Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA

Rajesh Duvvuru[1], Sunil Kumar Singh[1], Gudikhandula Narasimha Rao[2], Ashok Kote[3], Bangaru Bala Krishna[4], and Moturu Vijaya Raju[5]

[1] Department of Computer Science Engineering, National Inst. of Technology, Jamsehdpur, Jharkhand, India
[2] Department of Computer Science Engineering, K.I.T.S, Guntur, A.P., India
[3] Department of Computer Science Engineering, L.I.M.A.T, Vijayawada, A.P., India
[4] Department of Computer Science Engineering, T.I.T.S, Hyderabad, A.P., India
[5] Department of Information Technology, U.R.C.E.T, Vijayawada, A.P., India
{rajeshduvvuru.cse,sunilkrsingh.cse}@nitjsr.ac.in,
{gudikhandula,kote.ashok,bbk.tits,vijayaraju.m}@gmail.com

Abstract. Security and ease of use are two fundamental requirements of wireless network users. But they conflict with each other. The strongly secure network will put a lot of load on the server for security related work which may hamper the packet delivery ratio. But strong security is indispensable for maintaining the confidentiality of information in current real-time wireless communication networks. This research work combines both, the concepts of network security and the packet scheduling issues of the wireless data packets. Most of the users using wireless network are unaware about what level of security is needed for them. We present a new Automated Security-Aware Packet Scheduling Strategy or ASPS for real-time wireless network. This ASPS algorithm assigns the desirable level of security automatically to the respective data packets with guarantee of deadlines for the packets. Our simulation result proves that our proposal is performing better than existing algorithms in terms of the quality of security, guarantee ratio and reducing the load on the network switch.

Keywords: Load on network switch, security identification adapter, advanced radius authentication server, Automated Security-Aware Packet Scheduling Strategy, Wireless LAN Security.

1 Introduction

Wireless technology has created one of the greatest revolutions in the usage of mobile gadgets. In most of the wireless applications like accessing internet, video calling, live TV, and many other useful applications, wireless technology plays a vital role.

According to the recent survey report of 2008, approximately 86% of total network across the surveyed cities appeared to be vulnerable, since 37% of these networks appeared to have no encryption and 49% of networks to be using WEP encryption [1].

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 185–196, 2013.

Most of innovative applications made the wireless technology even more interesting a research area for the scientists and research scholars. Exchanging the information from the source to destination in a confidential and reliable manner, from one mobile node to another mobile node is always a challenging task. For example, data in wireless networks is broadcast in the form of radio waves. In the computer science literature there are lot of data-security related algorithms, yet information exchange faces a lots of security allied attacks like identity theft(MAC spoofing) [2], Man-in-middle [3], Denial of service [4], Network injection [5], and the like. All these security threats have worsened the secure data transmission in wireless networks which leads to bad service being provided by the wireless communication companies. It has also affected them badly in the commercial sense. This is the one of the main reason why security became a foremost part in the field of wireless networks. Plenty of security protocols have been introduced in the arena of wireless network for secure data transmission. The IEEE 802.11 family has mostly concentrated on the security issues like authentication and confidentiality [6]. Most of the data transmission was in static mode level of security. This reflects that, mobile nodes are using same level of security for the data transmission. Different levels of security should be maintained for different type of users. If the user is a highly important, for that particular user, security should be high, compared to the other mobile and wireless nodes [8]. These security levels should be maintained for each and every specific user. For instance, in the Banking system, the current data transaction record will need more level of security than data transaction record twelve years before. Modelling the security mechanism for wireless networks in flexible way is always a challenging task. In this paper, we present a new Automated Security-Aware Packet Scheduling Strategy or ASPS for real-time wireless network. This ASPS algorithm assigns the desirable level of security automatically to the desired data packets with guarantee of deadlines for the packets. Assigning the security level represents encrypting the data by applying the different cryptographic algorithms at each level. Maintaining same level of security is a disadvantage. This is one of the important fragile points of the wireless communication. To avoid this sort of security issues, we are assigning different levels of security for each and every wireless node according to the priority.

This paper comprises five major contributions (1) Simulator for which ASPS algorithm was implemented and tested. (2) Automatic assigning of security levels to the specific nodes (3) It combines the both security and guarantee ratio of packets (4) A new model of wireless data-packet have been designed (5)Novel performance evaluation by combining security, guarantee ratio and load on network switch. This paper is organized in the fallowing way: section 2 describes how the security and packet scheduling were achieved in the wireless communication. Section 3 explains about the ASPS algorithm. Section 4 discusses the simulation results. Lastly we will conclude and assert the future scope for this work in section 5.

2 Related Work

Our research work provides an automatic schema for assigning security levels to real-time wireless nodes. We are going to overcome the high level complexity of assigning security to the deserved N number of users sending or receiving the data through their

wireless devices. These are some real-time wireless packet scheduling algorithms [9][10]. These packets are going to be scheduled to reduce the latency time and increase the performance of data transmission. Normally most of the people who are using wireless networks for data transmission are not much aware of technical aspects of the security issues, but every user wants to send the data in a confidential and secure way. In 802.11 wirelesses LAN, we can provide common level of security to all users where there is no differentiation between the high-end user who requires high-level of security, middle-level user who requires average-level of security and low-end user who require very less amount of security. By classifying the users in different levels we can provide an efficient data transmission and which will reduces the burden and delay in the network. For instance, in WLAN we have applied AES algorithm for encryption and decryption of data. Assume the network is capable of transmitting 2KB/sec of data, where the network devices are bounded at maximum 10 meter range. For the similar WLAN with same bandwidth and same network setup if DES algorithm is applied for secure data transmission it will transmit more than 2KB/sec for maximum 10 meter. Because the key length of AES ranges up to 256 bits and for DES is 56 bits. No doubt AES algorithm is much secure than DES algorithm in terms of security [11] whereas data transmission is low due to key size. The wireless device users who are not much considered about applying AES in WLAN are giving additional burden to the network; for these sorts of users, DES will be the best for data transmission and data-packets exchange is also fast. Our research combines the better secure transmission of the wireless data-packet, packet scheduling algorithm and reducing the network load for the fast data transmission.

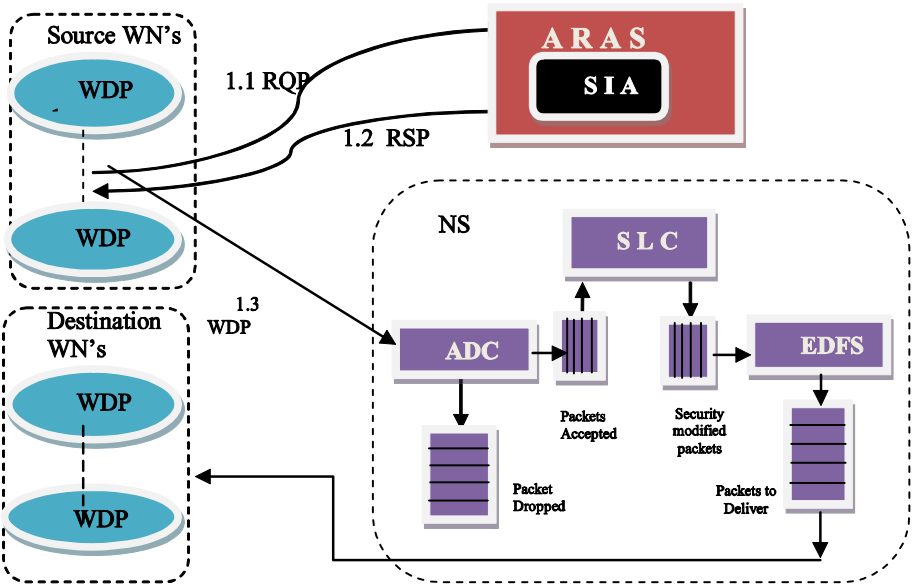

Fig. 1. Schematic Diagram of Network System

3 Advanced Security-Aware Packet Scheduling

In our research work we have modelled a novel Authentication server, Advanced Radius Server Authentication (ARSA), which will perform authentication of WN(Wireless Node) of particular network connected in Wireless Local Area Network (WLAN). Each and every WN works as both sender and receiver, which we call as the transceiver. Normal Radius Server Authentication (RSA)[12] will do perform authentication, authorization and accounting (AAA) of one particular WN by using its IP address, whether it is belongs to that network or not, if the WN is valid, then it will allow that particular WN to access all other resources in that specific network. In addition, we are making RAS to assign the security level for that particular WN by including the SIA (Security Identification Adapter). This SIA will recognize the IP address and assign the deserved security level to that particular WN. The IP addresses are classified into different classes [14], where each class got its own importance and according to its importance, SIA will assign the security level and acknowledge with AAA. For instance class E IP address of WN will be assigned higher level of security when we compared to the class D or C. Depending upon future requirement, further these IP address classes can be classified into sub classes. In addition to the Network Switch (NS), it contains the Admission Controller (ADC), Security Level Controller (SLC) and Earliest Dead line First Scheduling (EDFS), for further detail information please refers this research paper [13]. ADC will accept or reject the Wireless Data Packets (WDP) which are sent from the Wireless Node (WN), depending on their deadlines. SLC will increase the security level if it is having enough dead line. EDFS follows the policy of Earliest deadline first and processes WDPs from Security modified packets queue to Packets to Deliver queue.

3.1 Assumptions and Notations

In this Network we have designed three different types of packets they are request-packet (RQP), Response-Packet (RSP) and WDP. Two for communication between WNs and ARSA and other is communication between the WNs and NS. Before accessing the WLAN, WN should authenticated by means of ARSA, if the WN is valid then ARSA will grant the permission to access the network otherwise authentication will be rejected. Firstly, WN will send a RQP to the ARSA. RQP contains only IP Address (IPAi), and then the ARSA will check the RQP. If it is valid RQP, ARSA will sent back the RSP to WN over NS. RSPi represented by a tuple (ACi,SLi), where ACi denotes Permit/Reject of Access and SLi represents Security Level.

Once the source WN granted permission to access the network, then it will start communicating with NS. Then the WDP are directed from source WN to the destination WN through NS. Basically WDP is represented with a set of fields (ATi,PTi,SLi,Di)[8]. Here SLi and Di is represented with the security level and deadline of the packet i. ATi and PTi denotes arrival and processing time of packet i.

Equation (Eq)-1 specifies the formula for the calculation of deadline.

$$DLi >= CT_i - ST_i \quad (1)$$

Where STi starting time of the transmission of the ith packet, CTi is the completion time of the transmission, DLi is the packet's deadline.

To calculate the security operating cost without loss of simplification, we make use of formula Eq-2 to mold the security operating cost as the extra processing time experienced by packet i.

$$SOC_i = TT_i * (LS_i / MS) \quad (2)$$

Where SOCi represents security operating cost of the ith packet, TTi is the transmission time of the packet i, LSi is the level of security of the packet i, and MS is the maximum security level ranges from 1 to 10 according to the classes in the IP address.

Thus, the total processing time TPTi of packet i can be articulated as:

$$TPT_i = TT_i + SOC_i \quad (3)$$

For computing the load on network (LNS) switch we have used following equation 4.

$$LNS_i = (LS_i / MS) \quad (4)$$

3.2 The ASPS Algorithm

The ultimate aim of this research is to make the wireless users, confusion free, from assigning the security level for their wireless devices and reduce the load on NS, which results in improving the guarantee ratio and security level.

To accomplish this objective, we have designed the ASPS scheduling algorithm. Goal of ASPS is to maintain high guarantee ratio with automated security level. We can achieve high performance in terms of security level and guarantee ratio by instigating ARSA to our ASPS algorithm.

Fig.2 describes flow of the ASPS algorithm for the wireless transmission. The following steps will demarcate the procedure of the ASPS scheduling algorithm .Step1: WN will send RQP to the ARSA. RQP contains IPAi. Step2: After arrival of RQP from source WN, ARSA will check the RQP. If it is valid RQP, ARSA will send back the RSP to WN over NS. RSPi represented by a tuple (ACi,SLi). Step3: Once the RSP is received by the WN, depending on the RSP wireless node will be permitted to send and receive WDP on the network.Step4:If WN is permitted by ARSA it will access the Network through NS.Step5:WN sends WDPi to the NS , where WDPi denotes a set of attributes (ATi,PTi,SLi,Di).Step6: initializing the ASPS scheduler; the security standard of incoming WDPi and the number of rejected WDPi is set to zero. Hold until any incoming WDPi.Step7: If a packet i arrive at NS and it is the only packet available then process the packet instantly using its highest security level. The starting time (STi) and the completion time (CTi) of the WDPi are calculated.Step8: All the packets arriving in the NS during the time period [STi, CTi] are temporarily stored into a waiting queue in the ascending order of their deadlines. The starting time of the next packet STi + 1 is set to CTi.

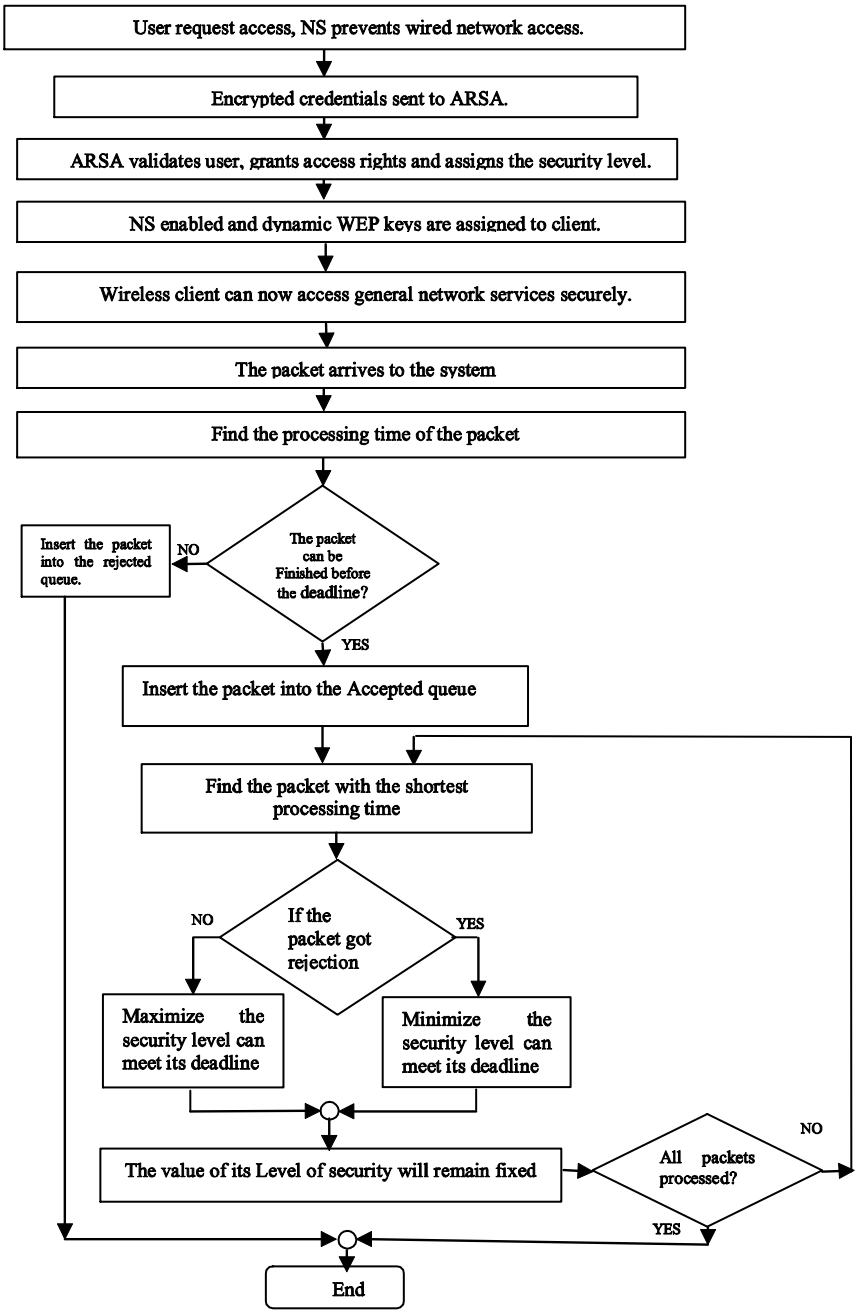

Fig. 2. The flow chart of the proposed system

Step9: The ADC will decide, if a WDPi in the waiting queue will be accepted or rejected with the respect to the deadline of WDPi. The WDPi which will meet its deadline will be sent to the accepted queue or else guided towards the rejected queue. Step10: The WDPi that are there in accepted queue will be forwarded to the SLC for modification(increment or decrement) of security level dynamically depending upon the various aspects like availability of bandwidth, congestion and data traffic in the network etc. Step11: The security modified WDPi will be sent to the EDF scheduler through security modified queue. Step12: The WDPi arrived in EDF scheduler will be delivered to the destination WN, according to their processing time. The WDPi having less processing time will be delivered first. Step13: Until all the WDPi are processed, the step 7 to step12 will be repeated.

3.3 Implementation Issues

We have implemented and tested the performance of ASPS, SPSS, MIN and MAX algorithms in NS-2 . We have chosen IEEE 802.11 WIFI, wireless LAN protocol for data transmission in our simulation environment.

Simulation of MIN, MAX and SPSS algorithm: We have considered four basic parameters i.e. data size = 0.3 KB, Bandwidth = 0.5 MBPS, dead line = 0.2 No/ Sec. Load on network switch and Level of Security (it will vary depending upon the algorithm) for all four algorithms. MIN, MAX and SPSS algorithm is having common simulation environment. Here, we have taken total six WN, one RAS and one NS. We have assumed WN {0-2} as source nodes, WN {3-5} as destination nodes, RSA represented with number 6 and lastly NS as 7. Initially all the three WN {0-2} will communicate with the RAS for authentication to access the network, once the WN is permitted by the RAS. WN starts transmission of WDP to the destination WN {3-5} through NS. Here RAS will not assign any sort of LS to any WN. In MIN algorithm by default, WN-{0-2} data packets is encrypted with a very low encryption algorithm WEP by the WN itself before transmitting. Here we have considered both LS and LNS as 1. Whereas in MAX algorithm WN-{0-2} data packets are encrypted with WPA2 .Here LS and LNS is 10. Finally SPSS algorithm encrypts with WEP for WN-1(unimportant user),WPA 2 for WN-2 (unimportant user) and WPA2 for WN-3 (important user) and in this algorithms the LS and LNS varied from 1to 3. WN-2 is using WPA2 for encryption; even that user is not deserved for it, which leads to the load on network switch. These simulation results were plotted and discussed in section 4.

Simulation of ASPS algorithm: Lastly, we have conducted simulations for proposed algorithm. Here the simulation environment will differ a bit from rest of the three base line algorithm. Also we have considered similar environment, but RAS is replaced with ARAS. WN-{0-2} has started to access the network, and it is validated and assigned a specific LS depending up on IPA by ARAS.Here we have intentionally assumed WN-1 as unimportant user (requires low LS1, encrypted with WEP),WN-2 as important user (requires average LS-5, encrypted with WPA) and lastly WN-3 as extreme important user (requires average LS-10, encrypted with WPA2) [6]. After encrypting WDP with specified algorithms, the communication will take place between source and destination WN through NS. Figure 3 represents snapshot of simulation environment of ASPS algorithm.

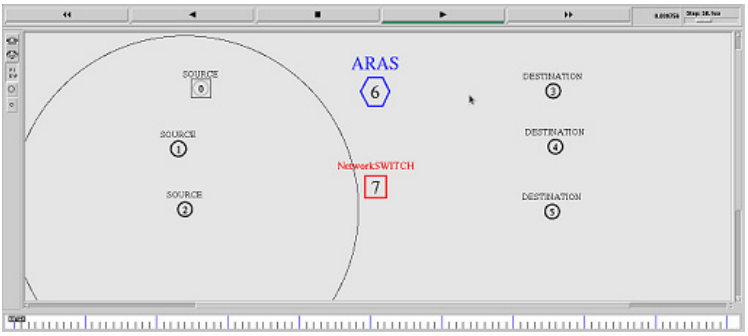

Fig. 3. Simulation of ASPS algorithm

4 Simulation Results

4.1 Comparison of ASPS with MIN, MAX and SPSS Algorithms

At this instant we are going momentarily summarize the baseline algorithms-SPSS, MIN and MAX. Further these algorithms are going to compare with the proposed ASPS algorithm. 1. MIN: All the WN's sends WDP's to NS with lower security level, here the specific WN user, who need high level security, can't do it and cost of guarantee ratio is enhanced at the cost of dropping SOC. 2.MAX: All the WN's sends WDP's to NS with higher security level, here most of the WN user, who don't require maximum security level, it leads to the load on the NS, where LS is improved, but guarantee ratio will be reduced. 3. SPSS: This algorithm will provide different levels of security to the different WN's user, which will results medium performance in levels of security and guarantee ratio of WDP. Limitation of SPSS is WN user have given individuality to assign LS to WDP's, which it leads to the unwanted user also will opt for high level of security to WDP's and sent to NS, which will increase burden to NS. We proposed a novel scheduling algorithm, which will give equal level of performance as that of SPSS in terms of LS and GR, in addition to this ASPS will assign automatic security levels to the specific user depending up on their necessity, which will reduce load drastically on NS.

4.2 Performance Evaluation

The performance of our approach will be evaluated by comparing the ASPS algorithm with SPSS, MAX and MIN. The performance measurement is based on mainly four parameters they are Guarantee ratio (GR), level of security (LS), overall performance (OP) and Load-on-Switch (LOS). Overall performance can be calculated by following Eq-5:

$$OP= (GR * LS) + LOS \tag{5}$$

4.3 Impact of Bandwidth

In the following experiment, we have varied bandwidth from 0.1 to 0.3 MBPS and compared our approach result with remaining three baseline algorithms namely SPSS, MIN, and MAX .It is a universal fact, whenever the bandwidth is high we can send more number of packets, high network bandwidth leads to short transfer times, which in turn result in short processing times of packets. This helps the WN to transmit and receive the WDP's efficiently. It leads to the high level of security that can be incremented, so that overall performance can be improved. Fig.5 Defines cross product of both Guarantee Ratio and Level of Security in addition of Load-on-Switch with respect to the bandwidth. The overall performance of ASPS is in peak state whereas SPSS, MIN and MAX follow next.

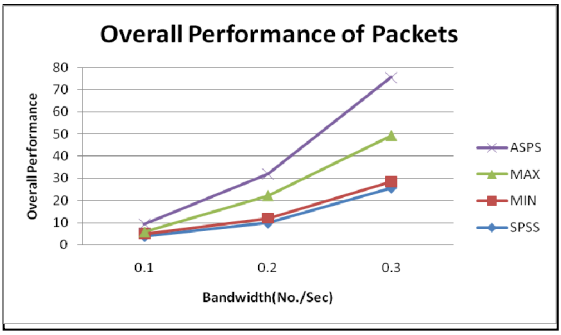

Fig. 4. Impact of bandwidth on Overall performance when data size = 0.3 KB, arrival rate = 0.5 No/Sec, and deadline = 0.2 No/Sec.

4.4 Impact of Arrival Rate

This research work is intended to compare ASPS stratagem with three baseline method. The first baseline method is called SSPS, which will assign different level of security for the incoming data packets .Secondly, MIN method which will assign smallest amount level of security to the incoming packets given to the network switch (NS) and finally, MAX method assigns the maximum amount of security to the data packets arriving at the network switch. To achieve this target, the arrival rate was increased of the incoming packets from 0.1 to 0.3 No./Sec. and the data size was set to 0.5 KB, the Bandwidth to 0.5mbps, and the deadline to 0.2 No./Sec. Fig. 5 Delivers ASPS will execute peak performance when we compared to the other baseline algorithms MIN, MAX, and SPSS in respect to the Arrival rate over the overall performance of the network system.

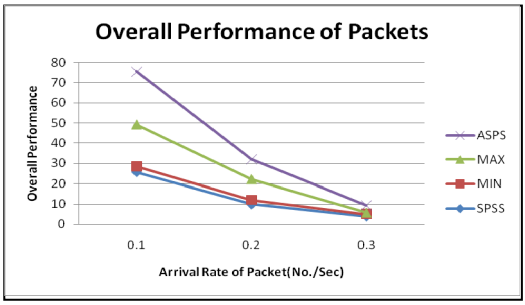

Fig. 5. Impact of arrival rate on Overall performance when data size = 0.3 KB, Bandwidth = 0.5MBPS, and deadline = 0.2 No/Sec

4.5 Impacts of Data Size

In this experimentation, we evaluate the efficiency of ASPS aligned with SPSS, MIN and MAX schemes changing the data size from 0.5 to 1.5KB. Further, we observe Fig. 6 On every occasion the data size is increased the overall performance of ASPS is incremented comparatively.

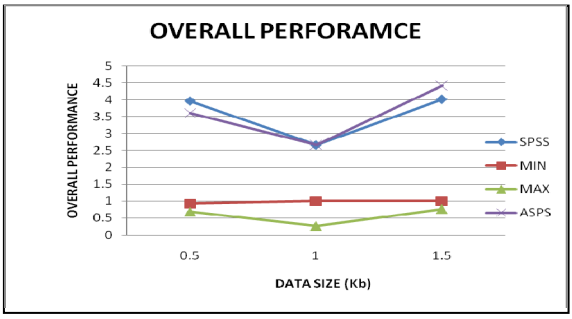

Fig. 6. Impact of Data size on Overall performance when Bandwidth = 0.5MBPS, arrival rate = 0.5 No/Sec and deadline = 0.2 No/Sec

4.6 Impacts of Deadlines

The deadline is another important concern, which has a great impression on our wireless network system. Initially, we vary our deadline from 0.1 to 0.3 no/sec. and we observe the consequence on the network system in detail. The figure below clearly reveals that when we vary the deadline from 0.1 to 0.3 no/sec, then the security level of the WDP's is automatically incremented in the network switch (NS) and eventually the performance is enhanced. The concept which unfolds this mechanism is whenever the deadline has some flexibility, then obviously there will be an advantage of time for that particular packet to get delivered and hence the security level will be increased for that particular packet because load on the network switch will be reduced. This verifies that the ASPS system has a high impact over SPSS, MIN or MAX in terms of security enhancement. Fig.19 exposes clearly that the overall performance is increasing exponentially along with growth in the deadline.

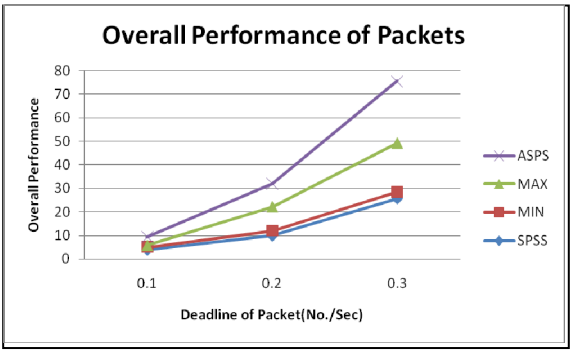

Fig. 7. Impact of Deadline on Overall performance of packets when data size = 0.3 KB, Bandwidth = 0.5MBPS, and arrival rate = 0.5 No/Sec

5 Conclusion and Future Scope

In the current real-time scenario wireless network has reached its summit. In spite of innumerable demands there still exists a lot of challenging task like quality of service, high-speed data transmission and secure communication etc. To overcome such a challenging task, we have designed and simulated an innovative approach (ASPS), which will result better in terms of guarantee ratio, level of security and load on network switch (for the fast data transmission).In our algorithm we are making Advanced Radius Authentication Server (ARAS) to think intelligently while assigning the security level for the incoming request packets, which will increase the data transmission and reduce the load on network switch. Comparing ASPS with other baseline algorithms, we have observed better performance regarding Load on network switch and Overall performance. Assigning dynamic security level to the wireless mobile node became interesting research area for the researchers. This research work provides future scope for Hybrid mechanism for assigning the security level to the specified user.

References

1. http://www.deloitte.com/assets/DcomIndia/Local%20Assets/Documents/All%20India%20Wifi%20Survey.pdf
2. Nagarajan, V., Arsaan, V., Huang, D.: Using Power Hopping to Counter MAC Spoof Attacks in WLAN. In: Conference on Consumer Communications and Networking Conference, pp. 1–5 (2010)
3. Eberz, S., Strohmeier, M., Wilhelm, M., Martinovic, I.: A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 235–252. Springer, Heidelberg (2012)
4. Huang, H., Ahmed, N., Karthik, P.: On a New Type of Denial of Service Attack in Wireless Networks: The Distributed Jammer Network. IEEE Transactions On Wireless Communications, 2316–2324 (2011)

5. Park, J.C., Kasera, S.K.: Securing Ad Hoc Wireless Networks Against Data Injection Attacks Using Firewalls. In: IEEE Wireless Communications and Networking Conference, Salt Lake City, pp. 1525–3511 (2007)
6. Lashkari, H., Mohammad, M., Danesh, S.: A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i). In: Second IEEE International Conference on Computer Science and Information Technolog 2009, Kuala Lumpur, Malaysia, pp. 48–52 (2009)
7. m [7] Xiao Qin, Mohamed Alghamdi, Mais Nijim, Ziliang Zong, Kiranmai Bellam, Xiaojun Ruan,and Adam Manzanares. : Improving Security of Real-Time Wireless Networks through Packet Scheduling. In: IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 2008, IEEE Communications Society, pp. 3273- 3279, (2011).
8. Moh'd, A., Jararweh, Y., Tawalbeh, L.: AES-512: 512-Bit Advanced Encryption StandardAlgorithm Design and Evaluation. In: 7th International Conference on Information Assurance and Security, pp. 292–297. Halifax, NS (2011)
9. Han, S.-J., Oh, H.-S., Park, J.: The improved Data Encryption Standard (DES) Algorithm. In: IEEE 4th International Conference on Spread Spectrum Techniques and Applications Proceedings, Jongan Park, pp. 1310–1314 (1996)
10. Dua, A., Bambos, N.: On The Fairness Delay Trade-off in Wireless Packet Scheduling. In: IEEE Proceedings of the Global Telecommunications Conference, Palo Alto, pp. 25–48 (2005)
11. Alanazi, H.O., Zaidan, B.B., Zaidan, A.A., Jalab, H.A., Shabbir, M., Al-Nabhani, Y.: New Comparative Study Between DES, 3DES and AESwithin Nine Factors. Journal of Computing, 152–157 (2010)
12. http://www.rsa.com/rsasecured/guides/imp_pdfs/Cisco_VPN3K_47_AuthMan7.1.pdf
13. Mattihalli, C.: Designing and Implementing of Earliest Deadline First scheduling algorithm on Standard Linux. In: 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing, Green Computing and Communications (GreenCom), Hangzhou, China, pp. 901–906 (2010)
14. Bruno, R., Conti, M., Gregori, E.: Throughput Analysis and Measurements in IEEE 802.11 WLANs with TCP and UDP Traffic Flows. IEEE Transactions On Mobile Computing, 171–186 (2008)