International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 10, 2020
ISSN: 1475-7192

# Custom Queueing method for enhancing security of a Packet Scheduling Process in Real Time Networks

[1]G.Karuna, [2]Swaraja K, [3]Meenakshi.K, [4]Padmavathi.Kora

***ABSTRACT —*** *The wireless technologies became a part of our day to day life, for sending and sharing data very rapidly so that everyone today uses wireless networks for their business or personal. The traditional wireless communication technology is unable to satisfy real-time transmission requirements in mobile electronic commerce application such as access of books from digital libraries, access of stock exchange information etc. Recent real-time wireless networks require high level security to guarantee the information passed through wireless channels. So, designing flexible security mechanisms for real time applications and transmitting packets through wireless networks is highly desirable. The present work introduces a new packet scheduling algorithm to enhance security which mainly aims to dynamically determine security levels of packets based on security requirements of an application and also guaranteeing deadlines for packets. By incorporating Custom Queuing method with this packet scheduling algorithm, the overall performance of real time networks is increased.*

***Keywords—*** *Wireless Networks, Packet Scheduling, Custom Queuing*

## I. INTRODUCTION

Wireless technology today has become one of the most affordable and easy to use in the field of information technology and academics because of its fastest growth of various applications in recent are using wireless networks. Almost every common man today can access to the Internet at their homes, libraries, universities, restaurants, railway stations, airports, and even while driving in vehicles to conduct their business, accessing and learning e-books, transfer money, paying electricity bills, booking movie tickets, sharing stock exchange information etc.

As Internet users become increasingly mobile and online business applications become very much interactive and traditional wireless communication technology methods are unable to satisfy the real-time transmission requirements in mobile electronic commerce applications such as access of books from digital libraries, access of stock exchange information etc. The remedy to this problem is real-time wireless communication techniques allowing users to collect and transmit data in a timely manner increases interest in many academicians, scholars and researchers. Supporting

[1]*Computer Science and Engineering, GRIET,Hyderabad, Telangana, India.*
[2]*Electronics and communication Engineering, GRIET,Hyderabad, Telangana, India.*
[3]*Electronics and communication Engineering, GRIET Hyderabad, Telangana, India.*
[4]*Electronics and communication Engineering, GRIET Hyderabad, Telangana, India*

**Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020** 

efficient and reliable data transmission, especially real time data transmission, through wireless networks is extremely difficult and challenging task because wireless networks must be facing more complicated environments compared with conventional wired networks such as computer viruses, intruders, worms, spy wares, and similar threats.

Many security policies related to authenticity and confidentiality strategies and wireless communication protocol-based security schemes [1] have been proposed and applied in real-time wireless networks. However, most of them considered only security issues in a static mode, in which security levels are all configured when wireless network systems are built. In some real-time systems like stock quote updating and trading system, users may need flexible quality of security, measured as security levels. Suppose in an industry the data may be more secured when compared to the past twenty years data in that company. i.e security levels are higher at present for that company. Thus designing flexible security mechanisms for real time applications transmitting packets through wireless networks is highly desirable.

The Custom Queuing method for improvement of Security Aware Packet Scheduling Algorithm aims to dynamically determine security levels of packets according to applications, security requirements while guaranteeing deadlines for packet and also increases the speed i.e overall performance. Apart from achieving high quality of security, it can significantly improve guarantee ratio, which is a fraction of total transmitted packets that are found to be delivered before their deadlines.

## II. RELATED WORK

There is a rapid growth of applications in the domain of wireless networks in the real world, i.e. usage of Internet at all places in homes as well as business for sales, purchases, finding remote locations, making payments and playing games and many more. Because enormous development of Wireless technologies makes a person day to day life more comfortable. Many devices with wireless technology developed and used for an individual and for business point of view which leads an increase of users every day.

Security risks automatically raised and it is a challenging task for secured transmission of data. National Telecommunications Cooperative Association (NTCA) reported in the year of 2005 nearly 61% of survey defendants provided wireless services to their regular customers and nearly 55% of real time services are for voice like services. In the coming years Wireless technologies will offer further many new features and functions for protecting data and safe transmission.

Wireless technologies, makes easy for communication due to no cables required for connection. i.e. two or more devices are enabling communication without connecting physically each other with transmission cables. Instead they use micro and radio waves [2] with specific range of frequencies for providing communications among larger distances. Depending on speed, coverage area and size there are many categories of wireless networks available. Wireless personal area networks which covers very smaller distances within a room (Bluetooth), Wireless Local Area Networks that covers few kilometers by connecting laptops with the device having wi-fi access point, wireless metropolitan area networks range hundreds of kilometers with multiple nodes and wireless wide area networks covers the distance across worldwide

through various cellular technologies (WiMAX, CDMA, GSM etc) [3]. Best example for Wireless Wide Area Network is an Internet. Wireless technologies range from complex systems to simple hand held devices [4]. Different packet scheduling algorithms surveyed from exited work [5, 6].

### *A. Security Issues*

Security plays an important role in the design and development of wireless mobile educational and business applications, international wireless organizations, wireless equipment providers and thus academic researchers made extreme efforts in increasing the features of existing security mechanisms [7, 8] and finding attractive and creative security policies of wireless networks. IEEE introduced many standards for improving security by defining various security related functions. Cisco provides the solutions for wireless applications by using strong encryption technology and providing unified WLAN. Papers addressing the security problems also provide valuable solutions for wireless business applications.

In recent years, wireless networking has become more popular and users are accessing wireless technology while moving also for their daily activities. Thus, protecting data from unauthorized access or the attacks like active and passive attacks etc is a challenging issue apart from efficient and reliable transfer of data. There are many existing algorithms to improve performance of wireless networks. This paper highlights those security threats, and explains what we need to know to use wireless safely, both in the home and in public

### *B. Packet Scheduling*

*A.* Packet Scheduling methods are generally used when multiple packets exist in a buffer and the share a commonoutgoing link. Packet scheduling algorithm determines the service policy of a node and it plays important role for providing quality of service.

Many packet-scheduling algorithms exist in the literature for increasing the quality of service within a node while delivering packets from source node to destination node. Chang and Yu presented packet-scheduling algorithms [9] to guarantee the quality of service in wireless applications of ATM and video traffic. Different packet scheduling algorithms developed for achieving quality of service in the nodes such as FIFO, Priority Queue, Weighted fair queue and low latency queue etc. In FIFO method the packets are served based on their arrival order. Priority Queues gives preference for important traffic to be cleared during transmission. Weighted fair queue works based on weighted bandwidth allocation. It divides bandwidth across multiple queues. However most of these packet scheduling algorithms works well for better delivery packets and achieve quality of service, but not concentrating on security constraints. This paper mainly integrates the proposed packet- scheduling algorithm [10,11] with dynamic security adjustment strategy. In doing so, we build a new secure packet scheduling scheme along with custom queueing policy for real-time wireless networks.

# III. PACKET SCHEDULING ALGORITHM WITH SECURITY CONSTRAINTS

The packet scheduling Algorithm with security has been introduced with the aim to increase the performance and reliable delivery of packets by using various security levels [14]. This Security based Packet scheduling algorithm improves the performance by raising security levels where a security level controller is used.

Initially packets are sent into the accepted queue and security levels are increased for every packet at accepted queue by determining the guarantee and deadline of packets. When packet has considerable deadline, it is admitted into accepted queue otherwise it will be sent into the rejected queue. The below given constraint verifies whether packet has considerable deadline.

CTi - STi <= diwhere, STi is the start time of transmission of the ith packet, CTi isthe transmission completion time, di is the deadline of packet.

Based on the deadlines of the packets, they are processed. i.e. the packet which is arrived first is scheduled first. This algorithm is initiated with very low-level security levels. Further, the security is increased based on below constraints.

(i) when Pi is transmitted earlier than given deadline. bipartite graph G =

(ii) Pi packets are guaranteed even the deadlines have been initiated later.

The above constraint (ii) is important and reasonable if the packet is arrived in real time link, then its timing constraint has to guaranty the arrival. Simply this security algorithm confirms that an admitted packet is not harmfully affected by simultaneous admitted packets. (V,U,E) is a subset of edges G (i.e., of E) such that no node in V or in U has more than one edge of this subset incident on it. A maximal matching in a bipartite graph is any matching such that given this matching, no other edge can be added to it without violating the definition of the matching. A maximum matching in a bipartite graph G is a

### *A. The* Custom *Queuing for Efficiency*

This strategy works for fixed-length packets scheduling matching consisting of the number of edges in G.=maximum possible

[10,11]. FIFO within priority queues. It is based on

interface or protocol. Time is divided into frames. Each session is assigned a weight in terms of number of packets that could be served during a frame. For every session a separate counter is kept in order to register the number of The central node or the scheduler could be either one of the *N* nodes or a separate entity.

This also includes a PAN, based on this model a

packets served in that specific frame. It guarantees bandwidth per queue. It is not used for voice. It increases speed and performance during transmission of packets

### *B. Algorithm*

**Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020** 

//calculate no. of packets to be served each round//min = find smallest weight For each flow f f.packets_to_be_served=f.weight/min//main loop Loop

For each non_empty flow queue f min(f.packets_to_be_served,f.packets_waiting).times do serve packet f.get packet

## IV. SYSTEM MODEL

The system model includes a wireless channel as an NN switch [2] shown in Fig.1. A transceiver is used for transmission of packets even though a separate transmitter and receiver is equipped by each wireless node in the system. As such, a node cannot transmit and receive packages simultaneously. A packet scheduler matching transmitter is equipped to the corresponding receivers in this model. Wireless Switched PAN or simply a Switched PAN.

With these assumptions, the model can be represented by a special bipartite graph.

**Figure 1:** N-Node Bipartite Graph (NNBG)


There are three more components in the system apart

In the above-mentioned model, a centralized scheduler collects, via a control channel, global network information. The scheduler uses a slotted system and a matching algorithm 2 to match transmitters to their from switch model, including Security Controller (SC), an Admission Queue Controller (AQC), and Deadline Controller (DC) as depicted in Fig. 2.

intended receivers. Clearly, there is no need for a transmitter to transmit to the receiver on the same mobile node. Therefore, the possibility of a transmitter sending to

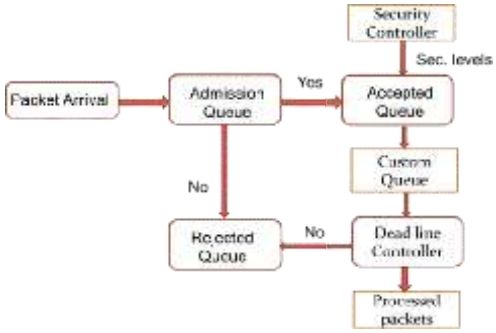


**Figure 2:** System architecture

This model represents a connection between two node

the receiver on the same mobile node is disallowed. Thein specified wireless network. And the packets are resulting system of *N* transmitters and *N* receivers, withsubmitted independently to the wireless link with arrival exactly one transceiver on each mobile node, can be modeled as a special case of an *NN* switch. The *N* transmitters can be thought of as the *N* input ports of switch and the *N* receivers as the *N* output ports. The rates abided by Poisson distribution. The Admission Queue Controller mainly decides given packet is accepted or not. If it is accepted then sent into accepted queue otherwise into rejected queue. The security levels centralized scheduler node is modeled as the arbiter or scheduler of the switch. This PAN model assumes that each node's transmission can reach any of the other *Ni nodes and the* for packets in the accepted queue will be assigned by the Security Controller. The Deadline Controller scheduler uses deadline policy for all admitted packets in which security levels have been increased by the Security Controller.

### *A. The Packet Model*

**Table 1:** Packet schedule process with CQ

| P.No. | Generation of packets | | | | Acc/rej | Incr. sec | With Custom Queuing (CQ) Method (packets) |
|---|---|---|---|---|---|---|---|
| | St (s) | End (s) | dead line | Secu. level | | | |
| 1 | 1 | 3 | 15 | 2 | acc | 7 | [4,4,9,10,7] |
| 2 | 2 | 5 | 14 | 6 | acc | 6 | Parallely sending [5,5,11,10,9] |
| 3 | 3 | 7 | 17 | 8 | acc | 8 | [2,2,5,14,6] |
| 4 | 4 | 9 | 10 | 7 | acc | 7 | Parallely sending [10,10,20,14, 7] |
| 5 | 5 | 11 | 10 | 4 | acc | 9 | [1,1,3,15,7] |

times based on the classical Poisson distribution. Packet Pi is represented as a tuple (ATi, PTi, DLi, SLi), where ATi and PTi represents the arrival time and the processing time of packet i.

The guarantee percentage (GP) and aggregate security level percentage (ASP) of SPACQ is calculated and compared with other algorithms SPSS [12,13], ISAPS[15], RSAPS[16] as shown in

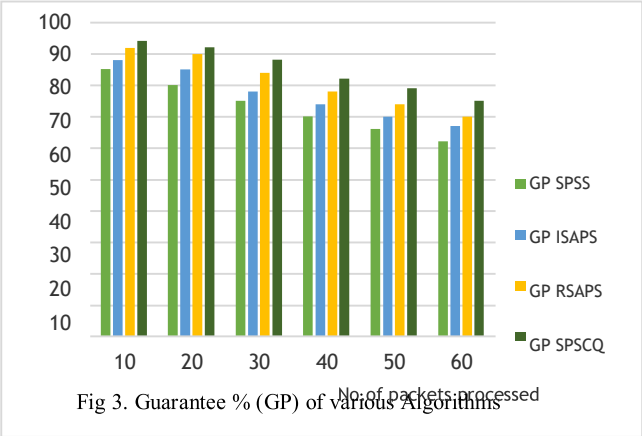


Fig 3. Guarantee % (GP) of various Algorithms

**Figure 3:** Security % (ASP) of various Algorithms

The experimental results shown that the new SPSCQ approach provides an improvement in terms of guarantee ratio, security level, and speed. Thus, the overall performance for real time wireless networks has been improved using Custom Queuing approach and the security levels organized dynamically based on the network traffic.

DLi depicts deadline and SLi specifies the security level of packet *i*. Besides, without loss of generality we assume that each packet is assigned a quality of security measured as a

security level *SLi* that in the range [1, 2, ..., 10], where 1 and 10 are the smallest and largest security levels. The security level 1 means that smallest security level of the packet and level 10 is largest. To calculate the security overhead without loss of generality, the below given formula (1) is used to model the security overhead envisioned as the extra processing time experienced by packet *i*.

$$SOi = ETi * (SLi / R) \quad (1)$$

where SOi and SLi depicts security overhead and security level of packet i, ETi is the transmission time of the packet and R is set to 10. Thus, the total processing time WLi of packet i can be expressed as shown in Eq(2).

$$WLi = ETi + SOi = ETi * (1 + SLi / R) \quad (2)$$

Where, SOi-security overhead of packet SLi - security level

ETi- transmission time of packet R value set to 10

## V. SIMULATION AND RESULT ANALYSIS

The transmission of packets with in a node while delivering from source node to destination node using custom queuing method is shown in the given table 1.

The simulation parameters considered for SPSCQ algorithm are 60 source nodes, 40 destination nodes and 5 intermediate nodes. The packets are transmitted from source node to destination node through intermediate nodes by changing security levels ranging 1-10. The arrival rate is 5 packets/sec. bandwidth taken as 1mbps.

(i) Guarantee % = (no.of accepted packets/no.of arrived packets) *100

(ii) Agg. security % = (security level used for accepted packets/ no. of arrived) *100

## VI. CONCLUSION

In modern wireless networks high quality of security is essential apart from guarantee ratio of packets, in order to protect data which is stored in the packets to be transmitted. The proposed work suggested a novel dynamic Security based Packet Scheduling algorithm with Custom Queuing approach (SPSCQ), which is capable of achieving high quality of security service for real-time packets and reliable while delivering packets. The algorithm is also designed in a way that makes it possible to achieve a reasonably high guarantee

ratio and optimized security level. In particular,the proposed SPSCQ algorithm leverages an intelligent Security Level Controller to adaptively assign security levels to incoming real-time packets transmitted through a wireless network links. The performance of the present approach can be further improved by using combinations of various other packet scheduling algorithms.

## REFERENCES

1. Manoharan, Rajesh, et al. "Selection of Intermediate Routes for Secure Data Communication Systems using Graph Theory Application and Grey Wolf Optimization Algorithm in MANETs." IET Networks (2020).
2. Rajesh, M., Gnanasekar, J.M. Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks. Wireless Pers Commun **97,** 1267–1289 (2017). https://doi.org/10.1007/s11277-017-4565-9
3. Rajesh, M. Streamlining Radio Network Organizing Enlargement Towards Microcellular Frameworks. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07336-9
4. .M. A Badamas, "Mobile computing systems–security considerations," Information Management and Security 2001, pp. 134–136.
5. W. Kensaku, K. Shoji, T. Yutaka, K. Yoshinobu, I.Eisaburo, A packet scheduling algorithm for max-min fairness in multihop wireless LANs, Comput. Commun. 32 (2009) 1437–1444.
6. Z. Zhang, S. Bronson, A packet scheduling algorithm for optimizing downlink throughput in wireless LANs with the one-sender– multiple- receiver technique. in: Proc. the 28th IEEE Conf. Global Telecommunications (GLOBECOM 2009), Dec. 2009, pp. 1–6.
7. V. Gupta and S. Gupta, "Securing the wireless Internet," IEEE Commun. Mag., pp. 68–74, Dec. 2001.Chang J.Chang and M.Yu "Guaranteed Quality of Service wireless access to ATM".IEEE J.select. Areas communications 1997.
8. Packet Scheduling Survey and Tutorial - Guansong Zhang Modeling Packet Scheduling Algorithms in IP Routers
9. Xiao Qian, Mohamed Alghamdi, Mais Nijim, Ziliang Zong, Kiranmai Bellam, and Adam Manzanares, "Improving Security of Real-Time Wireless Networks Through Packet Scheduling" ,IEEE Transactions on Wireless Communications, Vol. 7, No. 9, September 2008.'
10. Xiaomin Zhu , Hao Guo, Shaoshuai Liang, Xiaoling Yang, An improved security-aware packet scheduling algorithm in real-time wireless networks, Science and Technology on Information Systems Engineering Laboratory,
11. National University of Defense Technology, Changsha, 410073, PR ChinaWireless Sensor Network, 2016, 8, 77-84 Published Online May 2016 in SciRes. http://www.scirp.org/journal/wsn http://dx.doi.org/10.4236/wsn.2016.85008.
12. Xiaomim Zhu, HaoGuo, Shaoshuai Liang, Xioling Yang,"An improved Security-aware packet scheduling Algorithm", Information Systems Engineering Laboratory, National University of Defense, PR China.
13. Arun Raj, P.Blessed prince, "Round Robin based secure aware packet scheduling in wireless networks, IJEST, ISSN:0975-5462, vol 5, No. 3, March 2013.