THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-14-December-2019

A Novel Service-Level Security-Aware Packet Scheduling Algorithm

R. Nandakumar

Assistant Professor, R. V. Government College, Chengalpet

ABSTRACT

In mobile ad-hoc networks, several packet scheduling algorithms are provided for packet transmission. To improve the security, privacy along with less delay during the packet transmission is improved by using security-aware packet scheduling algorithms. Different security standards and algorithms are developed for protecting the data transmission over wireless networks. However, the dynamic security algorithms for real-time applications on wireless networks are mostly not developed perfectly. Therefore, an Improved Security-Aware Packet Scheduling (ISAPS) algorithm is introduced based on the dynamic Security-Aware Packet Scheduling algorithm.

Keywords: Mobile ad-hoc networks, Packet scheduling, Security-Aware Packet Scheduling, Scheduling algorithm.

1. INTRODUCTION

In ISAPS, each node has the single transmitter and receiver which are combined in the transceiver. Therefore, the node does not have ability to transmit and receive the packets simultaneously. The transmitters are matched with their corresponding receiver by using the packet scheduler. In addition, the system includes the three components such as Security Level Controller (SLC), Admission Controller (AC) and Earliest Deadline First (EDF) scheduler. The ISAPS is the heuristic algorithm. When the new packet is arrived, the minimal security level admission test is performed which means the packet is given the minimal security level and is inserted into the accepted queue of the node by using the Earliest Deadline First (EDF) policy. If this test can guarantee the timing constraints of the new packet and packets whose execution orders are later than that of the new packet in the accepted queue, it is denoted as the packets are accepted. Or else, the security level of packets waiting in the accepted queue using the Round-Robin (RR) policy is degraded by the ISAPS algorithm until the new packets are accepted.

If all the security levels of packets being degraded to minimal still miss the deadline of the new packet or violate the timing constraints of packets whose execution orders are later than that of the new packet, then it is rejected or it is allocated to the accepted queue. If the new packets are inserted into the accepted queue without any degradation of the security levels of packets waiting in the accepted queue, then ISAPS increases the security level as high as possible. If the new packets are not allocated with the minimal security level then the security levels of some packets in accepted queue are degraded for improving the schedulability whereas the new packets are rejected by the SPSS.

This algorithm includes the inputs such as packet count, bandwidth, packet size, arrival rate, deadline and security level and the output is scheduling decision. However, this ISAPS algorithm was not dealing with the packets with dependent relations. Hence, in this paper, dependent relations are considered in ISAPS algorithm by discovering the service dependencies in mobile ad-hoc networks. In this paper, service-level security-aware packet scheduling algorithm is explained in brief.

2. SERVICE-LEVEL SECURITY-AWARE PACKET SCHEDULING ALGORITHM

In this paper, our proposed service-level security-aware packet scheduling algorithm is described. The ISAPS algorithm is improved by considering the packets to be dependent to each other. This is achieved based on the dependence discovery method. Here, two types of dependencies are considered based on the service of packets. In this paper, these two types of dependencies are explained and detection of dependencies, representation of dependencies and construction the representation are also described.

2.1 Service Dependencies

The dependence in the service-based systems is defined as the relation between services which are defined by the flow of packet processing induced by the client requests. When there is a service dependence relation

ISSN:0971-1260

Vol-22-Issue-14-December-2019

between two services such as S_1 and S_2, one service is represented as the source of the dependence and the other service is denoted as target of the dependence. In our proposed system, two types of dependencies are considered over the given set of services. The two types of service dependencies are inter-dependencies and intra-dependencies. Inter-dependence is the fundamental dependence relation between the requester of the service and the receiver of that request. Intra-dependence is referred as more complex relation between services which relates an incoming inter-dependence to an outgoing inter-dependence (Novotny, P., et al. 2013).

2.2 Dependence Graph (DG)

The dependence graph is referred as the directed acyclic graph which is constructed from the set of nodes to represent the services and the set of edges to represent the direct inter-dependence from source to target (Wang, S., & Capretz, M. A. 2009). Every node is annotated with the intra-dependence information, theoretically including directed edges between the incoming and outgoing inter-dependencies of the service. The DG is used for maintaining the information regarding the particular time duration, resulting only the dependence packet information collected by the monitoring agents during that time duration. The time duration is the property of the interaction between the application behaviour, network behaviour, and the information accessible to the monitoring agents.

2.3 Intra-Service Dependent Security-aware Packet Scheduling Algorithm (ISDSPS)

Here, the packets are assumed to be dependent between service requester and receiver. The major objective of the proposed ISDSPS is scheduling and providing the security for the set of real-time packets based on their client service request. After discovering the service dependencies of packet then the security levels are provided by the following process. The clustering algorithm (CL_c) is utilized for clustering inter and intra-service dependence packets related to T_s according to the size of packets, type of protocol, packet deadline time, node IP and conversation identifier. Once the clustering process is performed, the transmission orders and sorted means are calculated for intra-service dependence packet in each cluster. The reason of this measurement is prioritizing the clusters with high intra-service dependence for scheduling process.

When the service dependent packets are arrived, the maximum security level is given to the packet and they are transmitted to the accepted queue of the node by using Earliest Deadline First (EDF) policy. The packets are scheduled based on the security levels. In the proposed approach, the inputs are packet count, bandwidth, packet size, arrival rate, deadline, target service, and security level and the output is scheduling decision.

Algorithm: ISDSPS

Input: packet count, bandwidth, packet size, arrival rate, deadline, target service and security level

1. Check the schedulability condition using (1) and (2)
2. Clustering the real time service packets based on similarity measurement calculated by (6)
3. Prioritizing intra dependency clusters and packets within the intra dependency cluster
4. Calculate the start time of each prioritized packets intra service dependency using (7)
5. Calculate the total processing time of packets with respect to deadline time using (8)
6. Provide security level to each packets using (10) and (11)
7. Scheduling the packets

2.4 Intra and Inter-Service Dependent Security-aware Packet Scheduling Algorithm (IISDSPS)

Nevertheless, intra-service dependency detection provides better security and schedulability for intra-service dependency packets; there may be a chance of misclassification during the clustering process. The packet

ISSN:0971-1260

Vol-22-Issue-14-December-2019

belonging to intra-service dependence cluster may be clustered into the inter-service dependence cluster. For this situation, packet shuffling process is required for packets which are again prioritized for packet scheduling.

If there is any packet in inter-service dependence cluster related to intra-service dependence cluster, then the similar priority is given to those packets as that of intra-service dependence cluster and the packet scheduling process is continued.

Algorithm: IISDSPS

Input: packet count, bandwidth, packet size, arrival rate, deadline, target service and security level

1. Check the schedulability condition using (1) and (2)
2. Clustering the real time service packets based on similarity measurement calculated by (6)
3. Prioritizing intra dependency clusters and packets within the intra dependency cluster
4. Check whether there is any packet in inter service dependency cluster is related to intra service dependency cluster using (12)
5. If yes, then give same priority as that of intra service dependency cluster packets
6. Calculate the start time of each prioritized packets intra service dependency using (7)
7. Calculate the total processing time of packets with respect to deadline time using (8)
8. Provide security level to each packets using (10) and (11)
9. Scheduling the packets

3. PERFORMANCE EVALUATION

The performance of the proposed security-aware packet scheduling algorithms is evaluated by using Network Simulator-2 (NS2). Consider, the number of nodes is 200 and the packet size is 5KB. The comparison is performed based on the performance metrics such as guarantee ratio, average security level, packet delivery ratio, and end-to-end delay. The parameters utilized for comparison are such as deadline of packets and packet arrival rate. Algorithms considered for comparison are ISAPS, ISDSPS, and IISDSPS.

3.1 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

$$GR\ (\%) = \frac{Total\ number\ of\ packets\ guaranteed\ to\ meet\ their\ deadlines}{Total\ number\ of\ packets} \times 100\%$$

Deadline versus Guarantee Ratio (%)

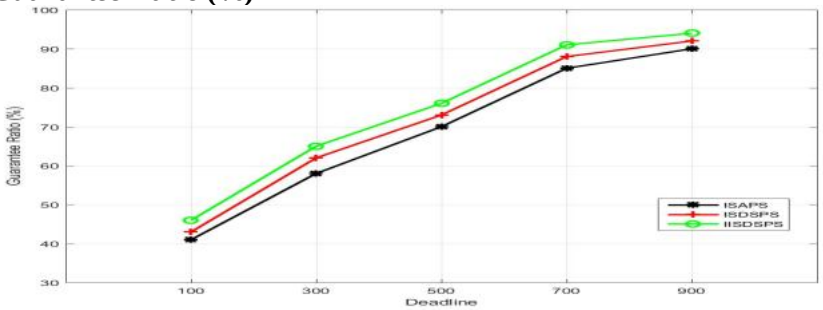

Figure-1: Deadline versus Guarantee Ratio (%)

Figure 1 shows that the result of guarantee ratio comparison in terms of deadline. From the graph, it is proved that, if the deadline increases then the guarantee ratio (%) is also increases. The major reason for achieving high guarantee ratio is that when packets have loose deadlines, they can more easily be delivered

ISSN:0971-1260

Vol-22-Issue-14-December-2019

before their deadlines. Thus, the guarantee ratio is increased. The proposed IISDSPS has higher guarantee ratio than the other algorithms.

3.2 Average Security Level

The average security level is defined for representing the security of accepted packets.

Deadline versus Average Security Level

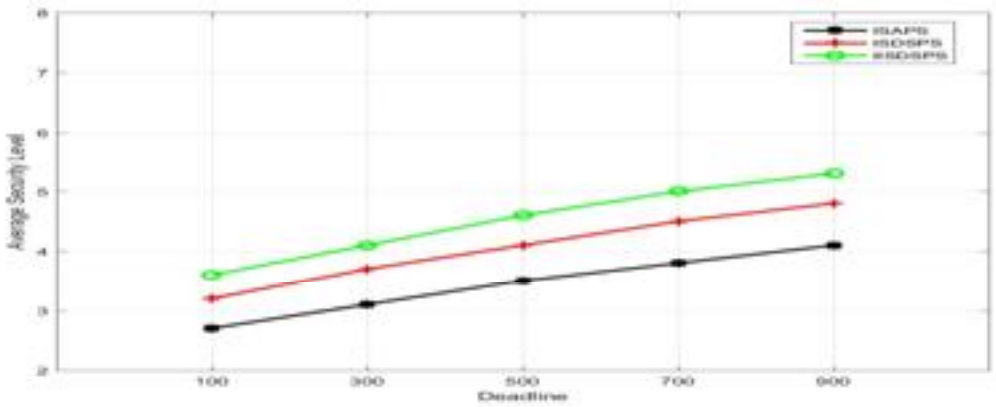

Figure-2: Deadline Vs Average Security Level

Figure 2 shows that the result of average security level comparison in terms of deadline. From the graph, it is proved that, if the deadline increases then the average security level is also increases. The major reason for achieving high average security level is that ISAPS cannot effectively adjust the security levels of accepted packets due to the lacking of the ability for adapting to the system workload changes. Thus, the average security level is increased. The proposed IISDSPS has higher security levels than the other algorithms by satisfying the user's requirements.

3.3 Packet Delivery Ratio (PDR)

The packet delivery ratio is defined as the fraction of number of delivered data packets to the destination and is measured as follows,

$$PDR = \frac{Total\ number\ of\ received\ packets}{Total\ number\ of\ transmitted\ packets}$$

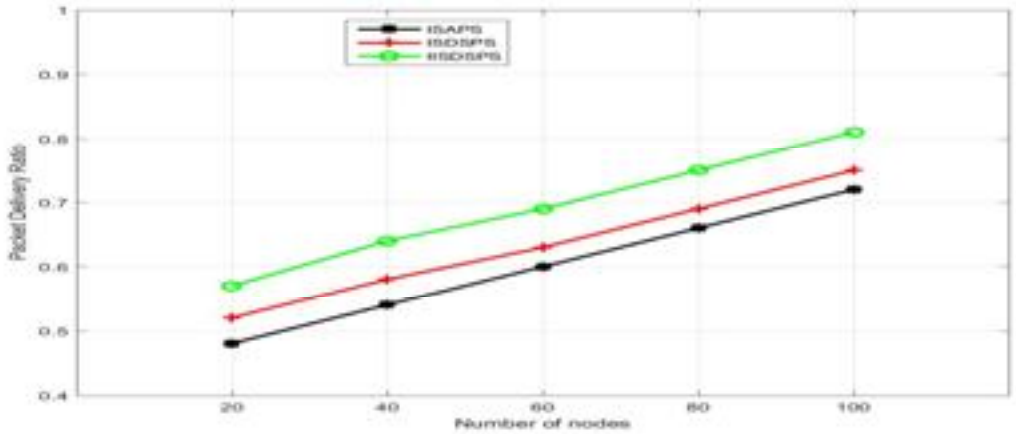

Figure-3: Number of Nodes versus Packet Delivery Ratio

Figure 3 shows that the comparison of packet delivery ratio. From the graph, it is proved that, when number of nodes increases the packet delivery ratio is also increases due to the proper schedulability and security,

ISSN:0971-1260

Vol-22-Issue-14-December-2019

more number of transmitted packets is delivered to the destination successfully. The proposed IISDSPS has higher packet delivery ratio than the other algorithms.

3.4 End-to-End Delay

The end-to-end delay is defined as the time period which is taken for the packet transmission from source to destination and is computed as,

$$End - to - end\ delay = \frac{Total\ delay\ of\ packets\ received\ by\ the\ destination}{Number\ of\ packets\ received\ by\ the\ destination}$$

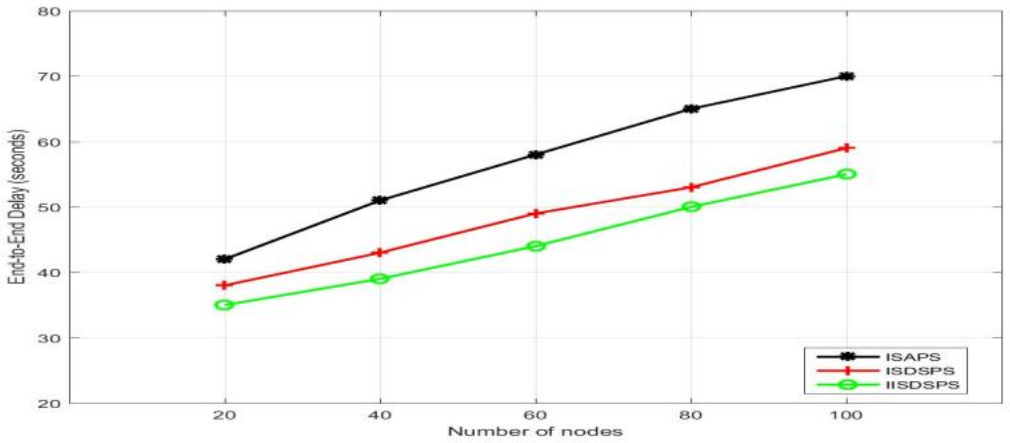

Figure-4: Number of Nodes Vs End-to-End Delay (Seconds)

Figure 4 shows that the comparison of end-to-end delay. From the graph, it is proved that, when number of nodes increases the end-to-end delay is decreases due to the packets are scheduled based on their deadline time and service which provides the reduction in delay time. The proposed IISDSPS has less end-to-end delay than the other algorithms.

4. CONCLUSION

The issues of the dependence of packets in security-aware packet scheduling algorithm for mobile ad-hoc networks are considered. These issues are removed by introducing the service-dependence discovery method which is based on the inter-service and intra-service dependency of packets and the service dependencies of packets are achieved by using dependence graph and dependence matrix. The security level of packets is provided based on the clustering process which is utilized for discovering the service relations of the packets. Hence, the proposed ISDSPS, and IISDSPS based algorithms perform better than the ISAPS based algorithm. The experimental results are proved that the proposed IISDSPS has better performance than the other algorithms.

REFERENCES

1. Zhu, X., Guo, H., Liang, S., & Yang, X. (2012). An improved security-aware packet scheduling algorithm in real-time wireless networks. *Information Processing Letters*, *112*(7), 282-288.
2. Qin, X., Alghamdi, M., Nijim, M., Zong, Z., Bellam, K., Ruan, X., & Manzanares, A. (2008). Improving security of real-time wireless networks through packet scheduling [transactions letters]. *IEEE Transactions on Wireless Communications*, *7*(9).
3. Novotny, P., Wolf, A. L., & Ko, B. J. (2013, May). Discovering service dependencies in mobile ad hoc networks. In *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on* (pp. 527-533). IEEE.
4. Wang, S., & Capretz, M. A. (2009, July). A dependency impact analysis model for web services evolution. In *Web Services, 2009. ICWS 2009. IEEE International Conference on* (pp. 359-365). IEEE.

ISSN:0971-1260

Vol-22-Issue-14-December-2019

5. Nasir, H. J. A., & Ku-Mahamud, K. R. (2016). Wireless Sensor Network: A Bibliographical Survey. *Indian Journal of Science and Technology, 9*(38).
6. Kumar, M. R., Geethanjali, N., & Babu, N. R. (2013). Security Issues in Mobile Ad Hoc Networks. *International Journal of Engineering Inventions, 2*(11), 48-53.
7. Reddy, P. N., Vishnuvardhan, CH., & Ramesh, V. (2013). Routing Attacks in Mobile Ad Hoc Networks. *International Journal of Computer Science and Mobile Computing (IJCSMC), 2*(5), 360-367.
8. Gupta, A., & Ranga, S. P. (2012). Various Routing Attacks in Mobile AD-HOC Networks. *International Journal of Computing and Corporate Research, 2*(4).
9. Remzi H. Arpaci-Dusseau; Andrea C. Arpaci-Dusseau "Chapter 7: Scheduling: Introduction, Section 7.6: A New Metric: Response Time. Operating Systems: Three Easy Pieces (PDF). pp. 6. Retrieved February 2, 2015.