A STUDY ON REAL-TIME PACKET SCHEDULING ALGORITHM IN WLAN WITH SECURITY AWARENESS

Girish Tiwari[1], Dheeresh Mishra[2]

[1]*Associate Professor, Department of Electronics and Communication Engineering, UEC, Ujjain, (M.P.), India*
[2]*M.E. Research Scholar Department of Electronics and Communication Engineering UEC, Ujjain, (M.P.), India*

Abstract

Due to the increasing popularity of IEEE 802.11 WLAN standards, WLAN have been wide spread to provide the last mile delivery of internet access to mobile users. Security is the critical issue in WLAN, because wireless network is open to everyone allow the illegal user to attack in open networks without any problem. Real time wireless networks require maximum level of security to assure high confidentiality to data stored in the packets transmitted via wireless medium. Here we focus on some Real Time Packets Scheduling with security Awareness algorithms, here we discuss both Security issues and Packet Guarantee.

Keywords: *Wireless Networks, Real-Time Packet Scheduling, SPSS, ISAPS, RSAPS, IPSASC, Security Protocols*

----------***----------

1. INTRODUCTION

Now a day's wireless networks are very popular. WLAN's have been widely used in colleges, IT industries, airports and many public places. WLAN is more efficient, flexible and require no wire compare to traditional wired networks. Due to its mobility Wireless LAN keep playing a key role in serving mobile users.

With this growing popularity, the security of WLAN is also a key issue. The communication medium of WLAN is air wave which are susceptible to interception from intruder [5]. Due to which wireless networks are prone to verity of attacks like eavesdropping, denial of service, data modification and replay attack. These attacks decrease the quality of services in a network.

In general network system some essential security requirements are required, such as:

A. **Data Confidentiality and Integrity:** Confidentiality mean allow only the legal individual to study the encrypted messages or the information and integrity described as the message is not being opened by third party and it should reach in the same format as it was sent by the sending party. Data confidentiality and integrity, supporting build a comfortable channel for data communication. The networks ought to provide strong data confidentiality and integrity [7].

B. **Mutual Authentication:** Authentication means identification plus verification. It is an important security requirement.

C. **Availability:** It shows robustness, which is another essential class of security requirement. The network resources should be available to every valid user in the system.

In other phrases, unavailability of resources should be removed.

To provide these important security requirements in wireless LAN we use security standards. Wireless networks are susceptible to attacks. There are plenty of attacks in wireless networks some of them are:

- **Eavesdropping:** It comes under confidentiality attacks in which captures and decodes the unprotected sensitive information.
- **Jamming:** In this type of attack, attacker transmits the same frequency radio signals as sends by legal sender, to disrupt communication and degrade the Signal to Interference plus Noise Ratio (SINR) [16].
- **Flooding:** Attacker inject large number of packets in to the networks, results denial of services and wastage of bandwidth.
- **Denial of Services (DoS):** It is a type of Availability attack. Due to DoS users are not able to use network resources. It is a very serious problem in Wlan.
- **Replay Attack:** In this attack, same information is transmitted by the attacker many times, thus providing delay in data transmission.
- **Impersonation:** Under this attack, attacker mimic the MAC address of any legal user doing this attacker may inter in to the protected network [17].
- **Black hole attack:** The attacker act as a malicious node which drops all the incoming packets sends by the legal node in the network. Here the purpose of the attacker to increase the congestion results Dos [15] [13].

To protect the wireless network from the above attacks Security is major issue.

Real Time data communications are increasing every day. Data propagation in wireless medium could be hindered by natural and manmade objects like mountains or tall buildings and disturbed by thunderstorms or radio waves

[1]. In real time network application the quality of services is extremely important, to achieve required quality of service real time communication a balance is required between overall network performance and security requirements [8] [10].

In this paper we discuss about some important real time packet scheduling schemes along with security awareness such as, Security-Aware Packet Scheduling Strategy or SPSS [1], Improved Security Aware Packet Scheduling Algorithm or ISAPS [2], Round robin based Security Aware Packet Scheduling algorithm or RSAPS [3], and Improved Real-Time Packet Scheduling Algorithm with Security Constraint or IPSASC [6]. Section 2 gives overview of Security Protocols. Section 3 will introduce various Schemes of scheduling along with security for real time packets in WLAN. Section 4 gives conclusion.

2. SECURITY PROTOCOLS

There are three important security protocols which are given by IEEE used to ensure the data security in Wireless LAN.

2.1 WEP (Wired Equivalent Privacy)

WEP is a security protocol for WLAN. It was developed by IEEE in September 1999 as a part of security standard. The main purpose of WEP was to provide security similar to that of wired network. WEP makes use of CRC-32 checksum for integrity and stream cipher RC4 algorithm for confidentiality [9].WEP supports 40-bit key and it also supports 128 or 256 bit key. A 24-bit initialization vector is used by WEP for initialization of the cryptographic key stream [12].

2.2 WPA (Wi-Fi Protected Access)

The WEP protocols had some weakness, like it uses RC4 improperly, it allow replay attack, it allow forgery of packet and there is no management of key. To overcome the drawback of WEP, WPA was developed in 2003 by the Wi-Fi alliance [4]. WPA uses TKIP (temporal key integrity protocol) for encryption, TKIP used Michael algorithm to generate a code called message integrity code (MIC). Integrity provided by MIC is much better then integrity provided by CRC-32 used in WEP. WPA does not need new hardware to overcome the cryptographic problem which was in the WEP. WPA makes use of 48 bit initialization vector and during communication keys are changing dynamically [5].

2.3 WPA2 (Wi-Fi Protected Access2)

WPA2 remove the flaws of WPA, it was the enhanced version of WPA and completely Implements IEEE 802.11i. It was introduced in September 2004 by the Wi-Fi alliance.

The important development was CCMP (Counter Mode with Cipher block Chaining Message Authentication Code Protocol) which uses block cipher AES (Advance Encryption Standard) for data encryption, TKIP is also available for backward compatibility with existing WAP hardware [11].

3. REAL-TIME PACKET SCHEDULING ALGORITHM WITH SECURITY

In Real-Time network Packet Scheduling is a key to enhance the open network performance, efficient transmission of packet, transmission rate of packets and Safety is a key for the packet reached destination as it is [6]. There are verity of Packet Scheduling Scheme exist. They degrade the Security level to improve the scheduling and a number of them degrade the scheduling to improve the security. This result the total system performance will reduce. To improve the system performance we need a balance between both security as well as scheduling.

3.1 SPSS (Security-Aware Packet Scheduling Scheme)

Fig.1 shows the system model of SPSS. In this model each wireless node acts as a transceiver and wireless channel as a NN switch [14]. All Packets are independent to each other and packet arrival rate follows poison distribution. There are three other important components in model includes an Admission Controller, a Security level Controller and an Earliest Dead Line First (EDF) Scheduler. The Admission Controller decides whether the incoming packets can be accepted or not. The function of the Security controller is to enhance the security level of the Real-Time packets which are residing in the accepted queue that can be finished before their deadline. The EDF Scheduler follow Earliest Dead Line First Policy to schedule admitted packets in which security levels are maximized by the Security level Controller.

Quin et al proposed the SPSS algorithm. The main aim of this algorithm is to improve total performance of the system. In SPSS the security requirement of the packets is dynamically adjusted.

It is assumed that all the incoming packets are independent to each other. In this scheme initially assign the minimal level of security to all incoming packets.

Then admission controller checks the deadline of all incoming packets. The equation given below is use to check the deadline of the packets.

$$Ct_i - St_i \leq D_i \quad (1)$$

Ct_i = completion time of transmission of ith packet,
St_i = start time of the packet
D_i = packets Deadline.

If incoming packets satisfied the above equation then it will go to the accepted queue otherwise it will go to the rejected queue. After that security level Controller increase the security level of the packets which is in the accepted queue by doing this one thing should be noted that increment of the

security level must not reject any currently accepted packet. Finally EDF scheduler, schedule the packets by the use of Earliest Deadline First policy [1]

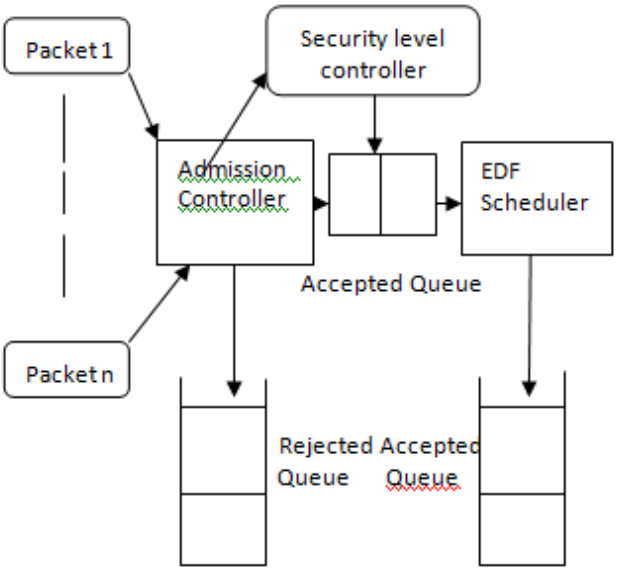

Fig-1: System model of SPSS [1]

3.2 ISAPS (Improved Security-Aware Packet Scheduling Algorithm)

Fig.2 shows an ISAPS Scheduler model proposed by Xiaomin Zhu et al, which is improved version of SSPS system model. In this model all incoming packets are going to scheduler queue which initially schedules the packets and assign the minimum security degree to the packets after that Real-Time Controller decides admission of the packets in to accepted queue or rejected queue and schedules the packets by using EDF policy, then Security level Controller enhanced the degree of security of packets which are resides in the accepted queue. The Real-Time Controller considers the packets in the accepted queue as well as new packets due to this the Schedulability is increase to its maximum value. Packets can be allocated successfully to the accepted queue if the following condition of p_i can be satisfied.

$$F_i \leq dl_i \qquad (2)$$

$$S_1 \leq S_i \leq S_n \qquad (3)$$

Where p_i is the ith packet in packet set p, it is assumed that all packets are independent, F_i = Finish time of p_i , dl_i = Deadline of p_i and S_i is the security level of p_i.

Real-Time packet is scheduled if the following inequalities satisfied.

$$ST_i + PT_i \leq D_i \qquad (4)$$

$$\forall P_k , O_k < O_i , W_k = 1 : \; St_k + Pt_k \leq D_k \qquad (5)$$

Where ST_i is the completion time of packet, PT_i propagation time of packet, D_i is the dead line of packet, O_i is the transmission order of packet and if w_k =1 then packet is ready inside the accepted queue.

Equation 3 and 4 indicates that the transmission of Real-Time packets consequences no violation of any deadline to the wireless networks [2].

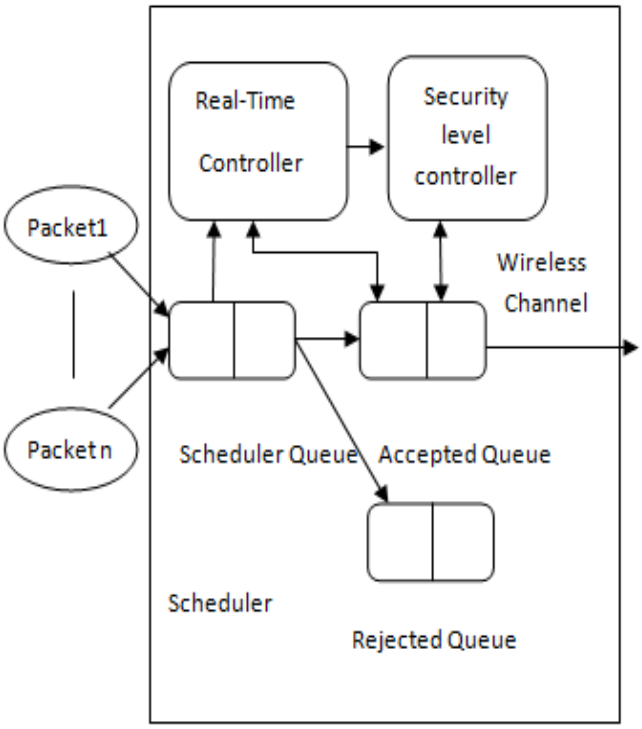

Fig-2: Scheduler model of ISAPS [2]

3.3 RSAPS (Round robin based Secure-Aware Scheduling)

Arun Raj et al proposed this scheduling model shown in fig.3, this model is very similar to previous model accept a round robin scheduler. Here scheduling is done at intermediate level.

In this algorithm all incoming packets are initially scheduled by scheduler queue and assign a maximum level of security, after the Real-Time controller sorts the packets based on Earliest Deadline First policy in the scheduler queue. Then scheduling is done by Round Robin scheduler, it selects n number of packets from the sorted packets for scheduling. When one round is completed finishing packets will be replaced by new packets, for a packet to be forwarded to the accepted queue Real-Time controller determine whether '**finish time of the packet is less than or equal to deadline of the packet**'. Packets which satisfy this condition accepted with maximum security. If any new packet does not satisfy this condition then Security level Controller reduces the security stage of such type of packets and again check this condition. This process continues until the packets have reached minimum level of security. If still the condition is not fulfilling by the packets Real-Time Controller drop these packet in to the rejected queue [3].

3.4 IPSASC (Improve Real-Time Packet Scheduling Algorithm with Security Constraint)

Surendra singh et al proposed IPSASC algorithm and the scheduler model of this algorithm is similar to ISAPS scheduler model which is shown in fig.2.

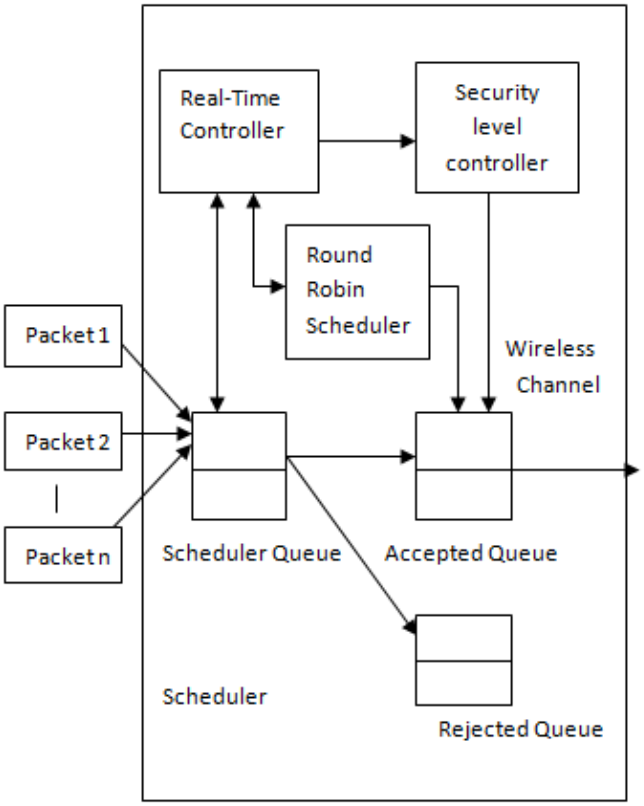

Fig-3: Scheduler model of RSAPS [3]

Property$_1$. $CT_i \leq Dl_i$

Where CT_i = Total Completion time of packet p_i

Dl_i = Deadline of packet P_i and P_i is the i^{th} packet in packet set P.

Policy$_1$. Reduce the security degree of the packets which is ready in the accepted queue to minimal stage that has better transmission time among the remaining packets ready in the commonplace queue.

In this algorithm the incoming packets are assumed to be independent among one another. Firstly incoming packets store in to the scheduler queue and assign minimum security level to the packets. After that real-time controller apply property $_1$to the all packets. If property$_1$ satisfied then packet is generic and real-time controller notify to the security controller to enhanced the degree of security to its maximum level but keep follow property $_1$, on the flip side real-time controller inform to the security level controller to reduce the degree of security of the packet ready inside the accepted queue according to the policy$_1$, till new packet may be accepted. If all the packets reached to minimal security stage in the accepted queue but still not follow deadline of the new packet or not satisfied property$_1$, then packets are rejected and put in to the rejected queue [6].

Table 1: Comparison of Real-Time Packet Scheduling Algorithms: SPSS, ISAPS, RSAPS And IPSASC

SPSS	SPSS is a security aware packet scheduling algorithm with soft deadline and dynamically adjusted the level of security of the incoming packets according to the traffic condition of the system. So, when system workload increases then a few new packets may be accommodated results packet drop ratio increases and overall performance of the system decreases. It has poor Guarantee Ratio ISAPS.
ISAPS	ISAPS is an improved scheduling algorithm. ISAPS have lower packet drop and better Guarantee ratio compared with SPSS. It is also a dynamic security mechanism which is based on system workload. Under light workload it provides highest security level which will improve guarantee ratio as well as security level of the system, but under heavy workload ISAPS main aim is to scheduling the packet to reduce the packet drop ratio which can be degrades the security level.
RSAPS	In ISAPS scheme if packet arrival rate increases then packet drop ratio also increases which decreases guarantee ratio. To improve guarantee ratio and reduce packet drops RSAPS used Round robin based scheduler. RSAPS gives equal chance of processing every packet, due to that packet drop ratio decreases. It is a dynamic security algorithm. RSAPS have better scheduling and security level as compare to ISAPS but still when the system is under heavy work load the number of packet drop increases.
IPSASC	IPSASC is an improved real-time packet scheduling algorithm with security constraint. According to the system workload it adjusts the scheduling and security level. When system having light traffic then security level is important and when the system having heavy traffic then it balances the scheduling and security level. IPSASC have much better guarantee ratio, less processing time and better level of security then above three real time algorithm.

4. CONCLUSION

In wireless networks Scheduling of real time packet along with Security is a challenging task. It is important to maintain the balance between Scheduling and Security to improve the total performance of the system. Though it is not possible to achieve complete balance between Security level and Guarantee Ratio, but in this study paper we try to achieve satisfactory balance between these two types of important parameter to improve the overall system performance.

In this paper we discuss about some important scheduling algorithms of real time packets: SPSS, ISAPS, RSAPS, and IPSASC. Each algorithm has dynamically adjusted Guarantee ratio and Security level according to system traffic condition and tries to improve overall system performance. Here we assume in every algorithm that all incoming packets are independent to each other.

In the upcoming work, we will focus on the dependent packets.

REFERENCES

[1]. 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.

[2]. 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.

[3]. Arun Raj, P. Blessed Prince, "Round robin based Secure-Aware Packet Scheduling in Wireless Networks", International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462, Vol. 5 No.03 March 2013.

[4]. Swati Sukhija, Shilpi Gupta – Wireless Network Security Protocol A comparative study – IJETAE 2012.

[5]. Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne - Vulnerabilities of Wireless Security protocols – IJARCET 2012.

[6]. Surendra Singh, Dr. Ranvijay, " Improved Real-Time Packet Scheduling Algorithm with Security Constraint", IEEE India Conference 2014 pp. 1-6.

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

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

[9]. A.Antony Vinoth Kumar, C.Karthikeyan, V.Karthikeyan – An Innovative Wireless Network Security for Air force using Wireless Protocols – IJSRP 2012.

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

[11]. Maocai Wang, Guangming Dai, Hanping Hu, Lei Pen, " Security Analysis for IEEE802.11", IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing 2008. Pp. 1-3.

[12]. Arash Habibi Lashkari, Masood Mansoori, Amir Seyed Danesh, ―Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)‖, in ICCDA Singapore Conference, 2009.

[13]. Girish Tiwari, Nishant Doshi, "A Ubiquitous Solution for Mitigation of Black Hole Attack in Cognitive Radio" International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 4, no. 6, pp 398-403, June 2016.

[14]. S. Al-Harthi and R. Rao, "A switch model for improving throughput and power fairness in Bluetooth piconets," in *Proc. Globecom 2003*, pp. 1279–1283

[15]. Shalini Sharma, Girish Tiwari "A new IDS scheme against blackhole attack to enhance security in wireless network" International journal of research in engineering and technology (IJRET) vol. 9, no. 8,pp 429-433,aug 2015

[16]. Satish Vadlamani, Burak Eksioglu, Hugh Medal, Apurba Nandi, "Jamming Attacks on Wireless Networks: A taxonomic Survey", Int. J. Production Economics 172 (2016) 76-94

[17]. Sachin Dev Kanawat, Pankaj Singh Parihar, "Attacks in Wireless Networks", International Journal of Smart Sensors and Ad Hoc Network (IJSSAN), vol. 1, no. 1, 2011