheduling for data packets in the network by interacting with each other.

A network monitoring technique provides buffer estimation at the destination by using the algorithm. It provides a network congestion control and protects the network from being congested by heavy traffic load. With the algorithm, the authentication security level of the packets can be adapted through the congestion control without affecting the network performance parameters. Therefore the QoS can be guaranteed for all data packets.

II.AUTHENTICATION/DIFF-EDFSECURITY AWARE SCHEDULER

It combines the Differentiated Earliest-Deadline-First (Diff-EDF) scheduler with the authentication security services. The architecture has 3 main agents they are source, destination, edge router. The edge router has 4 sub agents as coordinator, server, buffer queue, and scheduler. Each entity has its own sub tasks and behavior**.**

2.1 Source Agent

It generates data packets. This may be audio, video or text. The source agent sends the traffic with rate of λf. Which is used for packet inter arrival time. Then packet service rate is given as μf which is used for packet service time. The relative deadline of traffic is Df. A QoS requirement is specified for traffic in terms of deadline miss ratio Φf. In order to overcome the fake representation injected into the packets. The source agent uses cryptographic security algorithms. We implement 3 authentication security algorithm like Hash function, Diffie-Hellman algorithm and HMAC-SHA-1 algorithm [6]. They

are applied to the data packets by source agent. Among them hash function is weakest algorithm and HMAC-SHA-1.These security services are used according to the security level requirement of each packets. The source agent interacts with coordinator by sending requests to serve its packets with QoS requirements.

2. *Edge router sub agent*

Coordinator agent interacts with other agents. Since it is at edge router it interacts with source and destination. It also monitors the system behavior and changes if needed. The scheduler agent uses Diff-EDF scheduler which enforces timing constraint on the packet to provide QoS [5]. It uses the effective deadline for packet as

$$Def = Df + Cf . \quad (1)$$

Similarly effective deadline miss rate is given by

$$\hat{}\Phi f = \exp (Davg - Cf) . \quad (2)$$

Where Cf *is* the coordinator parameter. This is obtained by taking ratio of deadline miss rate and smallest deadline miss rate. *D*avg is the average effective deadline of all packets**.**

If the effective deadline is smaller than deadline miss rate , coordinator send accept message to the source agent and sends packet to the scheduler. The scheduler performs on the packet to obtain the effective deadline. The scheduler then forwards the packets to the queue agent , which queue packet based on its effective deadline. Then server agent complete the serving for the packet. Coordinator interact with queue agent to de - queue the process. The queue agent fetches a packet that is closest to expire and forwards it to the scheduler. Scheduler passes the packet to the server.

Server serves the unexpired packet or drop the expired packet .Then forward the packet to the destination. The server keep record of number of packet served for destination and sum of time difference for served packets. The coordinator stores the information about different cryptographic algorithm that is used for enhancing the packets authentication security service [7]. The coordinator determines the length of buffer that is needed to enhance the packet with security by using total processing time of the packet with 2 delay like 1.Delay due to the packets having equal priority. 2.delay due to the preemption of the process when an arriving packet is closer to expiration than the remaining time of current processing packet. The processing time of the traffic is given as below,

(3)

Tf-Time required to decrypt a packet. Coordinator compares the length of available buffers at the destination with length of buffer needed to enhance the packet using different authentication algorithm. Depending on that it uses the strongest algorithm to the packet. Based on that it enhances/ reduces the security level or stay at the same level. No notification will be sent to source if the packets are needed to be sending at the same security level. Upon receiving a notification source applies new security algorithm to the packets to be sent.

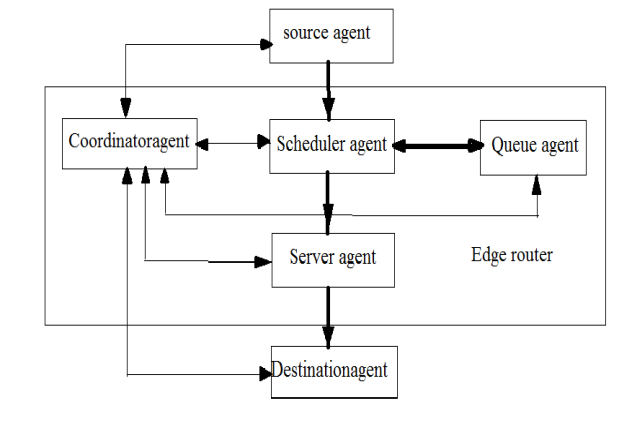

Fig .1. Multi agent system model

In the figure thick solid line represents the data transfer in the network and the thin solid line represents the interaction among agents in the network.

2.3 *Destination agent*

It receives packets from the server agent. It sends processing rate of the packets and available buffer at the destination to the coordinator agent [8]. These information are used to enhance security in the network. This information is exchanged periodically by them.

III.NUMERICAL RESULTS

The scheduling scheme with security enhancement is performed through simulations. The network consists of N distinct pairs of source and destination. Where total number of nodes in the network is 20.Each source has sending rate of λf..The packet size is fixed here because it is the maximum Ethernet payload. The source starts sending packets with lowest security level and expects to receive notification of security level change from the edge router. The length of

initial available buffer (maximum buffer) at the destination is chosen to be o $\lambda f/25$, $\lambda f/8$ and unbounded buffer. The coordinator periodically performs the security enhancement.

3. *Security Enhancement and QoS*

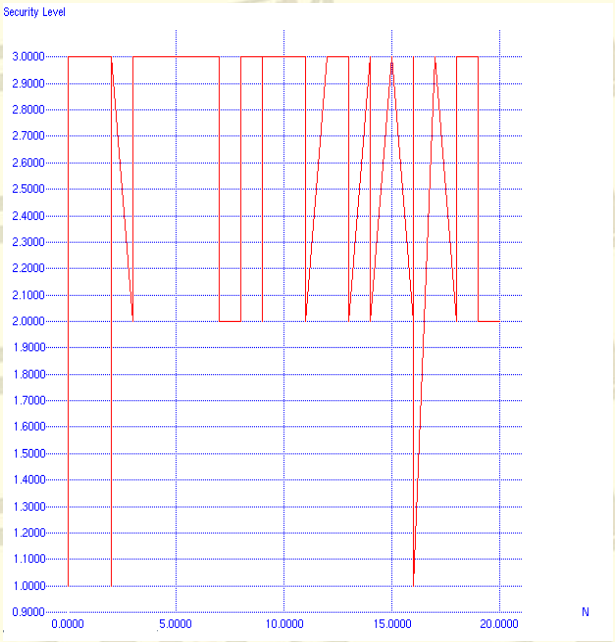

Fig. 2. Security level enhancement

This simulation result demonstrates the performance of the proposed algorithm at the destination agent. Fig 2. Shows the effect of buffer consumption of the destination agent which contributes to the network congestion. Then it also represents the security level changes based on the various security algorithms used. Then Fig. 3 represents the total packet delay. The security service level with larger number of available buffers will be higher since destination has more flexibility in decrypting packets.

In this simulation we demonstrate the efficiency of using the Diff-EDF algorithm at the scheduler agent. Fig.3 and Fig.4 shows 2 QoS metrices respectively, the packet loss ratio (at the server agent) and average total packet delay (at queue agent). Therefore this scheduler is suitable for all real time applications with time critical video, audio, or text packets.

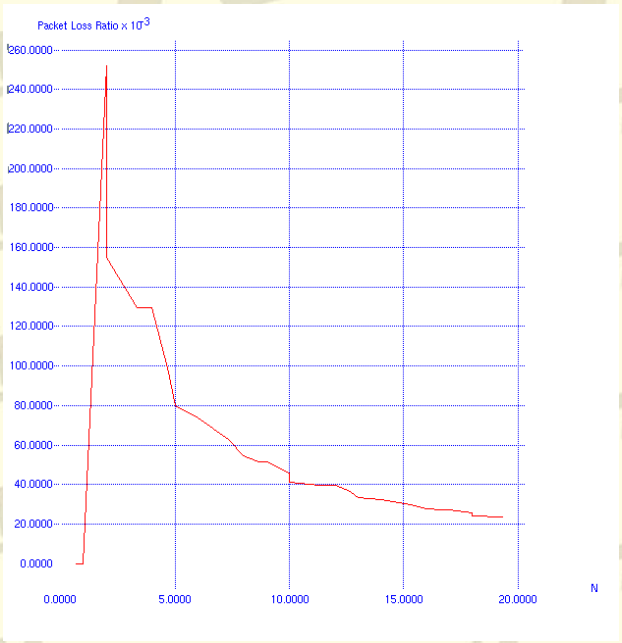

Fig. 3. Packet loss ratio at server agent

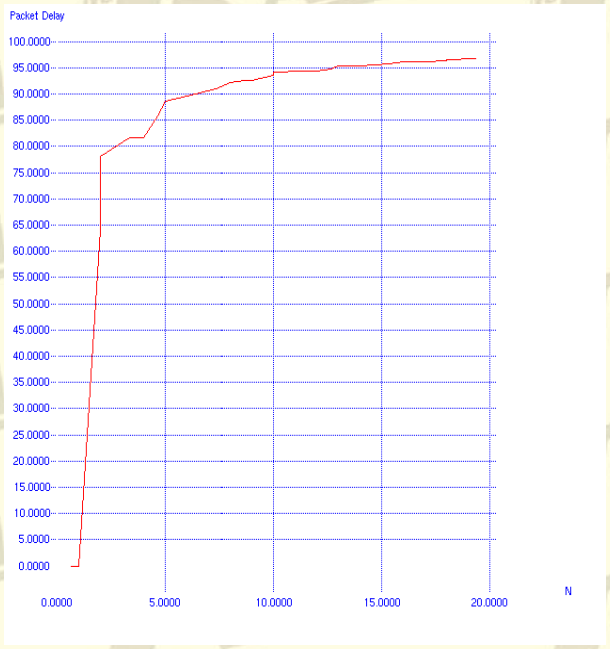

Fig.4. Packet delay at queue agent

IV. CONCLUSION

In this paper a security aware scheduler based on an object –oriented multi-agent system model is proposed. It combines the Diff-EDF scheduler with an adaptive authentication enhancement unit. This architecture efficiently utilizes the network's buffering system and regulates the traffic load in the network. The proposed scheme preserves the network performances by meeting both QoS and security requirements. The future work includes performing the security enhancement and QoS improvement by applying Hierarchical scheduling algorithm to serve the packets in the network.

REFERENCES

[1] K. Zheng, L. Lei, Y. Wang, Y. Lin, and W. Wang, "Quality-of-service performance bounds in wireless multi-hop relaying networks," *IET Commun.*, vol. 5, no. 1, pp. 71–78, Jan. 2011.

[2] M. Menth, B. Briscoe, and T. Tsou, "Precongestion notification: New QoS support for differentiated services IP networks," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 94–103, Mar. 2012.

[3] J. J. Jaramillo and R. Srikant, "Optimal scheduling for fair resource allocation in ad hoc networks with elastic and inelastic traffic," *IEEE/ACM Trans. Netw.*, vol. 19, no. 4, pp. 1125–1136, Aug. 2011.

[4] T. Xie and X. Qin, "Security-aware resource allocation for real-time parallel jobs on homogeneous and heterogeneous clusters," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 5, pp. 682–697, May 2007.

[5] E. Cody, R. Sharman, R. H. Rao, and S. Upadhyaya, "Security in grid computing: A review and synthesis," Decision Support Systems, vol. 44, pp. 749–764, 2008.

[6] R. Xie, D. Rus, and C. Stein, "Scheduling multi-task multi-agent systems," in Proc. Int. Conf. Autonomous Agents, May 2001, pp. 159–160.

[7] H. Zhu, J. P. Lehoczky, J. P. Hansen, and R. Rajkumar, "Diff-EDF: A simple mechanism for differentiated edf service," in Proc. IEEE Real- Time Embedded Tech. App. Symp., 2005, pp. 268–277.

[8] T. Xie and X. Qin, "Scheduling security-critical real-time applications on clusters," IEEE Trans. Comput., vol. 55, no. 7, pp. 864–879, Jul. 2006.