An Improved Intra and Inter Service Dependent Security Aware Packet Scheduling in Mobile Ad-hoc Networks

R. Nandakumar[#1], K. Nirmala[*2]
[#]Research Scholar, R & D Centre, Bharathiar University,Coimbatore, India.
[*]Associate Professor, Quaid-E-Millath College(W),Chennai,India.
[1]nandakumar1279@yahoo.com
[2]nimimca@yahoo.com

Abstract-**The main goal of this paper is to improve security level of packet scheduling by considering service dependencies of packets at each node. Service dependencies of packets are collected by using monitoring agents and the central authority is employed to integrate all the collected data in monitoring agents.. Packet service dependency can be concerned with both intra service dependencies and inter service dependencies. Intra service dependent security aware packet scheduling algorithm (ISDSPS) is proposed for maximizes the performance of packet scheduling. ISDSPS clusters the packets according to their client service request. Packets related to client service are grouped in intra service dependency cluster and packets that are not related to client service are grouped under inter service dependency cluster. Sometimes there may a chance of misclassification of packets. For effective clustering and scheduling, Intra and inter service dependent security aware packet scheduling (IISDSPS) is proposed for considering intra service dependency packets in inter service dependency clusters during packet scheduling process.**

Keywords - Packet scheduling, Intra service dependency, Inter service dependency, protocols, clusters

I. INTRODUCTION

In mobile ad-hoc networks (MANET), the most significant issue is anonymous communication. The anonymous communication is mostly utilized for protecting the source and destination of the communication link and the other intermediate nodes involved in communication connection which is difficult to find by the impostors. Different techniques are provided for improving the anonymous communication in MANET. However, MANET is vulnerable under particular circumstances such as passive attacks and traffic analysis attacks. In addition, the security-aware packet scheduling algorithm has less effectiveness since the attacker may easily identifies the source-destination links.

II. INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING (IIMLSDSPS)

The correlation of the dependencies between multiple layers such as service layers and network layers are considered with ISAPS algorithm. In the proposed method, the monitoring agents are used for collecting the dependency data from service layers and network layers. The collected data are correlated and utilized in the construction of the service layer dependence graph (SLDG). The directed acyclic graph is utilized as the local dependency graph while SLDG is utilized as global dependency graph. In addition, this approach is used for resolving the constraints by building the hypothesis list and rating the constraints for reducing the performance degradation. The policies which are employed across the networks are considered as constraints as they preclude the particular services from running on specific nodes or preclude two services from interacting. Therefore, the correlated dependencies across multiple layers are considered for enhancing the packet level security.

III. ANONYMITY-BASED INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING (AIIMLSDSPS)

The efficiency of security-aware packet scheduling algorithm is improved by including the concept of anonymity. The anonymity of the source locations are often breached by the attackers by traffic analysis and RF localization techniques. This can be protected by the proposed approach named fake source-location method. The fake source-location method introduces the fake sources in the network for confusing the attacker. The fake sources are generated dynamically while the event messages are transmitted by the original sources. The fake sources are utilized for constructing different fake paths in the network. As the number of fake paths is increased, the possibility of an adversary selection is increased. When selected, the adversaries are induced further away from the source. Initially, the attacker detects the original source node when it transmits the event messages to the base station. However, it is secured by the routing policy for prolonging the safety period of the original source. Hence, the chances of intrusion and packet loss are minimized by the proposed fake source-location method with minimum latency and overhead.

IV. 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.

A. Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

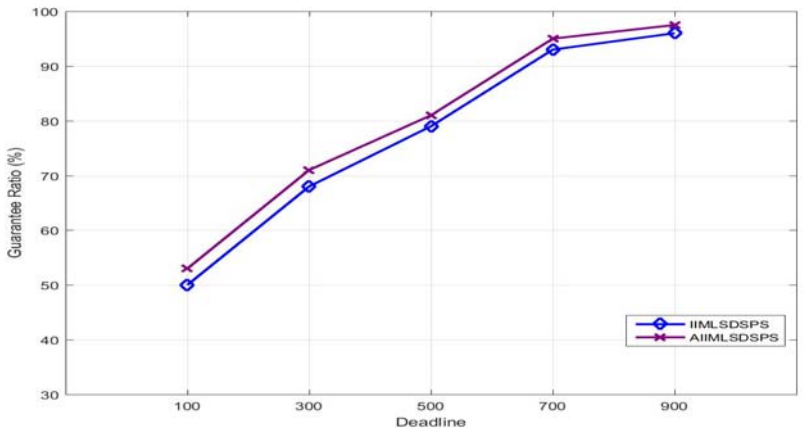

Fig.1. Deadline versus Guarantee Ratio (%)

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

B. Average security level

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

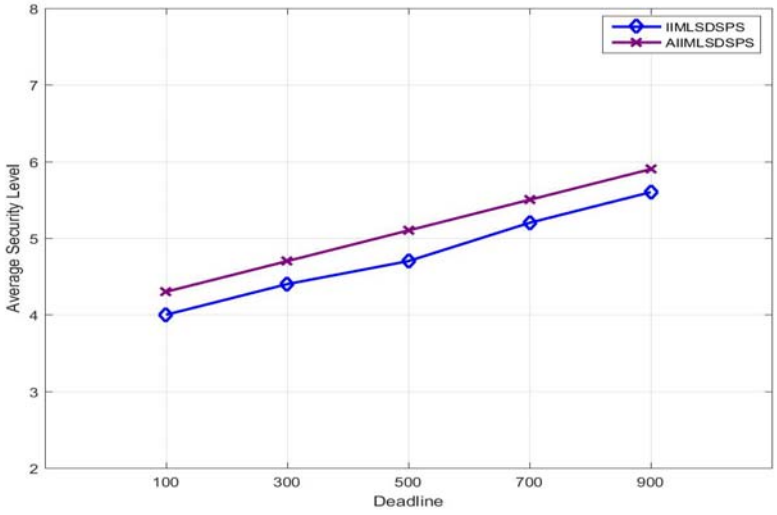

Fig.2. Deadline versus Average Security Level

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 IIMLSDSPS 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 AIIMLSDSPS has higher security levels than the other by satisfying the user's requirements.

C. 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,

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

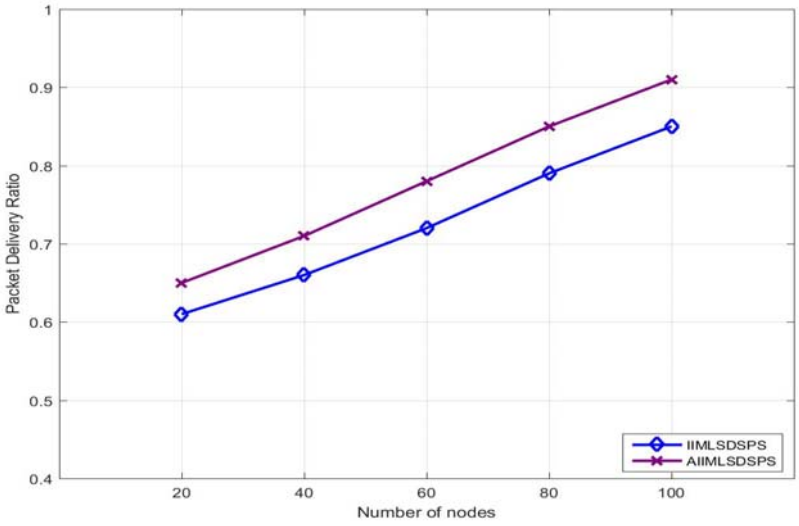

Fig.3. Number of Nodes versus Packet Delivery Ratio

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

D. 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,

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

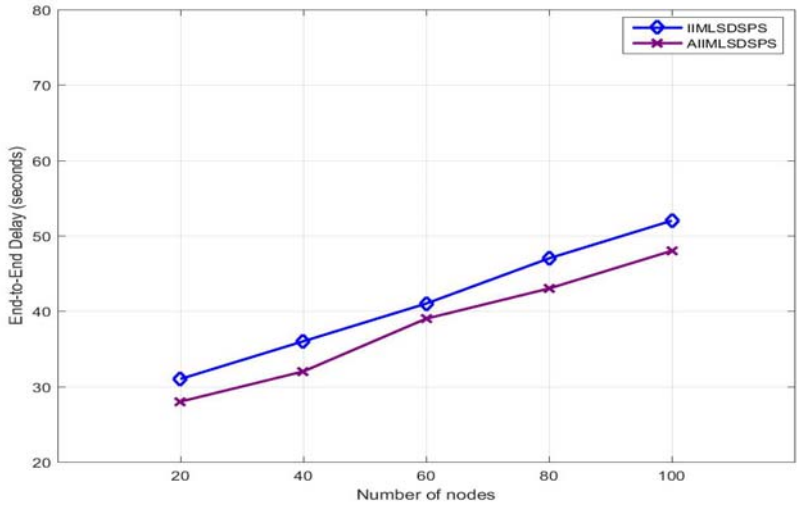

Fig.4. Number of Nodes versus End-to-End Delay (Seconds)

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 AIIMLSDSPS has less end-to-end delay than the other.

V. CONCLUSION

In this paper, the issues of the anonymous communication affected by the traffic analysis in mobile ad-hoc networks by using security-aware packet scheduling algorithm are considered. These issues are removed by introducing the anonymity-based fake source discovery algorithm which is integrated with the intra-inter and multiple-layer based service-dependence discovery method. The anonymity of the source locations are protected by using the fake source discovery and extension of the fake paths. Thus, the generated fake sources are utilized for confusing the adversaries during packet or message transmission. Hence, the proposed AIIMLSDSPS performs better than the IIMLSDSPS. The experimental results are proved that the proposed AIIMLSDSPS has better performance than the other.

REFERENCES

[1] Annadurai C. “Review of Packet Scheduling Algorithms in Mobile Ad Hoc Networks”. International Journal of Computer Applications, 15(1), pp.7-10. 2011.
[2] Zhu X, Guo H, Liang S & Yang, X. “An improved security-aware packet scheduling algorithm in real-time wireless networks”. Information Processing Letters, 112(7), 282-288.2012.
[3] Mansouri W, Zarai F, Mni, K, & Kamou, L. “New scheduling algorithm for wireless mesh networks”. In Multimedia Computing and Systems (ICMCS), International Conference on IEEE. pp. 1-6. 2011.
[4] Karim L, Nasser N, Taleb , & Alqallaf A. (). “An efficient priority packet scheduling algorithm for wireless sensor network”. In 2012 IEEE International Conference on Communications (ICC) pp. 334-338. IEEE. 2012.
[5] Saleh M & Dong, L. ().” Real-time scheduling with security awareness for packet switched networks”. In Radio and Wireless Symposium (RWS), pp. 391-394. IEEE. 2012.
[6] El M & Shaaban E. “Enhancing S-LEACH security for wireless sensor networks”. In Electro/Information Technology (EIT), 2012 IEEE International Conference on IEEE. pp. 1-6. 2012.
[7] Natarajan A, Ning P, Liu Y, Jajodia S, & Hutchinson S. E. “NSDMiner: Automated discovery of network service dependencies”. IEEE. pp. 2507-2515. 2012.
[8] Proano A & Lazos L. “Packet-hiding methods for preventing selective jamming attacks”. IEEE Transactions on dependable and secure computing, 9(1), pp.101-114. 2012.
[9] Thanikaivel B & Pranisa B.).” Fast and secure data transmission in MANET”. In Computer Communication and Informatics (ICCCI), International Conference on IEEE. pp. 1-5. 2012.