IOSR IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. II (Mar-Apr. 2014), PP 58-63
www.iosrjournals.org

Security-Aware Packet Scheduling Scheme with Multi-Level Queuing and RSA

J. Antony Suganiya[1], J. Viji Priya[2],
[1]*Ratnavel Subramanium College of Engineering and Technology, R.V.S Nagar, Dindigul, Tamilnadu.*
[2]*Professor, Ratnavel Subramanium College of Engineering and Technology, R.V.S Nagar, Dindigul, Tamilnadu.*

Abstract: *Emerging security-aware packet scheduling algorithms can efficiently improve the security measures while forwarding the packets over wireless links. Existing scheduling algorithms for real-time wireless networks are not capable of providing higher level of security. The proposed methodology overcomes the difficulties in the existing scheduling algorithm with the security enhancements. A multilevel queue scheduling algorithm is used to partition the ready queue into several separate queues.For security reasons, the proposed methodology uses the RSA algorithm for encrypting and decrypting the packets. The proposed Security-aware Packet Scheduling (SPS) methodology strives to improve the security levels while achieving high schedulability for real-time packets. The proposed model reduces the congestion occurred during scheduling the packets.The performance of the proposed method results better security than the existing Quality Based Searching algorithm. Also, the system takes lesser time, reduces congestion and traffic also provides higher arrival rate for scheduling the packets.*

Index Terms: *Encryption, Decryption, Multilevel queue scheduling, RSA, Real-time packets, andScheduling algorithms*

I. INTRODUCTION

With the development of wireless technologies, wireless networks have been widely used in many public places due to the greater flexibility, reduced wiring cost and improved efficiency. Particularly, the real time wireless technologies allow users to collect and transmit data in a timely manner and also it deals a good attention of the users. But, it is also noted that security is one of the critical issues in any wireless technology. Because, the communication medium of wireless networks is usually open to the intruders. It makes the wireless networks can be easily attacked by the attackers. The lack of security mechanism and the threat of denial of service (DOS) attacks are risks associated with the wireless transmissions. Unauthorized users may access the wireless networks to establish a variety of attacks such as preventing authorized users from accessing the network.

Packet scheduling is an efficient method to enhance and improve the system performance; it plays a significant role in the field of wireless networks. Usually, packet scheduling is applied to guarantee the quality of service, provide fairness and enhance the transmission rate in wireless networks[1, 2].For real-time packets in wirelessnetworks, the precision of them depends not only on thesuccessful transmissions, but also on the time instants atwhich the transmissions are completed. When a new file/packetenters, then it is put into the schedule queue. The files are waiting for schedule process and assigned the lowest level security.The packets are scheduled based on the several scheduling algorithms. If a new packet cannot be accommodated, then it will be put into the rejected queue. Otherwise it will put into the accepted queue. The security level mechanisms are applied to increase the security level of the packets which are placed in the accepted queue.

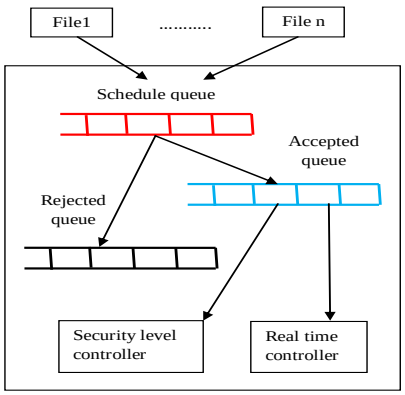

Fig.1. Scheduler model

In this paper, a novel security-aware real time packet scheduling model is proposed. Based on the scheduler model, the proposed system integrates the functionality of real time scheduling with the security enhancement mechanisms.A multi-level queue scheduling algorithm is incorporated to divide the queues into separate queues. The multi-level queuing determines when to upgrade a process to a higher priority queue. Also, it determines when to demote a process to a lower priority queue. RSA is applied to generate the pubic key encryption and decryption. RSA provides higher security level of packet transmission. The experimental results shows that the proposed model performs better than the existing quality based searching algorithm.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the scheduling concepts and the security mechanisms. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

II. RELATED WORK

This section deals with the works related to the scheduling algorithms used in the packet switched networks with secure enhancement approaches. *Jiang et al* proposed a dynamic programming based approximation algorithm. This algorithm was used to schedule aperiodic messages with guaranteed security performance. Theproblem of scheduling aperiodic messages with time critical and security-critical requirements was investigated. Also, a risk based security profit model was built to quantify the security quality of messages[3].*Gupta et al*proposed a queue grouping technique to handle the complex correlations of the service process resulting from the multihop nature of the flows. A general set-based interference model was assumed that imposes constraints on links that can be served simultaneously at any time. These constraints were used to obtain a fundamental lower bound [4].*Wang et al* proposed a Load Weighted Scheduling Algorithm (LWSA) to improve the packet aggregation performance for randomly varied traffic patterns [5].

Chou et al proposed a latency aware scheduling and an analytical model for all optical packet switching networks with fiber delay lines (FDL) buffers. The latency aware scheduling was intended to minimize the packet loss rate of the networks by ranking packets in the optimal balance between latency and residual distance. The analytical model was based on non-homogeneous Markovian analysis to study the effect of packet loss rate and average delay[6].*Meneguette et al* proposed an online packet scheduling model. It was based on vehicular network applications. The multiple networks was incorporated with non-persistent connectivity to know about the network availability[7].*Ghodsi et al*presented the analysis about several natural packet scheduling algorithms for multiple resources and their undesirable properties. The Dominant Resource Fair Queuing (DRFQ) was also proposed to retain the attractive properties that fair sharing provides for one resource. This algorithm was also applicable in other contexts where several resources need to be multiplied in the time domain[8].

Yang et al proposed solution for optimal packet scheduling problem in a two-user multiple access communication system. For the packet arrivals, the authors assumed that the packets have already arrived and ready to be transmitted at the transmitter before the transmission starts. Also, a generalized iterative backward waterfilling algorithm was developed to characterize the maximum departure regions at the energy arrivalinstants [9].*Nelms et al*evaluated three packet scheduling algorithms with the protocol analysis module (PAM) as DPI application using network traces acquired from production networks where intrusion prevention systems (IPS) were deployed[2].*Fashandi et al*applied a forward error correction (FEC) across multiple independent paths to enhance the end-to-end reliability. Also, the rate allocation problem across independent paths was studied.A memorization technique was incorporated with the polynomial run time for rate allocation over a finite number of paths[10].

*Jiang et al*proposed a Security-Slack based Heuristic Algorithm (SSHA) to judiciously allocate a slack time to the most suitable confidentiality level for each security critical message [11].*Li et al* proposed a QOS-aware fair packet scheduling (QFPS)in IEEE 802.16 wireless mesh networks. This scheduling fulfills the QOS provisioning. A traffic flow with urgent QOS aware was guaranteed to given priority in wireless resource allocation. A shorter end to end delay was expected to be offered for the traffic flows with time-urgent requirements. Also, a fairness model was proposed among different traffic flows traversing the same node. All flows pass through a node were served by the Deficit Round Robin scheduling algorithm to achieve fairness within the same priority group [1].*Almalkawi et al*proposed a Secure Cluster-based Multipath Routing protocol for Wireless MultimediaSensor Networks. SCMR satisfies the requirements of delivering different data types and support high data rate multimedia traffic. The hierarchical structure of powerful cluster heads and the optimized multiple paths to support timely and reliable high data rate multimedia communication with minimum energy dissipation was exploited. A light-weight distributed security mechanism of key management was used to secure the communication between sensor nodes and protect the network against different types of attacks[12].

*Ng et al*proposed a system to optimization problem for secure resource allocation and scheduling in orthogonal frequency division multiple access(OFDMA) half duplex decode and forward relay assisted networks[13].*Chi et al* proposed a power-saving scheduling algorithm for wireless sensor networks based on cluster architecture. Polling method was used to make the cluster head have an absolutely effective data receiving. Also, sleeping mechanism was used to ensure that the cluster head to achieve power saving under the premise of the data receiving[14].*Hirota et al* proposed a scheduling scheme based on Look ahead buffer and Loop back buffer in two stage variable optical packet switch network. Both methods improve the utilization of the switching process. The loop back buffer adaptively distribute the traffics in time and space domain [15].

III. SECURITY-AWARE PACKET SCHEDULING

The security based packet scheduling system is proposed for reliable and secure packet transmission.The following sections describe about the scheduling mechanisms and the security features on the packet switched networks. Fig.2. depicts the structure of the proposed model.

A. Multi-level Queue Scheduling

A multilevel queue scheduling algorithm partitions the ready queue into several separate queues. The processes are permanently assigned to one another, based on some property of the process, such as memory size, process priority and process type. The algorithm chooses the process from the occupied queue that has the highest priority and run that process either preemptively or non-preemptively. Multiple FIFO queues are used and the operations are as follows:

1. A new packet is positioned at the end of the top-level FIFO queue.
2. At some stage the process reaches the head of the queue and assigned.
3. If the process is completed, then it leaves the system
4. If the process voluntarily relinquishes control it leaves the queuing network, and when the process becomes ready again it enters the system on the same queue level.
5. If the process uses all the quantum time, it is pre-empted and positioned at the end of the next lower level queue.
6. This will continue until the process completes or it reaches the base level queue.

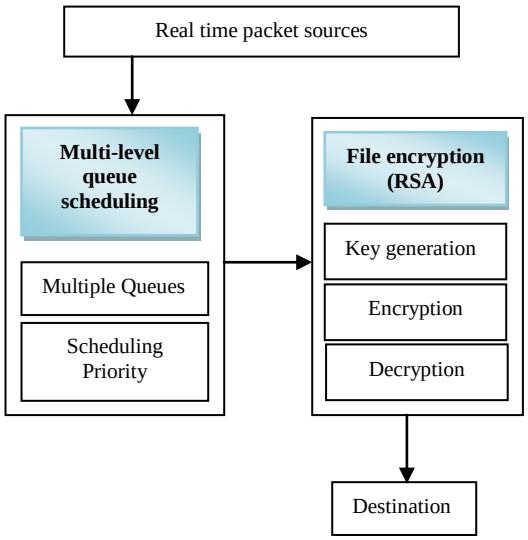

Fig.2. Flow of the proposed methodology

The server agent takes the responsibility of serving the real time data packets, which are chosen by the scheduler. It estimates whether to serve or drop a packet based on the packets remaining time until it expires. If the packet is not expired, then the server sends it to the corresponding destination according to the MAC address. The service time is estimated based on the exponential distribution with mean$\frac{1}{\mu_d}$.

$$\mu_d = \frac{B}{8p} \qquad (1)$$

Where B is the average aggregate bandwidth required for both audio and video real time traffics.

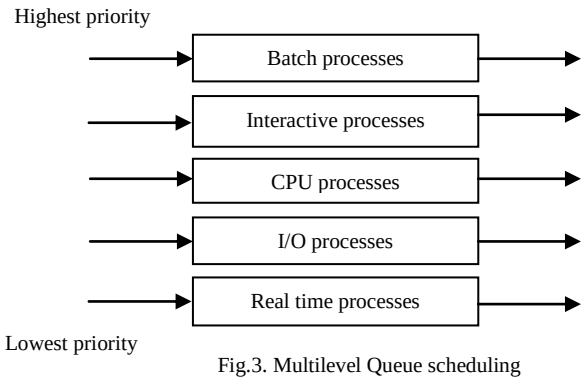

Fig.3. Multilevel Queue scheduling

In this scheduling the ready queue is partitioned based on the type of the processes that are required to be scheduled. The different types of processes are depicted in Fig.3.

B. Security Enhancements

The RSA algorithm is incorporated to provide secure transmission of packets. Here, the encryption key is public and differs from the decryption key which is kept secret.

1) Key generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. *Choose two distinct prime numbers a and b*
2. *Compute n=ab*
3. *Compute* $\varphi(n) = \varphi(a)\varphi(b) = (a-1)(b-1)$
4. *Choose an integer i such that* $1 < i < \varphi(n)$
5. $gcd(i, \varphi(n)) = 1$
6. *Find g as* $g^{-1} \equiv i(mod\varphi(n))$

// Encryption

7. $c \equiv m^e \ (modn) 0 \leq m < n$

// Decryption

8. $m \equiv c^d \ (modn)$

*m*is the original message and *c* is the cipher text.

The integer *a* and*b* should be chosen at random and it should be of similar length. *n*is used as the modulus for both the public and private keys. *φ*is the Euler's totient function. *i*is revealed as the public key component and *g* is kept as the private key component. The public key consists of the modulus *n* and the public (or encryption) exponent *i*.The private key consists of the modulus *n* and the private (or decryption) exponent g, which must be kept secret. *a*,*b*, and φ(*n*) must also be kept secret because they can be used to calculate *g*.

IV. PERFORMANCE ANALYSIS

This section presents the performance analysis of the proposed secure packet scheduling scheme for packet switched networks. The performance is tested based on the following constraints:

A. Arrival Rate

The arriving rate of the packets in the Security-Aware Packet Scheduling is described in Fig.4. It is estimated by varying the nodes as 2, 4, 6, 8 and 10. The average arrival rate is estimated as 1211 packets/sec.

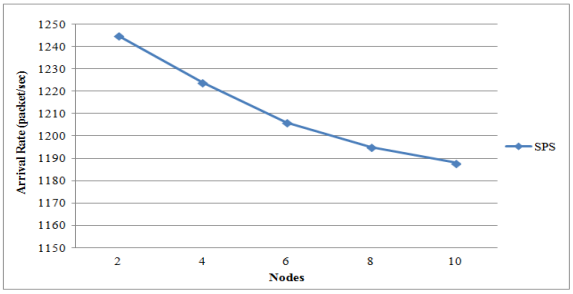

Fig.4. Arrival rate of SPS (proposed)

B. Average Time

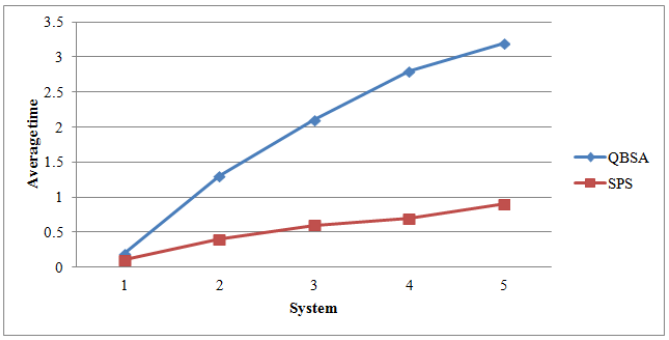

Fig.5. Average time between QBSA and SPS

The average timetaken between each system for the existing Quality Based Searching Algorithm QBSA and the proposed SPS is shown in Fig.5. It shows that the proposed scheduling approach provides lesser time than the exiting approach.

*C. **Interval between systems***

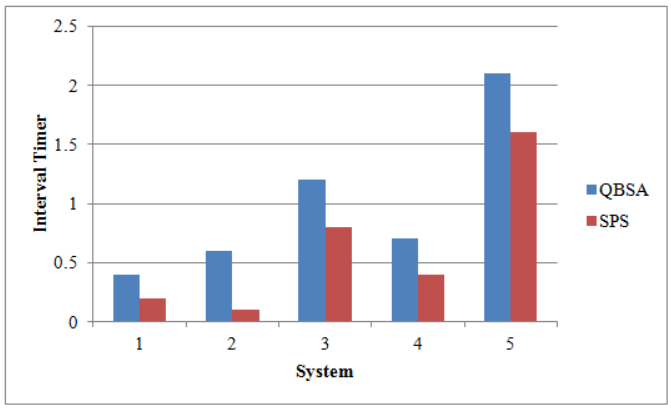

Fig.6. Interval timer between QBSA and SPS

The time interval taken to switch over from one system to other is visually displayed in Fig.6. The result shows that the proposed SPS have taken lesser time interval than the existing QBSA.

*D. **Average Security Level***

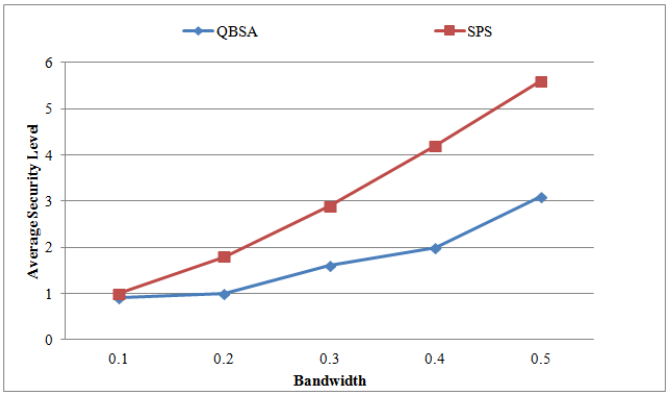

Fig.7 Average Security Level between QBSA and SPS

The average security level is estimated to know about the security of the accepted packets. The overall performance is measured based on the guarantee ratio and the security level. Fig.7. shows that the proposed system results better security level than the existing QBSA.

V. CONCLUSION AND FUTURE WORK

A Security-Aware Packet Scheduling system (SPS) is presented in this paper for real time packets in wireless networks. Multilevel queuing scheduling and RSA key generation algorithm are used for enhancing the security measures on scheduling the packets.The proposed system is effective for security and time critical applications. The performance is analyzed based on several criteria's. The proposed system results better security level than

the existing method. Also, it takes lesser time interval to switch over the process and it provides better arrival rate.Also, it reduces congestion and traffic across multiple queues. The future work includes the more advanced security enhancements to serve both the real-time(audio and video) and implementingthe scheduler with security improvements.

REFERENCES

[1] Y. Li, Y. Yang, L. Zhou, A. Wei, and C. Cao, "QoS-aware fair packet scheduling in IEEE 802.16 wireless mesh networks," *International Journal of Communication Systems*, vol. 23, pp. 901-917, 2010.

[2] T. Nelms and M. Ahamad, "Packet scheduling for deep packet inspection on multi-core architectures," in *Proceedings of the 6th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, 2010, p. 21.

[3] W. Jiang, G. Xiong, X. Ding, Z. Chang, and N. Sang, "Confidentiality-aware message scheduling for security-critical wireless networks," *Systems Engineering and Electronics, Journal of*, vol. 21, pp. 154-160, 2010.

[4] G. R. Gupta and N. B. Shroff, "Delay analysis and optimality of scheduling policies for multihop wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 19, pp. 129-141, 2011.

[5] Z. Wang, W. Hu, W. Sun, H. He, and L. Yi, "An efficient aggregation scheduling algorithm for unbalanced traffic distribution in optical packet switch network," in *Communications and Photonics Conference and Exhibition (ACP), 2010 Asia*, 2010, pp. 635-636.

[6] K.-H. Chou and W. Lin, "A latency-aware scheduling algorithm for all-optical packet switching networks with FDL buffers," *Photonic Network Communications*, vol. 21, pp. 45-55, 2011/02/01 2011.

[7] R. I. Meneguette, E. R. Madeira, and L. F. Bittencourt, "Multi-network packet scheduling based on vehicular ad hoc network applications," in *Network and Service Management (CNSM), 2012 8th International Conference on*, 2012, pp. 214-218.

[8] A. Ghodsi, V. Sekar, M. Zaharia, and I. Stoica, "Multi-resource fair queueing for packet processing," *ACM SIGCOMM Computer Communication Review*, vol. 42, pp. 1-12, 2012.

[9] J. Yang and S. Ulukus, "Optimal packet scheduling in a multiple access channel with energy harvesting transmitters," *Communications and Networks, Journal of*, vol. 14, pp. 140-150, 2012.

[10] S. Fashandi, S. O. Gharan, and A. K. Khandani, "Path diversity over packet switched networks: performance analysis and rate allocation," *IEEE/ACM Transactions on Networking (TON)*, vol. 18, pp. 1373-1386, 2010.

[11] W. Jiang, W. Guo, and N. Sang, "Periodic real-time message scheduling for confidentiality-aware Cyber-Physical System in wireless networks," in *Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on*, 2010, pp. 355-360.

[12] I. T. Almalkawi, M. Guerrero Zapata, and J. N. Al-Karaki, "A secure cluster-based multipath routing protocol for wmsns," *Sensors*, vol. 11, pp. 4401-4424, 2011.

[13] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *Wireless Communications, IEEE Transactions on*, vol. 10, pp. 3528-3540, 2011.

[14] T.-C. Chi, P.-J. Chen, W.-Y. Chang, K.-C. Yang, and D.-J. Deng, "Power-Saving Scheduling Algorithm for Wireless Sensor Networks," in *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*. vol. 260, Y.-M. Huang, H.-C. Chao, D.-J. Deng, and J. J. Park, Eds., ed: Springer Netherlands, 2014, pp. 127-133.

[15] Y. Hirota, S. Yatsuo, H. Tode, and K. Murakami, "Scheduling scheme using Look-ahead Buffer and Loop-back Buffer in Two-stage variable optical packet switch," *Optical Switching and Networking*, vol. 9, pp. 252-263, 7// 2012.