Dynamic Secure-Aware Real Time Scheduling Algorithm for Packet Switched Network

[1]Girish Tiwari
Associate Professor
Department of Electronics and Comm. Engg,
Ujjain Engg. College, Ujjain
tiwari_girish@yahoo.com

[2]Dheeresh Mishra
PG Scholar
Department of Electronics and Comm. Engg,
Ujjain Engg. College, Ujjain
dheereshmishra@gmail.com

Abstract:Now a day wireless networks are mostly preferred over wired networks because wireless networks are flexible and required no wire. If we talk about successful communication then end to end delivery of message is very important. In a heavy loaded networks scheduling of packets are key, by the proper scheduling of packets we can improve the guarantee ratio hence overall performance of the network is improved. If we focus on real time communication then real time packet scheduling plays an important role for enhance the performance of the system. In any network security plays a vital role, to protect the data from intruder and many security threats proper security of data is very important. So we can say that overall performance of the system is a combination of security and scheduling. In this paper we talk about real time packet scheduling in wireless networks. Here we use Dynamic Secure-Aware Real-Time Scheduling Algorithm for Packet Switched Network [DSASA]. This is a dynamic real time packet scheduling technique which reduce packets drop, increase guarantee ratio of data traffic and provide security for data packets.

Key words:*Real time packets scheduling,EDF, Guarantee ratio, packets drop, network Security.*

*****

I. INTRODUCTION

In this era, computerized network applications are mainly depending on the ability of the serving packet switching networks and provide different quality of services guarantees based on the traffic type. The qualities of services (QoS) are different in different types of network. There are many QoS like, Packet miss ratio, bandwidth, throughput, packet delays and any combinations of the above matrices. There are so many methods to provide such QoS guarantees, proper packets scheduling among them is very effective to provide such QoS [1] [5].

In computerized networks there are different types of traffic but the main two types are real-time traffic and non-real-time traffic, non-real-time traffic is also called best effort. If we talk about best effort traffic then there is no requirement of guarantee, but in the case of real-time traffic QoS guarantee plays a vital role. In real-time application time constraints are important. In real-time networks data packets must meet end to end deadlines. Real time traffics are also of two type hard real time and soft real time. In case of soft real time there is flexibility of timing constraints but in the case of hard real time any flexibility of timing constraints are not allowed [7] [8] [11].

In any type of network Scheduler is the one who decides the next packet to be transmitted among multiple packets. First-Come-First-Serve Scheduler is used for non-real-time type of data traffic where there is no requirement of QoS guarantee. Earliest Deadline First Scheduler mostly used in real-time data traffic, it is basically a priority based scheduler.

Security is another important factor in any computerized networks. Wireless network are open to everyone so there are more number of attacks are possible in wireless network compare to wired network. Attacks like Denial of Services are more common and more dangerous in wireless network.

Due to these unwanted attacks we need a secure channel for end to end communication. For real-time applications, a balance is required between security requirement and overall network performance [9] [11]. In any computerized network some important security requirements are describe below.

a) Data Confidentiality and Integrity: Confidentiality of data is very important, it means only the valid individual read the information or message which is transmits by the sender to receiver. Integrity shows that the entire message does not open and alter between the sender and the receiver, data should be reached in the same format to the receiver as it was sent by the sender. For a strong network these two requirements are important [4] [6].
b) Mutual Authentication: It shows identification along with verification. It is also a key requirement for any network [4].
c) Availability: It indicates how strong the network are, which is also a key requirement of the system. It means the network resources are available for every legal user [6].

These above security requirements are very essential for any general network.

In this paper weDynamic Secure-Aware Real-Time Scheduling Algorithm for Packet Switched Network [DSASA]. Under this scheduling algorithm we discuss Earliest Deadline First scheduler for dynamic real time packet scheduling. This scheduler prioritizes the data flow and gives more priority to the data which has short deadline. This scheduler also provides adaptability means it control the overloading of data flow hence reduce miss ratio.

II. RELATED WORKS

Packet scheduling is very important if we want to achieve high performance in real-time wireless network. To achieve overall performance of the system, security is also play an important role in wireless mobile commercial applications. So for real-time applications scheduler needs to guarantee both security and real time constraints of packets.

M. Saleh et al. gives a comparative study between FCFS (First-come-first-serve) scheduling algorithm and EDF (Earliest deadline first) scheduling algorithm for packet switched network. This comparative study conclude that FCFS is suitable for best effort data traffic system where no need of QoS guarantee are required, only arrival rate of data are required for scheduler to make any decision and EDF is suitable for real-time dynamic data traffic system where QoS are required, EDF is a priority biased packet scheduling. EDF gives more priority to the packet which has short deadline i.e. less remaining time for the packet to expire and gives less priority to the packet which has long deadline, so EDF decreases packet miss ratio when compare to FCFS packet scheduling [11].

Two base line algorithm Min and Max [12], Max: In this algorithm security gives more importance than guarantee ratio, initially incoming packets assign maximum security and store in the queue, the drawback of this scheme is guarantee ratio of the system decreases. Min: In this scheme scheduling gives more priority than security, initially incoming packets provide minimum security and store in the queue, drawback of this algorithm is security level of the system is decreases.

Qin X. et al. proposed a real time algorithm [SPSS] which provide real-time packet scheduling and also improves the security level of data packets. Initially this security algorithm assigns minimum security level to all incoming data packets and after that increases the security level of data packets according to requirement. This algorithm also maintains the guarantee of the packet deadlines. When system workload increases then this algorithm suffers from packet drops [2].

Xiamin Zhu et al. addressed an ISAPS algorithm. This algorithm increases overall performance of the system by improving both security levels as well as guarantee ratio. Initially it assigns the minimum security level to the incoming data packets and according to the system need it adjust the security level by security level controller. When system is overloaded it mainly focuses to the scheduling so security level is decreases [3].

In this paper we propose a dynamic secure aware real-time packet scheduling algorithm. In this algorithm we use EDF scheduler which prioritizes the incoming data according to its deadline. In this algorithm we decreases packet drops in real-time packet scheduling here we also provide security mechanism to secure the data.

III. SYSTEM MODEL

3.1 *Scheduler model with Assumption*

Fig shows the diagram of packet scheduling system for real-time network. Here we model a wireless channel, where packet scheduling is done between source and destination. In this system model Source is the real time data packet generator, suppose that it generates up to n real time data packets. Here P1 is the packet1 and Pn is the packet nThe size of data packets is fixed p_i =1500 bytes, maximum size of the Ethernet packet frame is also 1500 bytes.

The real time data traffic s sends by the source with a rate of λ_s. An exponential distribution with mean $1/\lambda_s$ is used to model the packet inter arrival time. The deadline d_i associated with real time traffic is model by uniform distribution.. Monitor interacts with entire system to coordinate their functionalities. Monitor check the incoming packets admission properties if it is ok then packets resides in the accepted queue otherwise packets drop in to the rejected queue. Monitor interacting with the source using a known IP address and with the destination using a known MAC address. It also interacts with security level controller, accepted queue and server to successfully deliver the packets. Security level controller adjusts the level of security of the data packets which is resides in the accepted queue.

EDF scheduler schedules the data packet according to the deadlines of the data packets. Data packets those have short deadline assign highest priority and data packets which have long deadline assign minimum priority. Server is mainly used to serve the real time data packet which is scheduled by the scheduler to the destination. It decides whether to serve or drop a packet based on the packets remaining time till expiration. if the packet is expired then it sends to the rejected queue and if not expired then it sends to the specific destination according to the MAC address.

Service time of the packets modeled by the exponential distribution with mean $1/\mu_s$, where μ_s is the packet service rate. Destination receives the packet by the server according to the FCFS scheduling algorithm.

1.2 *Security model with assumption*

TABLE 1 Security level of different algorithm

Cryptographic algorithm	**Sl_i: security level**	**w_i: KB/ms**
SEAL	0.1	168.75
RC4	0.2	96.43
BLOWFISH	0.3	37.5
Khafre	0.4	33.75
RC5	0.5	29.35
Rijndeal	0.7	21.09
DES	0.9	15
IDEA	1.0	13.5

This paper discusses about Real-Time packet scheduling as well as security requirement of the real time system hence to improve the overall performance of the real-time system. The key security services which are necessary for real time packets are confidentiality, authentication and data integrity. The security overhead is used to achieve required QoS with minimum rejection of packets.

When data packets travel in wireless medium chances of attacks is more so there is a need of security. So for Real time packets assigns the level of security according to the situation of the network system. By the use of encryption and decryption algorithm security like authentication, confidentiality and data integrity can be achieved. For some standard encryption algorithm, the security level is shown in the table below. Here each security algorithm is assigned with the security level in the range of 0.1 to 1.0 on the basis of security performance. Security level of security algorithm can be calculated by using following equation [12],[5].

$$sl_i = 13.5/ w_i \ \{0.1 \leq i \leq 1\}$$

Where,

sl_i = confidentiality security level of packet p_i

w_i = security performance of the i^{th} standard encryption algorithm

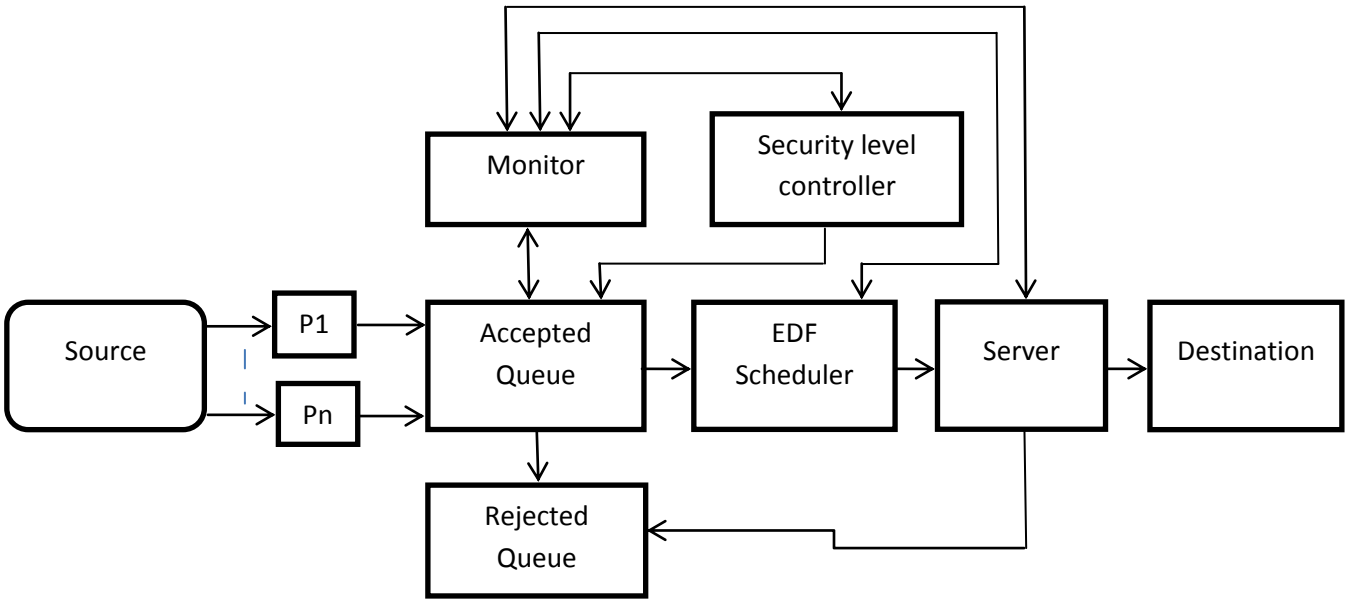

Fig.1.DSASA scheduling model

IV. DSASA ALGORITHM

This is an real time packet scheduling algorithm. In this algorithm we give more priority to scheduling rather than security so we want to reduce number of packets drop.

In this algorithm source generates the real time packets, the deadline of packets are abided by uniform distribution. These incoming packets are temporarily stored in the queue. Monitor perform the packets admission test which based on the admission condition.

Admission condition $tp_i < d_i$ ----------(1)

$$tp_i = pt_i + t_i + so_i \quad \text{----------(2)}$$

where

tp_i = total processing time of i^{th} packet

pt_i = processing time of i^{th} packet

t_i = transmission time of i^{th} packet

so_i = security overhead of i^{th} packet

d_i = deadline of i^{th} packet

if this admission condition satisfied then packets are stored in the accepted queue otherwise packets are dropped in to the rejected queue. Monitor initially provides minimum security level to the data packets and then inform to the security level controller to increase security level to the data

packets according to the situation. These packets then schedule by the Earliest deadline first scheduler according to the deadline of the packets. Packet which has short deadline provide maximum priority and packets which has long deadline provide minimum priority. This priority wise scheduling called dynamic scheduling, advantage of such type of scheduling is packets drop decreases and guarantee ratio increases. If packets are coming large in number then scheduler inform to the monitor to reduce the packets rate so packets are not going to drop. These scheduled packets then forwarded to the server by the wireless channel. Server is responsible to serving the real time datapackets to the destination. Packets which expire its deadline are drop in to the rejected queue and packets which are not expire its deadline are forwarded to the destination. Server also provides feedback to the monitor if packets drop ratio increase. Monitor adjusts the parameter like processing time, security level to reduce the packet drop ratio. Destination performs the FCFS algorithm on the received packets from the server.

V. SIMULATION RESULTS

DSASA is a real time packet scheduling algorithm. Here we mainly focus on scheduling. To calculate the performance of our algorithm, we compared with Security-Aware Packet Scheduling Algorithm [SPSS][2] and Improved Security-Aware Packet Scheduling Algorithm[ISAPS][3] in terms of number of packets being dropped and guarantee ratio. In this comparison total number of packets taken common constrain. Guarantee Ratio (GR) [3] can be defined as:

$$GR = \frac{\text{Total number of packets Accepted}}{\text{Total number of packets}} \times 100\%$$

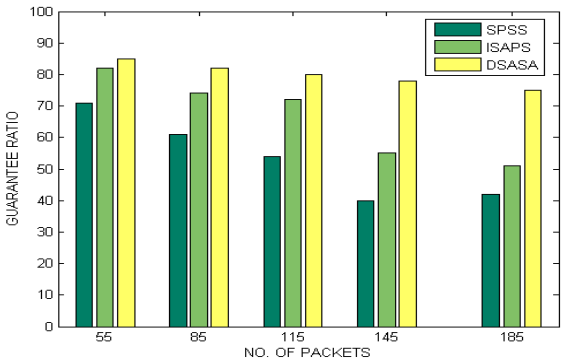

Fig.2. Comparison of Guarantee ratio

Fig.2. shows the comparison of guarantee ratio of packets among other two packet scheduling algorithm. In this simulation we taken range of packets 55-185, Fig indicate that guarantee ratioof ISAPS is greater than SPSS, and the guarantee ratio of DSASA is greater than both scheduling algorithm ISAPS and SPSS in each instance. In any real time system application guarantee ratio should be high.

Fig.3 shows the comparison of packet drop among SPSS,ISAPS and DSASA. In this comparison we take packet range from 55-185. In this simulation we evaluate that packets drop are increases as the number of packets increases, among three algorithm DSASA has minimum number of packets drop throughout the result shown in fig. below. In any real time network system packet drop should be as low as possible.

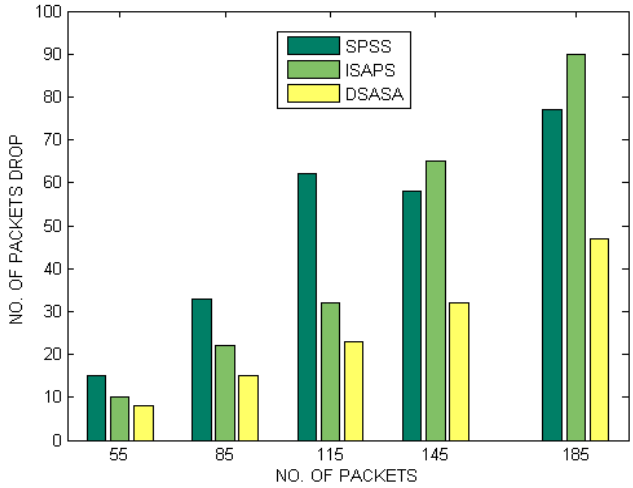

Fig.3. Comparison of packets drop

VI. CONCLUSION

Improvement of overall performance in any system is very important factor. In real-time system proper scheduling of data packets are a key to improve the overall performance of the system.

In this paper we discuss dynamic security aware real time scheduling which provide better scheduling compare to prior two already existing algorithm. The simulation results show that DSASA has better guarantee ratio as well as minimum number of packets drop compare to SPSS and ISAPS algorithm. This algorithm is also suited for heavy load system, under heavy load minimum level of security provided so guarantee ratio does not decrease and in case of light load maximum security provided so it increase the security level. This concludes that our algorithm is best suited for dynamic real-time packet switched network.

For the future work, we extend our algorithm to serve both the real-time (video, audio) and the best-effort (text) data flows, and security improvement is also concern.

REFERENCES

[1]. Maen Saleh, Liang Dong, “Real-Time Scheduling With Security Awareness for Packet Switched Networks”, IEEE Radio and Wireless Symposium (RWS) 2012.

[2]. Qin X, Alghamdi M, Nijim M, Zong Z, Bellam K, Ruan X, ManzanaresA ,”Improving security of real-time wireless networks through packet scheduling”, IEEE

Trans. Wireless Communication.7 (9) (2008) 3273-3279.

[3]. Xiaomin Zhu , HaoGuo, Shaoshuai Liang, Xiaoling Yang, "An improved security-aware packet scheduling algorithm in real-time wireless networks", Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410073, PR China.

[4]. Dheeresh Mishra, Girish Tiwari, "Security Protocols in Wireless LAN: A Comparative Study", NCACT India conference 2015.

[5]. S. Lu, V. Bharghavan, and R. Srikant, "Fair scheduling in wireless packet networks," *IEEE Trans. Networking*, Aug. 1999.

[6]. Girish Tiwari, Dheeresh Mishra, "A Study on Real-Time Packet Scheduling Algorithm inWLAN with Security Awareness", International Journal of Research in Engineering and Technology (IJRET), eISSN: 2319-1163, pISSN:2321-7308, Volume:05, Issue:07, jul-2016.

[7]. M. Saleh and L. Dong, "Real-Time Scheduling with Security Enhancement for Packet Switched Networks", IEEE Transactions on Network and Service Management, 2013.

[8]. M. Saleh and L. Dong, "Adaptive Security-Aware Scheduling using multi-agent system," in 2012 IEEE International Conference of Communication.

[9]. HaiFengzhu, John P. Lehoczky, Jeffery P. Hansen, RagunathanRajkumar, "Diff-EDF: A Simple Mechanism for Differentiated EDF Service", IEEE Real Time and Embedded Technology and Application Symposium (RTAS'05) 2010.

[10]. Rama Shankar Yadav, Rudra P. Ojha, SarsijTripathi. "A utilization based approach for securing Real time applications on clusters". International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009 IEEE DOI 10.1109/ACT.2009.112

[11]. M. Saleh and L. Dong, "Comparing FCFS & EDF Scheduling Algorithms for Real-Time Packet Switching Networks" in 2010 IEEE international conference on Networking, Sensing and Control (ICNSC).

[12]. S. Lu, V. Bharghavan, and R. Srikant, "Fair scheduling in wireless packet networks,"IEEE Trans. Networking, Aug. 1999.