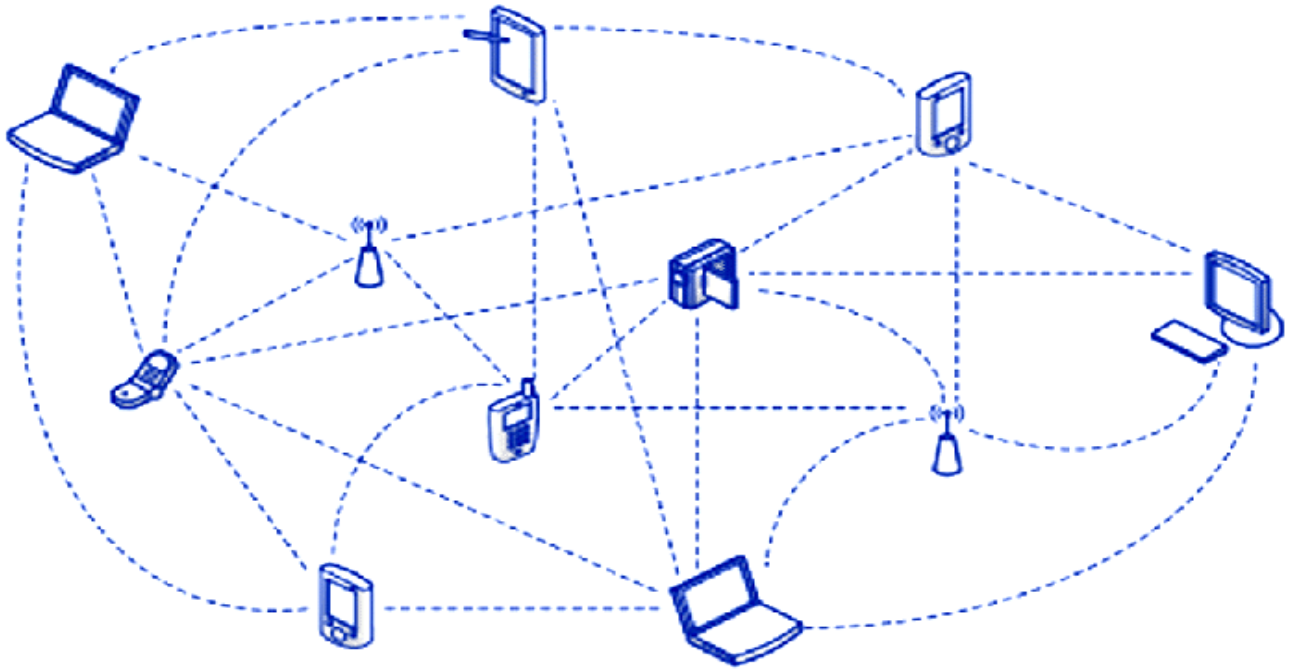
Dr. R. Nandakumar



ENHANCING PACKET-LEVEL SECURITY IN MOBILE AD-HOC NETWORKS

Enhancing Packet-Level Security in Mobile Ad-Hoc Networks

EMPYREAL PUBLISHING HOUSE

India | UAE | Nigeria | Uzbekistan | Montenegro

Enhancing Packet-Level Security in Mobile Ad-Hoc Networks

By:

Dr. R. Nandakumar

First Impression: 2020

Enhancing Packet-Level Security in Mobile Ad-Hoc Networks

ISBN : 978-81-946373-9-4

Rs. 650/- ($18)

DISCLAIMER

Information contained in this book has been published by Empyreal Publishing House and has been obtained by the authors from sources believed to be reliable and are correct to the best of their knowledge. The authors are solely responsible for the contents of the articles compiled in this book. Responsibility of authenticity of the work or the concepts / views presented by the authors through this book shall lie with the authors and the publisher has no role or claim or any responsibility in this regards. Errors, if any, are purely unintentional and readers are requested to communicate such error to the authors to avoid discrepancies in future.

Published by:
Empyreal Publishing House

Preface

Enhancing Packet-level Security in MANETs

MANETs are self-configuring, infrastructure-less network of mobile devices connected using wireless medium such that each device in MANET moves independently. In such scenarios there is higher risk of security in all levels and intruders are more open to the network. The packet level security is considered to be a major threat to the network performance as breach in packet level security causes high packet loss. For protecting the data transferred, secured wireless standards are utilized. However the lack of dynamic security mechanism allows the malicious users to access the networks and blocks authorized users and launch different attacks especially the packet dropping attacks.

In “An improved security-aware packet scheduling algorithm in real-time wireless networks” a secured scheduling called improved security-aware packet scheduling algorithm (ISAPS) has been developed. ISAPS method provides high priority to the packets to provide better scheduling when the load is higher. When the load is lighter, the security levels are increased along with the scheduling of the packets. In ISAPS, when a new packet arrives, the minimal security level admission test is carried out. The packet is provided with a minimum security level and then it is inserted into the accepted queue of a node by the earliest deadline first (EDF) policy. If this test can guarantee the timing constraints of the new packet and packets whose execution orders are not earlier than that of the new packet in the accepted queue, it is denoted that the packet can be accepted. Or else the ISAPS degrades the security level of packets waiting in the accepted queue using the Round-Robin policy until the new packet can be 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, it is rejected, or it is allocated to the accepted queue. If a new packet can be inserted into the accepted queue without degrading the security levels of packets waiting in the accepted queue, ISAPS raises the security level as high as possible to suit the adaptivity. Thus the packet level security is enhanced and packet loss is avoided completely or minimized considerably.

However the problem with ISAPS is that the approach assumes that all the packets are assumed to be with independent relations. So the approach lags behind when considering the packets with dependent relations.

In the first work, the problem of ISAPS is considered and the solution for the packets with dependent relations is proposed. The dependencies of the packets are needed to detected inorder to improve ISAPS to provide packet security. The service dependencies of the packets are of two types: inter-dependencies and intra-dependencies. Inter-dependence detection identifies pairs of source and target services from the flow of messages exchanged between the services. Intra-dependence detection is used to expose the correspondence between the incoming and outgoing inter-dependencies of a service. The proposed approach makes use of the monitoring agents in the mobile hosts to collect the dependencies data by intercepting the message traffic between

services and extracting relevant information. The data collected by the monitoring agents are local values and when global values of the dependencies relations are required, a central authority is employed with integrating all the data from the monitoring agents. However the central authority contacts only the monitoring agents with the relevant analysis and hence the communication is minimized. A dependence graph (DG) and a dependence matrix are utilized to represent the service and dependencies detected by the monitoring agents for better analysis of the service dependency relationships. Thus the packet service dependencies can be detected accurately with minimum delay and minimal data storage and communication requirements which can be employed for the security aware packet scheduling for better packet level security. However the performance can be further improved when the multiple layer dependencies are considered.

In the second work, the correlation of the dependencies across multiple layers, such as service layers and network layers, are included and the problems across the multiple layers are located. In the proposed approach, the dependency data collected by the monitoring agents are from service layers. The problem in representing the dependencies and detecting the relations is due to the scalability, decrease in accuracy and increase in computational complexity. Inorder to overcome the problems, the dependencies of the services collected at network layer and service layer are correlated and used in the construction of the service layer dependence graph (SLDG).The directed acyclic graph is used as the local dependency graph while the SLDG is used as global DG. The approach resolves the constraints by building a hypothesis list and then rating the constraints for performance degradation. The policies that are employed across the networks are considered as constraints as they preclude certain services from running on specific nodes, or preclude two services from interacting. Thus the correlated dependencies across multiple layers can be included for enhanced packet level security. Though the approach is efficient the non-inclusion of anonymity concept results in the intruder easily locating the source-sink nodes so that the packets from and to those nodes become insecure.

In the third work, the concept of anonymity is included for enhancing the efficiency of security aware packet scheduling inorder to provide higher packet level security. The anonymity of the source locations are often breached by the intruders through traffic analysis and RF localization techniques. This can be overcome by the proposed approach of protection called fake source-location method. The proposed fake source-location method introduces the fake sources into the network inorder to confuse the intruder. When the original sources send event messages to the base station, the fake sources are generated dynamically so that it is flexible. The fake sources construct several fake paths in the network and as the number of fake paths is more, there is higher possibility of an adversary selecting them. When selected, the adversaries are induced further away from the source. At the initial phase of the proposed method, the intruder eventually detects the original source node when it send event messages to the base station, but it is secured by a routing policy to prolong the safety period of the original source. Thus the proposed fake source-location method minimizes the chances of intrusion and reduces the packet loss with minimal latency and reduced overhead. However the main concern is that the approach consumes more energy inorder to satisfy security as the normal flooding requires considerable energy which is increased with fake paths and fake messages.

In the fourth work, the objective of reducing the energy consumed for satisfying the security of packets is considered. In order to optimize the energy consumption, the flooding process of the network is needed to be monitored. The proposed false source-location based privacy method is enhanced by including a flexible routing protocol called phantom routing. The proposed approach monitors the flooding process. The flooding process alone cannot provide privacy protection as the adversary can easily identify the shortest path between the source and the sink. This process also consumes more energy and the use of fake messages by the fake sources to generate the fake paths also increases the energy consumption. Hence Phantom routing is employed which is a two-stage routing scheme that consists of a directed walk along a random direction, which is followed by routing from the phantom source to the sink. Phantom flooding shares the same insights as probabilistic flooding in that they both attempt to direct messages to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source. Thus the proposed security aware packet scheduling method with the fake source-location and phantom routing enhances the security of the packets in the MANETs with reduced energy consumption and better efficiency.

Acknowledgements

I thank the almighty for having extended his choicest blessings by providing all the required resources, an able and amicable doctoral guide, good environment and a set of affable persons, to carry out this work successfully.

I would like to express my grateful and sincere thanks to my beloved parents, family members for always supporting, helping and encouraging me with their best wishes for my entire study.

I would also like to thank the guidance and advice given by friends who helped me in all my work to complete this work successfully.

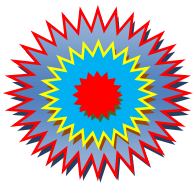
Finally and most importantly I would like to thank my wife and daughters for supporting, encouraging and cheering me up and stood with me throughout the good and bad times.

Dr. R. Nandakumar

Table of Contents

Preface	**IV - VI**
Acknowledgements	**VII**
Table of Contents	**VIII**

CHAPTER	**Page No.**
CHAPTER - 1	1 - 10
INTRODUCTION	
CHAPTER - 2	11 – 21
LITERATURE SURVEY	
CHAPTER - 3	22 – 34
A NOVEL SERVICE-LEVEL SECURITY-AWARE PACKET SCHEDULING IN MOBILE AD-HOC NETWORK	
CHAPTER - 4	35 – 44
INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (IIMLSDSPS)	
CHAPTER - 5	45 – 57
ANONYMITY-BASED INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (AIIMLSDSPS)	
CHAPTER - 6	58 – 69
ANONYMITY-BASED FLEXIBLE ROUTING PROTOCOL WITH INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (AFIIMLSDSPS)	
CHAPTER - 7	70 – 77
RESULTS AND DISCUSSION	
REFERENCES	78 - 84



CHAPTER - 1

INTRODUCTION

INTRODUCTION

This chapter introduced about the wireless networks, Mobile Ad-hoc Networks (MANET) and packet scheduling algorithms. In addition, the general motivation of the research, objectives and contributions of the research towards improving the secure-aware packet scheduling algorithm in mobile ad-hoc networks are also presented.

1.1 WIRELESS NETWORKS

The wireless networks are the kind of computer network which utilizes the wireless data connections in order to connect the network nodes. The wireless networking is a technique which is used for avoiding the expensive process of deploying the cables into the constructions or a connection between different equipment locations. The wireless networking is utilized in different applications (Nasir, H. J. A., & Ku-Mahamud, K. R. 2016). These networks are implemented and managed by using the radio communication. The implementation of the wireless network is initiated at the physical layer of the Open Systems Interconnection (OSI) network model. The examples of wireless networks are such as mobile phones, satellite communications, terrestrial microwave networks, and etc.

1.2 TYPES OF WIRELESS NETWORKS

There are several types of wireless networks are considered such as follows:

- Wireless Personal Area Network (WPAN)
- Wireless Local Area Network (WLAN)
- Wireless Ad-hoc Network (MANET)
- Wireless Metropolitan Area Network (WMAN)
- Wireless Wide Area Network (WWAN)
- Global Area Network (GAN)
- Space Network

1.3 MERITS OF WIRELESS NETWORKS

The different merits of wireless networks are including:

- Convenience
- Mobility
- Productivity
- Simple setup
- Easily expandable
- Security
- Cost

1.4 MOBILE AD-HOC NETWORK

Mobile Ad-hoc Network (MANET) is one of the kinds of wireless ad-hoc networks and defined as the continuously self-configuring and infrastructure-less network of mobile nodes which are connected wirelessly (Hoebeke, J., et al. 2004). In MANET, each node travels independently in any direction and regularly adjusts the connections to other nodes. Every node should transmit the traffic through the router. These networks are having multiple numbers of transceivers between the nodes. Therefore there is highly dynamic and autonomous topology is achieved.

Generally, MANET has the routable networking environment on top of the link layer ad-hoc network. It consists of the peer-to-peer network, self-forming network and self-healing network. Typically, these networking are communicating at the radio frequencies such that the range between 30MHz to 5GHz. These networks are utilized for facilitating the collection of sensor data for data mining in different applications such as environmental monitoring and etc. (Cheng, X., et al. 2013).

1.5 CHARACTERISTICS OF MANET

The different characteristics of MANET (Aarti, D. S., & Tyagi, S. S. 2013) are given below:

- Distributed functionalities: There is no background network for the central control of the network functions. The control of the network is distributed among the nodes. The nodes associated in the MANET must cooperate with each other and communicate among themselves and each node acts as the relay for implementing the particular functionalities like routing and security.
- Multi-hop routing: The packet must be transmitted by using one or more intermediate nodes while the node tries to send the information to other nodes which are located at outside of its communication range.
- Autonomous terminal: In MANET, each mobile node is an independent node which can act as both host and router.
- Dynamic topology: Nodes are free to travel arbitrarily at various speeds. Therefore, the network topology is changed randomly at unpredictable time. The node in the MANET are dynamically establishing the routing among them as they move around and establishing their own network.
- Light-weight terminals: In many cases, the nodes in MANET are mobile with less CPU capacity, low power storage and small memory size.
- Shared physical medium: The wireless communication medium is accessible to any entity with the suitable equipment and adequate resources. As a result, access to the channel cannot be restricted.

1.6 MERITS OF MANET

The merits of mobile ad-hoc networks (Kumar, M., & Mishra, R. 2012) are including:

- They are used to provide the access to information and services despite the consequences of geographic location.
- Independence from the central network administration. Self-configuring network where the nodes are act as routers.
- Less expensive compared to the wired network.
- Scalability (Chitkara, M., & Ahmad, M. W. 2014).
- Improved flexibility.
- Robust due to the decentralized administration.
- Easily implemented at any place and time.

1.7 CHALLENGES IN MANET

The challenges in mobile ad-hoc environments (Bang, A. O., & Ramteke, P. L. 2013) are including:

- Limited bandwidth: Wireless link continue to have significantly lesser capacity than infrastructure networks. Also, the realized throughput of wireless communication after accounting for the effect of multiple accesses, fading, noise, and interference conditions, etc., is lesser than the radio's maximum transmission rate frequently (Goyal, P., et al. 2011).
- Dynamic topology: The dynamic topology can disturb the trust relationship among nodes. The trust can also be disturbed if some nodes are detected as compromised (Raja, M. L., & Baboo, C. D. S. S. 2014).
- Routing overhead: In wireless ad-hoc networks, nodes often change their position within the network. Hence, some stable routes are generated in the routing table which provides unnecessary routing overhead.

- Hidden terminal problem: The hidden terminal problem is defined as the collision of the packets at the receiving node due to the simultaneous transmission of those nodes which are not within the direct transmission range of the sender, but within the transmission range of the receiver.
- Packet losses due to the transmission errors: The mobile ad-hoc networks are experienced with the highest packet loss due to the factors like increased collisions caused by the presence of hidden terminals, presence of interference, uni-directional connections, frequent route breaks due to the mobility of nodes.
- Mobility-induced path changes: The network topology in a mobile ad-hoc network is highly dynamic due to the mobility of nodes. Therefore, an on-going session suffers frequent route breaks due to the frequent route changes.
- Battery constraints: Devices utilized in MANET are having the restrictions on the power source for maintaining the portability, size and weight of the device.
- Security threats: The wireless mobile ad-hoc nature of MANET provides new security challenges to the network design (Orozco, A. L. S., et al. 2012). As the wireless medium is vulnerable to eavesdropping (Kumar, S., & Dutta, K. 2014) and ad-hoc network functionality is established through node cooperation, mobile ad-hoc networks are intrinsically exposed to several security attacks (Stieglitz, S., & Fuchß, C. 2011).

1.8 APPLICATIONS OF MANET

There are many applications of MANET (Raza, N., et al. 2016) are provided such as follows:

- Personal area network and Bluetooth: A personal area network is referred as a short range and localized network where the nodes are normally connected with the known person. Short range MANET like Bluetooth is utilized for simplifying the inter communication between different mobile devices like mobile phones and laptops.
- Military environments: Mobile ad-hoc networking is used to allow the military for providing the merits of commonplace network technology in order to maintain the information network between soldiers, vehicles and military information head quarters (Gupta, P. 2016).
- Collaborative work: For few business environments, the collaborative computing is required for cooperating and exchanging the information on the given project.
- Civilian environments: Mobile ad-hoc networks may anonymously connect an instant and temporary multimedia network by using notebook computers for spreading and sharing the information among participants at conference or classroom.
- Emergency operations: Mobile ad-hoc networks are also used in search-and-rescue operations for disaster relief efforts like in fire, flood or earthquake. Emergency rescue operations must take place where non-existing or damages communication infrastructures and rapid deployment of the communication network are required.

1.9 SECURITY SOLUTIONS IN MANET

The security schemes which are used for protecting the mobile ad-hoc networks from malicious behaviours are given below:

Security Criteria

The most utilized criteria (Rana, A., & Gupta, P. 2013) for evaluating the security of the mobile ad-hoc networks are including:

- **Availability:** The availability is referred as the node must maintain its ability for providing the all designed services regardless of the security state of it. This criterion is challenged mainly during the Denial-of-Service (DoS) attacks, where all nodes in the network may be the attack target. Hence, few selfish nodes make some of the network services unavailable like routing protocol or key management service (Sarika, S., et al. 2016).

- **Integrity:** The integrity is used for ensuring the identity of the messages when they are forwarded. It can be compromised in two ways such as malicious altering and accidental altering. A message may be eliminated, replayed or revised by an adversary including with the malicious target which is observed as malicious altering. If the message is lost or its content is varied due to few benign failures which may be transmission errors in communication or hardware errors as hard disk failure then it is classified as accidental altering.
- **Confidentiality:** The confidentiality defines that the particular information is only accessible to those who have been authorized for accessing it.
- **Authenticity:** The authenticity is essential for assuring that the participants in communication are genuine and not impostors. It is essential for communication participants for proving their identities as what they have claimed by using few techniques therefore as for ensuring the authenticity. If there is not such an authentication mechanism, the adversary can impersonate a benign node and so get access to confidential resources or propagate some fake messages for disturbing the normal network functions.
- **Nonrepudiation:** The nonrepudiation is used for ensuring the sender and the receiver of the message cannot disavow that they have ever transmitted or received such a message. If the node identifies that the message it has received is erroneous then it can utilize the incorrect message as an evidence for notifying the other nodes that the node transmitting the improper message should be compromised.
- **Authorization:** Authorization is defined as the process where the entity is issued a credential which specifies the privileges and permissions it has and cannot be falsified by the certificate authority. Normally authorization is utilized for assigning the different access rights to different level of users. Hence, the authorization process is required before the network administrator accesses the network management functions.
- **Anonymity:** Anonymity refers that the all information which is utilized for identifying the owner or the current user of the node must default be kept private and not be shared by the node itself or the system software. This criterion is relatively connected to the privacy preserving for protecting the privacy of the nodes from arbitrary disclosure to any other entities.

1.10 ATTACKS AGAINST ROUTING

One of the most significant services in the network is routing that is also one of the major target for attackers to conduct their malicious behaviours (Kumar, M. R., et al. 2013). In mobile ad-hoc networks, generally the attacks against routing are categorized as two types such as attacks on routing protocols and attacks on packet forwarding or delivery. Attacks on routing protocols are having the target that to block the propagation of the routing information to the victim even if there is few paths from the victim to other destinations. Attacks on packet forwarding or delivery are trying to interrupt the packet delivery along the fixed path. There are some attacks against routing such as follows:

- Impersonating the other node to spoof route message.
- Advertising the false route metric to misrepresent the topology.
- Transmitting the route message with wrong sequence number for suppressing the other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack.
- Modifying the Route Reply message for inserting the false route.
- Generating bogus Route Error for disrupting the working route.
- Suppressing the Route Error to mislead others.

The validation of the all route messages is very difficult since the mobility and frequently modifying topology of the mobile ad-hoc networks (Reddy, P. N., et al. 2013). The attacks on packet delivery or

forwarding are not easy to detect and prevented. The attack strategies are mainly classified into two types. One type is selfishness where the malicious node selectively drops route message which are assumed for forwarding in order to save its battery power. The other type is Denial-of Service (DoS), where the adversary transmits overwhelming network traffic to the victim for exhausting its battery power (Gupta, A., & Ranga, S. P. 2012).

1.11 SCHEDULING ALGORITHMS

In MANET, different functionalities of nodes such as routers, terminals, and multi-hop which are used for forwarding the packets, and mobility induced frequent transmission of route packets may generate the unique queue dynamics. The selection of scheduling algorithms are provided for determining which queued packet to process further will have the significant effect on the total end-to-end performance while the traffic load is high. Different scheduling algorithms are developed for MANET in which simple priority scheduling algorithm has mostly utilized where the data packets are scheduled in First-In-First-Out (FIFO) manner and all routing packets (RREQ, RREP, and RERR) are given priority over data packets for transmission at the network interface queue (Arpaci-Dusseau, R. H., Arpaci-Dusseau, A. C. 2015).

There are different scheduling policies are provided for different network scenarios. Different methods of scheduling are utilized by the different routing protocols. The drop-tail policy is used as the queue management algorithm in all scheduling algorithms to manage the buffer. For scheduling algorithms which gives high priority to control packets, different drop policies are used for data and control packets while the buffer is full. Nowadays, priority scheduling algorithms are mostly used in mobile ad-hoc networks.

Different scheduling algorithms are developed by using distance metrics, fairness, and applying the multiple roles of nodes as both routers and data sources. The scheduling algorithm which provides higher weight to data packets including with smaller number of hops or shorter geographic distances to their destinations are reduces the average delay and improves the average throughput. Network traffic is classified into two types such as control packets and data packets. The scheduling is classified as packet scheduling and channel access scheduling. The packet scheduling algorithm is used for deciding the order in which the packets waiting for transmission at any node should be dispatched whereas the channel access scheduling is used for deciding how different nodes share the channel in the contention region (Garg, K., & Singh, R. 2012).

1.12 PACKET SCHEDULING ALGORITHM

Packet scheduling is defined as the process of data packet transmission and a key function of quality of service. The packet scheduling is also referred as the decision process which is utilized for selecting which packets should be dropped or serviced. In addition, the process of assigning user's packets to appropriate shared resource for achieving some performance guarantee is called as packet scheduling (Jandaeng, C., et al. 2011).

Packet scheduling is anticipated that packetized transmissions over connections through proper packet scheduling algorithms can provide higher resource utilization via statistical multiplexing of packets which is compared to the conventional circuit-based communications. The appropriate packet-level scheduling algorithms are designed for scheduling the order of packet transmission by considering the different QoS requirements of individual users or other criteria like fairness may alter the service performance and improve the system capacity. The major objective of packet scheduling algorithms is maximizing the system capacity when satisfying the QoS of users and achieving the particular level of fairness (Tsai, T. Y., et al. 2010).

1.13 SIGNIFICANCE OF PACKET SCHEDULING ALGORITHM

Nowadays, the packet scheduling algorithms are proposed for achieving the following properties:

- Efficiency: The fundamental operation of packet scheduling algorithm is scheduling the transmission order of packets queued in the system according to the available distributed resource which satisfies the set of QoS requirements of each user. If larger capacity region is provided by

the packet scheduling algorithm then it is more effective than other algorithms. Hence, it can achieve the same QoS guarantee under a heavy traffic load or more number of served users.

- Protection: The another property of packet scheduling algorithm is treating the flows like providing an individual virtual channels such that the traffic characteristics of one flow can have small effect to the service quality of other flows as possible. This property is referred as flow isolation in other scheduling contexts. Flow isolation may facilitate the system for providing flow-by-flow QoS guarantees which are independent of the traffic demand of the other flows. The most flexible performance guarantee service method is also allowed by logically separating the users which are connected to the wide range of QoS requirements and traffic characteristic when providing the protection from affecting each other.
- Flexibility: The packet scheduling algorithm has the ability for supporting the users with widely different QoS requirements. Nowadays, by providing applications with enormous diversity of traffic characteristics and performance requirements is the typical case in most practical integrated system.
- Low complexity: The packet scheduling algorithm is having the reasonable computational complexity to be implemented. Nowadays, the processing speed of packets is more and more critical due to the fast growing of bandwidth and transmission rate in communication system. Therefore, the complexity of the packet scheduling algorithm is also the important characteristic.

1.14 DIFFERENT PACKET SCHEDULING ALGORITHMS

There are different packet scheduling algorithms are presented for both wire and wireless network systems (Borve, B. H. 2008). These are described in below:

1.14.1 No-Priority Scheduling

The simplest packet scheduling algorithm is No-priority scheduling or First Come First Serve (FCFS) for the scheduler in order to schedule the packets. FCFS does not consider the QoS parameters of each packet, but it transmits the packets based on the order of their arrival time. Hence, the QoS guarantee provided by FCFS is generally not effective and highly depends on the traffic characteristics of flows. For instance, if there are some flows which are having very bursty traffic under FCFS then the packet will very likely be blocked for the long time by packets burst which arrives before it. In worst case, the unfairness between different flows does not bind and the QoS does not provide longer guaranteed. Though, FCFS has many advantage of easy to implement and adopted in many communication networks especially the networks providing best effort services. If few levels of QoS are required then, more sophisticated scheduling algorithm is required.

1.14.2 Priority Scheduling

The priority scheduling is utilized for providing high priority to control packets. In the priority scheduling, control and data packets are maintained in the separate queues in FIFO order and high priority is assigned to control packets. In MANET, the priority scheduling algorithm is mostly utilized.

1.14.3 Round Robin

The drawbacks of FCFS are compensated by the Round Robin (RR) method which is also having low computational complexity. The newly arrival packets are queued up by flow in which each flow has its corresponding queue. The scheduler polls each flow queue in the cyclic order and serves the packet from any empty buffer encountered. Hence, the RR method is also known as flow-based RR method. RR scheduling is one of the simplest and widely utilized scheduling algorithms which are designed especially for time-sharing systems. They are used for providing higher fairness and better bandwidth utilization. Though, the lack of flexibility is provided by RR which is an attempt for treating all flows identically (Raj, A., & Prince, P. B. 2013).

1.14.4 Greedy Scheduling

In greedy scheduling algorithm, each node transmits its own data packets before transmitting those of other nodes. The other node’s data packets are serviced in FIFO order.

1.14.5 Strict Priority

Another classical service discipline is the strict priority which assigns the classes to each flow. Different classes can be associated with the different QoS level and having different priority. The eligible packets connected to the flow with higher-priority classes are transmitted earlier than the eligible packets which are associated to the flow along with lower-priority classes. The transmitting order of packets using strict priority is depending upon the classes of the packets. They are called strict because the eligible packets with lower-priority classes are not allowed for transmit before the eligible packets with higher-priority classes. This scheme also having the demerits of FCFS since the packet may also wait arbitrarily long time for its transmission. Specifically, the packets with lower-priority classes are starved by the packets with higher-priority classes.

1.14.6 Earliest Deadline First (EDF)

One of the most well-known scheduling algorithms for real-time network services like multimedia applications is Earliest Deadline First (EDF). The EDF is used for scheduling the packets in greedy manner where the packets with the nearest deadline are always selected. It provides time-dependent priority for each eligible packet compared to the strict priority scheme. Generally, the priority of an eligible packet under EDF is an improving function of time since the transmitting order in EDF is based on the closeness of packet's deadlines. Hence, it allows the guarantee of QoS if the traffic characteristic of each flow follows the particular constraint.

1.14.7 Idealized Wireless Fair Queuing (IWFQ) Algorithm

The Idealized Wireless Fair Queuing (IWFQ) algorithm is one of the earliest packet scheduling algorithms for wireless access networks for handling the characteristic of location-dependent burst error in wireless links. The IWFQ takes an error-free Wireless Fair Queuing (WFQ) service system as its reference system where the channel predictor is involved in the system for monitoring the wireless connection status of each flow and determining the connections which are in wither good or bad states. The difference between IFWQ and WFQ is that while the picked packet is predicted in the bad connection state then it will not transmitted and the packet with the next smallest virtual finish time will be picked. The process is repeated until the scheduler finds the packet with the good state.

The flow is called as lagging, leading or in sync while the size of the queue is smaller than or larger than or equal to the size of queue in the reference system. When the lagging flow recovered from the bad link state, it should have the packets along with smaller virtual termination periods compared with the other error-free flows packets. Hence, it will have the precedence to be picked for transmission. Therefore, the compensation is guaranteed. However, the delay or jitter requirements based on IWFQ are not considered in real time applications.

1.14.8 Channel-condition Independent packet Fair Queuing (CIF-Q) Algorithm

The Channel-condition Independent packet Fair Queuing (CIF-Q) algorithm is also using an error free fair queuing algorithm as a reference system. The main difference between CIF-Q and IWFQ is that in CIF-Q the leading flows are facilitated for progressing to receive the service at an average rate and also the compensation is distributed among the lagging flows in proportion to their allocated service rates which are instead of selecting the packet along with the smallest virtual service tag in IWFQ. This algorithm has better scheduling fairness and also has better properties of guaranteeing delay and throughput for error-free flows such as IWFQ. But, the requirement of decoupling of delay from the bandwidth is still not achieved by CIF-Q.

1.14.9 Improved Channel State Dependent Packet Scheduling (I-CSDPS) Algorithm

The modified version of Deficit Round Robin (DRR) scheduler is deploying in wireless scheduling algorithm which is called as Improved Channel State Dependent Packet Scheduling (I-CSDPS). In DRR, each flow has its own queue and the queues are served in the round robin manner. Two parameters such as Deficit Counter (DC) and Quantum Size (QS) are maintained by each queue. The Deficit Counter (DC) is defined as the total credit in bits or bytes that the flow has for transmitting the packets. The Quantum Size (QS) is used for determining how much credit is given to the flow in each round. At starting of each round, the credit of size QS is included to the DC for each flow. I-CSDPS includes the Compensation Counter (CC) for each flow in order to permit flows for receiving the

compensation for their lost service due to the link errors. The CC is utilized for keeping track of the amount of lost service for each flow. If the scheduler reschedules the transmission of a packet since link errors, the corresponding DC is reduced by the QS of the flow and the CC is improved by the QS.

1.14.10 Load-based Queue Scheduling

In load-based queue scheduling algorithm, nodes are considered their own load states during transmission. Priorities to packets are assigned based on the load level of the current node. When load is less, node helps the other nodes for constructing the route and when load is high, they must function normally for avoiding the network transmission delay and packet loss. Queue length is utilized as the load indicator and three load levels are defined by two thresholds such as maximum and minimum threshold. The first level is light load that the queue length is less than the minimum threshold. The second level is medium load that the queue length is between minimum and maximum threshold. The last level is heavy load that the queue length is greater than the maximum threshold. The scheduling is classified into two processes such as scheduling policy and dropping policy. The scheduling policy is used to decide the order where the packets waiting for transmission at any node should be dispatched. The dropping policy is used to decide how different nodes sharing the channel which may utilize the resources.

1.14.11 Cluster-based Multi-Channel Scheduling

Cluster communications are classified into intra-cluster and inter-cluster communications in two-level hierarchical clustering topology. The quality-of-service (QoS) and high throughput is guaranteed by TDMA which is adapted for cluster communications by allocating the predetermined time slot per packet to each node over multiple channels. In the intra-cluster communication, packet transmission of each cluster member is processed within its cluster. Each cluster member has the packet to the random destination. If its packet destination is located within the similar cluster then it transmits the packet directly to the destination through direct link. Otherwise, it transmits the packet to its own cluster head for saving the battery energy which refers uplink. Similarly, in inter-cluster communication, each cluster head broadcasts the packets received from its members to their destination over the specific channels of their destination similar to the broadcast scheduling. The aim of cluster-based multi-channel scheduling algorithms is maximizing the end-to-end throughput by optimizing the number of total TDMA slots in the cluster communication.

1.14.12 Channel Aware Packet Scheduling

The channel aware packet scheduling algorithm in MANET is developed by considering both congestion state and end-to-end path duration (Chen, X., et al. 2011). During path setup, the path lifetimes are estimated and collected and also stored. This path lifetime value is utilized as the parameter for representing the end-to-end channel condition. During packet scheduling, this algorithm is used for selecting the packets which has high probability of reaching the destination and takes the cost of the link failure by providing the priority to flows which have longer normalized along with the path residual lifetime backlog queue (Sridhar, K. N., & Chan, M. C. 2008).

1.15 MOTIVATION OF THE THESIS

Nowadays, several security and routing challenges and issues are arising in mobile ad-hoc networks. These challenges are due to link failure, packet loss, and etc. In addition, the lack of confidentiality, integrity and threat of malicious attacks are also associated with wireless communications. Therefore, such challenges and issues are eliminated by enhancing the security-aware packet scheduling algorithm in mobile ad-hoc networks based on anonymity and routing protocol. By utilizing the anonymity and flexible routing with security-aware packet scheduling algorithm, the packet transmission in mobile ad-hoc networks are improved in terms of improved security, reduced end-to-end delay and packet loss and so on efficiently.

1.16 PROBLEM DEFINITION

The research is mainly concerned on the improvement of security-aware packet scheduling algorithm for mobile ad-hoc networks. However, the problems which are associated with the previous algorithms are listed as follows:

- The packets were considered to be independent with each other in Improved Security-Aware Packet Scheduling (ISAPS) algorithm (Zhu, A., et al. 2012).
- The computational complexity was increased due to the correlation of multiple layer dependencies and accuracy was reduced due to the scalability.
- The efficiency of security aware packet scheduling was less since the attacker easily identifying the source-sink nodes.
- The energy consumption was high for ensuring the security while the fake paths and fake messages were increased.

1.17 OBJECTIVES OF THE RESEARCH

The objectives of our research are programmed as follows:

- To consider the packets with dependent relations in Improved Security-Aware Packet Scheduling (ISAPS) algorithm.
- To improve the correlation of multiple layer dependencies for reducing the computational complexity and increasing the accuracy.
- To enhance the efficiency of security aware packet scheduling algorithm by including anonymity scheme.
- To reduce the energy consumption based on the flexible routing protocol.

1.18 CONTRIBUTIONS OF THE RESEARCH

The major contributions of the research are given below:

- The dependencies of packets are considered and identified by using Dependence Graph (DG) based on the Intra-Service Dependent Security-aware Packet Scheduling (ISDSPS) and Intra and Inter-Service Dependent Security-aware Packet Scheduling (IISDSPS) algorithms.
- The correlation of the multiple layer dependencies of packets are collected and improved by the Service Layer Dependence Graph (SLDG) based on the directed acyclic graph method.
- The anonymity of the system is improved by analysing the traffic characteristics by using fake source-location method which introduces the number of fake paths in the network.
- The energy consumption due to routing is reduced by monitoring the flooding process based on the flexible routing protocol called Phantom routing protocol.

1.19 ORGANIZATIONS OF THE THESIS

The remainder of this work is structured as follows:

Chapter 2: Presents the previous research of this thesis in the area of the packet scheduling algorithms in wireless networks.

Chapter 3: Describes the first contribution such as a novel service level security-aware packet scheduling in MANET.

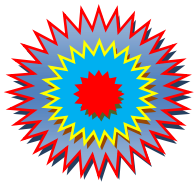
Chapter 4: Describes the second contribution such as Intra-Inter and multiple layer service dependent security-aware packet scheduling algorithm.

Chapter 5: Presents the third contribution such as anonymity-based Intra-Inter and multiple layer service dependent security-aware packet scheduling algorithm.

Chapter 6: Presents the fourth contribution anonymity-based flexible routing protocol with Intra-Inter and multiple layer service dependent security-aware packet scheduling algorithm.

Chapter 7: Includes the overall Results and Discussions of the research work.

Chapter 8: Concludes our research and provides the scope of future enhancement.



CHAPTER - 2

LITERATURE SURVEY

LITERATURE SURVEY

This chapter provides the detailed about the previous researches which are associated with the packet scheduling techniques and anonymity schemes for security of the packets in mobile ad-hoc networks, real-time wireless networks and etc. Different packet scheduling algorithms and techniques which are related to our research are discussed in detail.

2.1 EXISTING TECHNIQUES

Real-time scheduling with security enhancement (Saleh, M., & Dong, L. 2013) was proposed for packet switched networks. An adaptive security-aware scheduling system was proposed for packet switched networks by using the real-time multi-agent design framework. In the proposed method, the real-time scheduling algorithm was combined with the security service enhancement. The Differentiated-Earliest-Deadline-First (Diff-EDF) scheduler was utilized by the scheduling unit and the congestion control technique was adopted by the security enhancement method. The required QoS was guaranteed for different types of real-time data transmissions while the packet security levels were adaptively enhanced based on the feedbacks from the congestion control unit. However, the average end-to-end delay was high.

Online energy efficient packet scheduling (Deshmukh, A., & Vaze, R. 2016) was proposed for the common deadline with or without energy harvesting. In this paper, the issues in online packet scheduling were considered for minimizing the required grid energy to transmit the fixed amount of packets given a common deadline. The proposed algorithm was utilized for terminating the transmission of each packet where all future packets are assumed as going to arrive at equivalent time periods within the left-over time. In addition, the hybrid energy paradigm was considered in which energy was obtained by extraction from the renewable sources. However, the complexity was high.

Adaptive flow assignment and packet scheduling (Wu, J., et al. 2015) were developed for delay-constrained traffic over heterogenous wireless networks. The Flow-Assignment and Packet Scheduling (FA-PS) was proposed for multi-homed communication of delay constrained traffic over heterogeneous wireless networks. Moreover, an Adaptive Flow Assignment and Packet Scheduling (AFAPS) scheme was provided for reducing the end-to-end delay and burst packet losses. Initially, a horizontal water filling algorithm was introduced for integrating the channel resources in heterogeneous wireless networks for maximizing the aggregate goodput. Then, an alternative path interleaving method was provided for spreading out the packet's departures over multiple communication paths within the delay constraint for mitigating the burst losses. However, the complexity of the method was high.

Energy-efficient opportunistic packet scheduling (Zhang, Z., et al. 2015) was proposed for mobile relay systems. The fundamental scheduling issues in three-node mobile relay systems were studied. The major objective of this paper was to completely exploit the communication opportunities brought by relay mobility for minimizing the energy consumption under the data throughput constraint. Initially, a 2D-FSMC channel model was applied for reflecting both large and small scale channel fading in the mobile networks. After that, the scheduling issue was formulated as a constrained Markov Decision Process (MDP) and resolved by Lagrange relaxation approach. According to this, a probabilistic algorithm named Opportunistic Packet Scheduling (OPS) for reducing the energy consumption. However, the computational complexity of the proposed method was high.

An enhanced dynamic priority packet scheduling algorithm (Yantong, W., & Sheng, Z. 2016) was proposed for wireless sensor networks. In the proposed algorithm, three types of priority ready queues in every sensor node were considered. Higher priority queue was used for storing the real-time communication packages whereas the middle priority queue was utilized for storing the non-real time data packets for transmitting to the other nodes. Lower priority queue was used for storing the non real-time packages whose destination is local node. The scheduling sequence in higher priority was according to the priority of packets. However, the time complexity and time delay of the proposed method were high.

Anonymity and fairness in packet scheduling (Mishra, A., & Venkitasubramaniam, P. 2016) was proposed in networks. In this paper, the relationship between fairness and anonymity was studied for three fair scheduling techniques such as First-Come-First-Serve (FCFS), Fair Queuing (FQ) and Proportional Method. The degree of out-of-order transmissions was measured by the common temporal fairness index and information-theoretic metric. The anonymity under these scheduling techniques was characterized and their anonymity-fairness tradeoffs were compared. However, the optimization problem was occurred for tradeoff between anonymity and fairness of the network.

Energy-efficient and delay-aware packet scheduling (Yu, Q., et al. 2015) were proposed for high-speed networks. In this paper, a congestion and energy-aware packet scheduling method was proposed for achieving the balance between network delay and energy consumption. The proposed method was known as Queue Length based Delay-Aware packet scheduler (QLDA) which utilizes the multiple queue length thresholds for perfectly capturing the network congestion. The proposed QLDA was utilized for effectively designed frequency adjustment strategies for controlling execution rates in line cards and achieving the high energy savings with not including the delay requirements of the underlying applications. However, the complexity of the method was high.

Packet scheduling and access priority control (Kongsili, L., et al. 2015) were proposed for QoS and fairness in wireless LAN. In this paper, QoS, fairness and downlink or uplink traffic asymmetry were achieved by the proposed method which combines the operation of channel access priority control and packet scheduling including with require modifications. The Fair QoS Agent (FQA) was mainly focussed which considered the information about QoS and fairness and Adaptively Priority Controller (APC) for solving the issue of traffic asymmetry as a packet scheduling and access priority control mechanism correspondingly. However, the proposed method was not used for obtaining better throughput.

An online packet scheduling algorithm (Li, F. 2013) was investigated. In this paper, the bounded-delay model was studied for Quality-of-Service (QoS) buffer management. The main aim of this paper is to increase the total value of the transmitted packets by their corresponding deadlines in an online. The performance of an online algorithm was computed by using competitive ratio, while the online algorithm was compared to the clairvoyant algorithm in order to achieve the maximum total value.

Packet scheduling with playout adaptation (Hung, T. Y., et al. 2011) was proposed for scalable video delivery over wireless networks. In this paper, a novel playout adaptation algorithm was proposed for reducing the playback interruptions through jointly considering the active playout buffer status and adaptive playout rate. In addition, a packet priority analysis technique was proposed according to the layer information of Scalable Video Coding (SVC). Then, an optimal packet scheduling algorithm was proposed according to the priority of the video packet and the adaptive playout-deadline. Furthermore, a benchmark was also adopted for the packet priority analysis by computing the distortion impact of each packet including with the consideration of the packet dependency in SVC. However, this method was utilized for video packets transmission.

Packet transmission scheduling algorithm (Sharifkhani, A., & Beaulieu, N. C. 2009) was proposed for dense wireless sensor networks with mobile sink. In this paper, the proposed algorithm and the reduced complexity algorithm were performed according to the well known tradeoff between the energy consumption and the probability of successful packet arrival at the sink, while the sensor nodes were required for sharing the single transmission channel at every time slot. While the algorithm was utilized for transmission scheduling, it has more advantages in terms of power consumption and successful packet transmission rate for networks including with higher node densities. In addition, the effect of the cost of transmission power at the sink node was investigated for various node densities. However, the complexity of the algorithm was high.

Selfish aware queue scheduler (Lakshmi, S., & Radha, S. 2012) was proposed for packet scheduling in mobile ad-hoc networks. In this paper, the Selfish Scheduler Queue Methodology (SSQM) was proposed as an optimal solution for ad-hoc networks. The proposed methodology was utilized for managing the queues by which the packets were transmitted from the source to the destination through

the selfish or malicious nodes. The performance of the proposed algorithm was analyzed for different number of mobile nodes in the network. However, the energy consumption was not considered for each node in the ad-hoc networks.

An efficient priority packet scheduling algorithm (Karim, L., et al. 2012) was proposed in wireless sensor networks for reducing the processing overhead and transmission delay. The three-class priority packet scheduling method was proposed. The emergency real-time packets were positioned in the highest priority queue. The packets other than emergency were prioritized according to the location of the sensor nodes and positioned into the other queues. The lowest priority packets were preempted their processing in order to process the emergency-highest priority packets after waiting for the number of timeslots. However, the end-to-end delay was increased while the number of zones was increased.

Multilevel priority packet scheduling technique (Kumar, R. A., & Varshini, M. K. 2014) was developed for reducing the large processing overhead and energy consumption. The Dynamic Multilevel Queue Scheduling (DMQS) algorithm was proposed where the ready queue was separated into three levels of priority queues. The real-time packets were located in highest priority queue whereas the non-real time packets were located in another two queues. However, the performance effectiveness was less and dependent packets were not considered.

Real-time scheduling algorithm (Rewadkar, D. N. & Khot, S. 2014) was developed for security of packet switched network. In the proposed system, a GAIA technique was provided for analyzing and designing the multi-agent system. The GAIA method was utilized for combining the real-time scheduling function along with security service enhancement. The differentiated earliest deadline first scheduler was utilized by he scheduling and congestion control method was utilized by the security service enhancement. The high quality of security was required by the real-time systems for guaranteeing the data processing on the clusters which are not modified by means of the malicious users. However, the energy consumption was not considered for achieving the effective performance.

Optimal sinks deployment and packet scheduling method (Achir, N., & Muhlethaler, P. 2014) was proposed for wireless sensor networks. An optimal deployment and distributed packet scheduling of multi-sink were proposed for computing the optimal deployment of sinks for maximum number of hops between nodes and sinks. In addition, an optimal distribute packet scheduling algorithm was proposed for estimating the minimum energy consumption by determining the lower-bound of overhearing. But, the energy consumed by overhearing process was high for both small and large networks.

Real-time packet scheduling algorithm (Tiwari, G., & Mishra, D. 2016) was investigated on the WLAN including with security awareness. The issues in packet guarantee and security were analyzed. Different real-time packet scheduling algorithms were discussed. Each algorithm was provided for dynamically adjusting the guarantee ratio and improving the entire system performance. However, the dependency packets were not considered whereas all incoming packets were considered to be independent to each other.

Anonymous user communication (Wan, Z., et al. 2010) was developed for protecting the privacy in wireless metropolitan mesh networks. In this paper, two solutions were proposed for security and privacy protection in wireless mesh networks. The primary scheme relies on the group signatures combined with the user credentials for delivering the security and privacy protection. The user identity was disclosed to mesh networks by enforcing the access control based on the user credentials. This criterion was removed by the second proposed method which employs the pairwise secrets between any two users for achieving the robust privacy protection. The user was kept anonymous to mesh network in the second method. However, the packet delivery ration was decreased and packet delivery latency was increased during heavy traffic.

Packet scheduling and fairness (Torabzadeh, M., & Ajib, W. 2010) was proposed for multi-user MIMO systems. In this paper, a flexible packet transmission algorithm was provided at the Medium Access Control (MAC) layer for developing the novel scheduler which is referred as MIMO Packet

based Proportional Fairness (MP-PF). The new scheduler was provided for achieving high performance in terms of low average packet transmission delay and time and service fairness. BY using the proposed approach, the well known ideal service fair scheduler named max-min was improved by considering the traffic characteristics. However, the complexity of the proposed method was high.

Multi-path transmission control scheme (Tsai, M. F., et al. 2010) was proposed including with the bandwidth aggregation and packet scheduling for real-time streaming in multipath environment. In bandwidth aggregation method, a mathematical model was proposed for finding the transmission rate over each path in order to obtain the optimal average throughput. In addition, a packet scheduling scheme was proposed for arranging the transmission sequence to reduce the impact of packet reordering at the receiver effectively. The proposed method was utilized for both aggregation of bandwidth of multiple paths as well as reducing the time of packet reordering at the receiver. However, the peak-signal-to-noise ratio of the proposed method was high.

Optimized packet transmission scheduling method (Tajima, T., & Okabe, Y. 2016) for wireless local area networks. The packet transmission scheduling strategies were developed for enhancing the Web Quality-of-Experience (QoE). The proposed strategy was used for prioritizing the transmission of the top part of a web to another part in the page. The prioritization of the packet transmission was triggered by detecting the initial 3-way handshake at TCP connection establishment. The prioritization was achieved in controlling the transmission timing at mobile device and changing the Contention Window (CW) dynamically at access point in priority queuing.

Randomized gathering of mobile agents (Ooshita, F., et al. 2014) was proposed for anonymous unidirectional ring networks. In this paper, the problem of gathering multiple mobile agents in anonymous unidirectional ring networks was considered and the relationship between probabilistic solvability and termination detection were completely characterized. The relaxed gathering problem named gathering problem without detection was considered which does not require the termination detection. However, the optimization was required for the cost along with memory space and the total number of moves.

Multi-generation packet scheduling (Huang, S., et al. 2016) was proposed for live streaming with network coding. In this paper, an unrecoverable transmission was resolved by determining the scalable layer subscription and scheduling strategy. The proposed scalable layer subscription algorithm was treated as the video quality maximization problem in multiple generations. After that, the problem was solved based on the dynamic programming algorithm.

Jitter-aware packet scheduler (Chan, M. C., et al 2016) was proposed for concurrent multipath transmission in heterogeneous wireless networks. The performance of delay-aware packet scheduling was analyzed based on the jitter. Then, the Jitter-Aware Packet Scheduler called JAPS was proposed for improving the performance of the algorithm in terms of throughput under various data volume, receiver buffer size, network jitter, and bandwidth ratio. However, the bandwidth consumption and energy consumption were not considered.

The Packet Scheduling Algorithm (PSA) (Jandaeng, C., et al. 2011) in wireless sensor networks. In this paper, the PSA was proposed for reducing the packet congestion in MAC layer and reducing the overall packet collision in the system. The proposed algorithm was performed based on the greedy algorithm which is provided for easy implementation in resource constrained devices. The proposed PSA was compare to the simple CSMA/CA using network topology benchmarks in mathematical model. However, the average delay of the proposed PSA was high.

Distributed Anonymous Secure Routing (DASR) (Dang, L., et al. 2010) was proposed including with better scalability in mobile ad-hoc networks. The proposed protocol was utilized for addressing the issues of anonymous routing and anonymous data transmission through the dynamic identity pseudonymity method by using incomparable public keys. The Diffie-Hellman key exchange method and symmetric key cryptography were proposed for achieving better scalability. In the proposed

algorithm, no public key operations were performed for improving the performance. However, the effectiveness of the anonymous secure multicast routing protocol was less.

Trust-based Anonymous Communication Technique (TACT) (Gunasekaran, M., & Premalatha, K. 2012) was proposed for malicious user disclosure in mobile ad-hoc networks. The TACT as provided for restraining the misuse of anonymity so that any user cannot transmitting cooperation message utmost once, upon receiving the warnings two times was identified. Also, any user transmitting the multiple cooperation messages per warning per malicious behaviour type was identified as malicious user. The proposed TACT algorithm was provided based on the broadcast with trapdoor information which is the cryptography concept for monitoring the users and reporting the malicious users to the network anonymously. However, the energy consumption was not considered in the proposed TACT algorithm.

Anonymous on-demand Routing and Secure Checking of traffic forwarding (ARSC) (Jiang, R., & Xing, Y. 2012) was proposed in wireless ad-hoc networks. The proposed ARSC consists of anonymous routing according to the identity-based encryption pseudonym and single-round onion and secure checking of traffic forwarding in data transmission phase based on the hash chain for achieving the robust route anonymity and improving the reliability of packet delivery in the data transmission phase. In addition, the concept of onion routing was adopted by ARSC which is utilized in the RREP phase. However, the route establishing latency was high.

Trust-Enhanced Anonymous on-demand routing Protocol (TEAP) (Gunasekaran, M., & Premalatha, K. 2013) was proposed for mobile ad-hoc networks in order to restrain the misuse of anonymity in two methods. In the first method, the user was revealed as a misbehaving user to another user, if the user does not transmit the cooperative messages upon receiving the two warnings. In the second method, if the user attempts to transmit the multiple claims against the certain user for the same reason it will also named as the misbehaving user. The proposed TEAP was proposed based on the broadcast with trapdoor information for detecting the misbehaving users anonymously in the network. However, in this method, the energy consumption was not considered.

Hash-based Anonymous Secure Routing (HASR) protocol (Lo, N. W., et al. 2015) was proposed for mobile ad-hoc networks. In this paper, a novel secure routing protocol was proposed based on the collision-resistant one-way hash function and pseudo-name generation or exchange mechanism for supporting the identity anonymity, location anonymity and route anonymity and also defending against major security threats like replay attack, spoofing, route maintenance attack and denial of service (DoS) attack. However, the selection of an effective hash function was complex.

Location aware sector-based routing (Malwe, S. R., & Biswas, G. P. 2015) was proposed for wireless ad-hoc networks. In this paper, the request zone was determined for limited control packet flooding which is measured on the basis of previous destination location. The proposed protocol was implemented based on the network nodes with directional antenna along with 120 degree scope of each sector. According to the expected destination location, one of the three sectors was selected for route request transmission in the neighborhood. The proposed technique was developed for nodes with directional antennas for improving the efficiency of the routing and reducing the control overhead without affecting the path length between the peers. However, the security of the packet transmission was not considered.

Routing-based and location-aware service discovery (Schellenberg, S., et al. 2014) was proposed in mobile ad-hoc networks. In this paper, a location-aware service discovery method was proposed according to the routing-based name resolution mechanism which is combined in an adaptive routing method. Moreover, a proactive method was introduced based on the Optimized Link State Routing (OLSR) in an adaptive routing framework. In addition, the service discovery and service announcement were integrated into the reactive and proactive routing protocols. However, the security of packet transmission was not considered.

An anonymous secure routing protocol (Sheklabadi, E., & Berenjkoub, M. 2011) was proposed for wireless ad-hoc networks. In this paper, an anonymous version of ARAN was proposed for providing

the anonymity and preserving the security of nodes in mobile ad-hoc networks. The proposed protocol was designed based on the combination of the anonymous communication including with the security specifications of ARAN. The major objective of the proposed protocol was to integrate the different anonymous functionalities like identity privacy, location privacy and route anonymity combined with the security features of ARAN. However, the prevention of malicious nodes was not effectively performed.

Linear regression based energy aware location-aided routing protocol (Singh, K., et al. 2015) was proposed for mobile ad-hoc networks. The proposed node dependent energy efficient location aided routing protocol was performed based on the linear regression and curve intersection point area for reducing the requested zone and node categorization on the basis of the battery power. The major objective of the proposed method was improving the energy utilization in the network. However, the average energy consumption was high.

Packet scheduling algorithms (Kathrine, J. W., & Raj, A. 2012) were investigated in different wireless networks. In this paper, different packet scheduling algorithms were studied in different wireless networks. Every wireless network has the different packet scheduling strategy and their merits and demerits. Most of the packet scheduling algorithms was not utilized for providing the security. By using this survey, the packet scheduling algorithms were discussed for providing the security in terms of giving priority to schedulability.

Sampling traffic analysis of anonymous communications (Wang, Z. J., et al. 2013) was proposed for mobile ad-hoc networks. In this paper, a novel traffic analysis method of Mix anonymous communication networks was proposed. Initially, a statistical model was proposed for anonymous communications. The traffic analysis problem was transformed into the sampling problem by employing the principle of Bayesian inference. The analysis of sampling problem was achieved by the Metropolis-Hastings algorithm. However, the complexity of the method was high.

Survey of packet scheduling algorithms (Annadurai, C. 2011) was provided for mobile ad-hoc networks. In this paper, different scheduling algorithms were studied which are utilized in wireless ad-hoc networks. The design of the scheduling algorithms was described for mobile ad-hoc networks for removing high link error rates and dynamic nature of the network. Different required features and classifications of the schedulers were discussed for various scheduling algorithms.

Real-time packet scheduling algorithm (Chennakesavula, P., et al. 2013) was proposed for real-time wireless sensor networks. In this paper, an Effective Real-Time packet Scheduling (ERTS) method was proposed which is used for real-time data communication. The ERTS was proposed based on the Just-in Time Scheduling (JiTS) algorithm along with the shortest path routing protocol. The shortest path routing algorithm was utilized for selecting the shortest path among all paths in the network. Moreover, the proposed scheduler may be sandwiched between routing and MAC layer or within the routing layer of the protocol stack. However, the traffic conditions were not considered.

An efficient data packet scheduling schemes (Gomathi, R., & Mahendran, N. 2015) were proposed in wireless sensor networks. In this paper, different packet scheduling algorithms were discussed for real-time data communication for achieving the predictable and bounded end-to-end delay when the deadlines of queries were assembled. Different packet scheduling algorithms were such as First-Come-First-Serve Scheduling (FCFS), Dynamic Conflict Free Transmission Scheduling (DCQS), Dynamic Multilevel Priority Packet Scheduling (DMPPS), Traffic Pattern Oblivious Scheduling (TPO), Real-Time Query Scheduling (RTQS), Earliest-Deadline-First (EDF), and Nearest Job Next (NJN). The performance of these algorithms was evaluated based on the scenarios like offline and online data collection method.

Dynamic multilevel priority packet scheduling design (Jain, V., et al. 2014) was proposed for wireless sensor networks. In the proposed method, each node has three types of priority queues. In addition, the sensor nodes were designed into the hierarchical structure and nodes were considered at identical level while they have the equivalent hop distance. The data were processed based on the TDMA method at various levels. The similar priority data were processed based on the shortest job first scheduler for

improving the average waiting time. However, the throughput was reduced when the number of nodes was increased.

New scheduling algorithm (Mansouri, W., et al. 2011) was proposed for wireless mesh networks. The proposed work was used for developing the scheduling algorithm for wireless mesh networks. This novel algorithm was performed based on the channel quality which is essential for the scheduling decision. The type of connection such as handoff or new calls, class of service, delay, and quality of channel were considered by the proposed algorithm for serving the real-time packets in priority and ensuring better quality of service. However, the performance of the network was not efficient.

An automated discovery of network service dependencies (Natarajan, A., et al. 2012) was developed for enterprise networks. In this paper, a novel technique was proposed and a novel tool called NSDMiner (Mining for Network Service Dependencies) was developed for discovering the dependencies between the network services automatically from passively collected network traffic. The proposed NSDMiner was non-intrusive so it does not require any software modifications or injection of network packets. In addition, different techniques were discussed for learning the network service dependencies automatically by analyzing the dynamic network traffic. However, the network configuration modifications wee not handled by the proposed approach.

Real-time scheduling algorithm (Saleh, M., & Dong, L. 2012) was proposed for packet switched networks including with the security awareness. In this paper, the real-time GAIA multi-agent system framework was proposed for combining the real-time scheduling functionalities with the confidentiality security service enhancements for packet switched networks. The differentiated earliest deadline first scheduler was utilized by the real-time scheduling scheme. Also, the resource estimation method was adopted by the security service enhancement scheme. The proposed method was utilized for providing the desired quality-of-service for the real-time data traffic when the packet's confidentiality security service level was enhanced adaptively. The buffering systems at the edge router and the destination nodes were optimally utilized for protecting the network from heavy traffic load. However, the energy consumption was not considered.

Improve real-time Packet Scheduling Algorithm with Security Constraint (IPSASC) was proposed for wireless networks. The major objective of the proposed algorithm was to remove the problems in security constraints under light traffic load. The proposed IPSASC paid high attention on security when the system has light traffic load and heavy traffic load. The proposed algorithm was performed with the scheduling and security for improving the guarantee ratio of the system and decreasing the number of packet drops in the network. However, the proposed algorithm was not utilized for hard deadline packets and periodic packets.

A practical secure mechanism (Tsou, Y. T., et al. 2013) was proposed for wireless sensor networks. In this paper, a security mechanism named MoteSec-Aware developed on the network layer for wireless sensor networks. The proposed algorithm was focussed on the secure network protocol and data access control. A Virtual Counter Manager (VCM) was provided with the synchronized incremental counter in the secure network protocol of MoteSec-Aware for detecting the replay and jamming attacks according to the symmetric key cryptography by using AES in OCB mode. The Key-Lock Matching (KLM) method was investigated for access control in order to prevent an unauthorized access. However, the issue of reducing the storage overhead was not considered.

A dynamic monitoring for energy consumption reduction (Lupia, A., & Marano, S. 2016) was proposed for trust-based intrusion detection system in mobile ad-hoc networks. The major objective of the proposed system was to decrease the packets monitored by the promiscuous mode of the wireless interface in terms of defining the relationship between the probability of monitoring the packet and the trustworthiness of the agent node. The proposed approach was known as Dynamic Monitoring Function (DMF) so the monitoring probability was lesser while the agent has the highest trust value. This approach was used for saving the energy without affecting the accuracy of intrusion detection system. However, the further improvements were required for energy saving and detection efficiency.

A low energy consumption routing protocol (Nuruzzaman, M. T., & Ferng, H. W. 2016) was proposed for mobile sensor networks including with the path-constrained mobile sink. In this paper, a method was proposed for delaying the data transmission from mobile nodes until the mobile sink was approaching the location where the shortest path may be reached. The future location of the mobile sink was predicted by the mobile nodes by using the broadcast packets which consists of timestamp, broadcast location, destination, and average speed acquired from its GPS-based navigation system along with the traffic information from the mobile sink. In addition, the proposed approach was utilized for reducing the energy consumption. However, the multiple mobile sinks were not considered in this approach.

Minimizing energy consumption in mission-specific mobile sensor networks (Ouchitachen, H., et al. 2015) was proposed by locating the sensors and base station in the best locations. In this paper, two novel algorithms such as Sensors Genetic Algorithm (SGA) and Base station Genetic Algorithm (BGA) were proposed. The proposed SGA and BGA were utilized for solving the energy constraint in the critical sensor network where each sensor was satisfied its missions depending on its locations. The proposed SGA was provided at equilibrating the mission and communication cost by locating the all sensors in the best locations rather to the degree of mission satisfaction and the quality of communication between all nodes. The BGA was located at the base station regarding available resources in the network. However, the convergence process was very slow.

An energy-aware and scalable multipath routing protocol (Cai, X., et al. 2015) was proposed for wireless sensor networks based on the dynamic cluster and foraging behaviour of the bee swarm. The proposed energy efficient and scalable multipath routing protocol was called as Bee-Sensor-C. Initially, a dynamic clustering technique was introduced. The Bee-Sensor-C scheme was provided for parallel data transmissions by reducing the overhead and improving the scalability. In addition, an enhanced multipath construction method was adopted by the Bee-Sensor-C for achieving the balance of the network energy consumption. However, the compatibility of the proposed scheme was less.

An Independent Zone Routing (IZR) protocol (Samar, P., et al. 2004) was proposed for ad-hoc wireless networks. This IZR protocol was developed from zone routing protocol used for allowing adaptive and distributed configuration for optimal size of every node's routing zone on the per-node premises. The configuration was achieved at every node by means of analyzing the local path control traffic and providing the tuning mechanism. The protocol was used for improving the performance, scalability and robustness. However, QoS and security and power consumption were not investigated.

Neighbor node anonymity in mobile opportunistic social networks (Chen, K., & Shen, H. 2016) was developed with the fine-grained control. In this paper, the FaceChange approach was proposed for supporting both anonymizing the real ID among neighbor nodes and collecting the real ID-based encountering information. Two encountering nodes were communicated anonymously for node anonymity. The group of novel methods were provided for ensuring the confidentiality and uniqueness of encountering evidences. The FaceChange was used for supporting the fine-grained control over the information which is shared with the encountered node based on the attribute similarity such as trust measured without the disclosing the attributes. In addition, the advanced extensions were proposed for sharing the real ID between mutually trusted nodes. However, the complexity was high.

A dynamic fake source algorithm (Bradbury, M., et al. 2015) was proposed for source location privacy in wireless sensor networks. In this paper, a novel dynamic fake-sources-based algorithm was proposed for Source Location Privacy (SLP) which does not require the prior knowledge about the network. The proposed algorithm was performed based on the online estimation of the identified network configuration parameters. The parameters were such as the temporary fake source duration, the temporary fake source period and the permanent fake source period. However, the computational complexity of the algorithm was high.

The source location privacy (Jhumka, A., et al. 2012) was investigated in wireless sensor networks by using fake sources. In this paper, different fake source approaches were discussed for providing the novel formalisation of the source location privacy (SLP) problem and ensuring the source location

privacy problem to be NP-complete. In addition, this approach was used to provide the heuristic which yields an optimal level of privacy under appropriate parameterisation. The novel formalisation of the SLP was provided for identifying the two important parameters such as message rates and fake message transmission duration in order to improve the efficiency of the algorithm. However, the algorithm was performed well for the network structure like grid structure with the sink at the centre.

Privacy preservation (Liu, J., et al. 2012) was proposed for location based services in mobile ad-hoc networks. In this paper, a novel solution of pseudonym modification was proposed for non-cooperative users and in the absence of intermediary. The main objective of the proposed method was ad-hoc anonymity. The proposed solution was utilized for allowing the users for deciding whether or not participating based on their motivations. Moreover, artificially generated dummies mixed up the all users who were participated in the pseudonym modifications at various times. Furthermore, the theoretical analysis was used for demonstrating the asynchronous pseudonym modification and dummy participation to enhance the privacy protection.

The impact of broadcast rates and collisions (Thomason, A., et al. 2013) were evaluated on fake source protocols for source location privacy. In this paper, practical factors were explored for the configuration and application of the fake source protocols including with the interplay between the broadcast rates of sensor nodes, message collisions and achieved privacy. Initially, the SLP problem was addressed based on the fake sources. The proposed method was utilized for finding the real and fake source broadcast rates were inversely connected to the number of collisions due to the message propagation increasing the potential for collisions, an increase in the proportion of collided messages on the wireless sensor networks to decrease the privacy afforded and reducing the broadcast rate of source nodes in pursuit of energy efficiency and increased yield for privacy. However, the performance evaluation was limited by considering the few factors.

Anonymity, unlinkability and unobservability (Vijayan, A., & Thomas, T. 2014) were discussed in mobile ad-hoc networks. In this paper, different anonymous routing and secure communications were studied in mobile ad-hoc networks. Different routing protocols were analyzed according to the public or private key pairs and cryptosystems within the Unobservable Secure Routing (USOR) for protecting the user privacy against inside as well as outside attackers. The proposed method was based on the combination of the group signature method and ID based encryption method. These were operated during the route discovery process.

Location-aware Location Privacy Protection (L2P2) (Wang, Y., et al. 2016) was proposed for mobile location based services. In this paper, a novel location privacy problem was addressed such as L2P2 problem in which the users may define the dynamic and diverse privacy requirements for various locations. The objective of L2P2 problem was to discover the smallest cloaking area for every location request so the diverse privacy requirements over spatial and/or temporal dimensions were satisfied for all users. The L2P2 problem was formalized as two versions and different effective heuristics were proposed for providing the location-aware location privacy protection for mobile users. However, in this paper, only four heuristic were considered and the performances were also varied for four heuristics.

Random selection false source-based algorithm (Bai, L., et al. 2016) was proposed for protecting the source-location privacy in wireless sensor networks. In this paper, the proposed algorithm was utilized for selecting the phantom source node with the random walk. The intermediate node was selected from the nodes on the shortest phantom source-sink path including with the random number and information about the hops to sink. The fake source node was selected by the intermediate node by using random walk. For evaluating the performance of the proposed algorithm, both theoretical and practical analysis was presented.

Optimal-cluster-based Source Anonymity Protocol (OSAP) (Niu, X., et al. 2014) was proposed in delay-sensitive wireless sensor networks. In this paper, initially, OSAP was proposed based on the FitProbRate and unequally clustering for reducing the network traffic and achieving the balance in the network traffic and real event report latency by adjusting the transmission rate and the radius of

unequal clusters. The, the problem of reducing the network traffic was transformed into the mathematical programming problem which is resolved by using mathematical techniques.

The privacy measure of the source location privacy scheme (Gurjar, A., & Patil, A. R. B. 2013) was evaluated in the wireless sensor network. In this paper, a source location scheme was proposed by using the cluster based anonymization and random routing. The privacy measure index was evaluated or estimating the overall privacy achieved by using the SLP method. Moreover, the effect of the privacy scheme was analyzed on the end-to-end message delay in order to estimate the network performance degradation and establish the efficacy of the SLP approach. The proposed model was analyzed by using information theoretic approach of both entropy and probability. However, the energy consumption and packet delivery ratio were not considered.

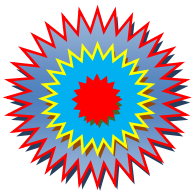
Preserving source-location privacy through redundant (Dong, M., et al. 2015) was proposed for loop in wireless sensor network. In this paper, a redundant fog loop-based method was proposed for preserving the source node-location privacy and achieving the energy efficiency by using two significant techniques for wireless sensor networks. The first technique was utilized for generating the fogs with the loop paths. The second technique was used for generating the fogs in the real source node region with many interference fogs in other regions of the network. Moreover, the fogs were dynamically changing and the communication among fogs were formed the loop path. The proposed method was provided for improving the network privacy status and optimizing the network energy resource utilization in order to improve the lifetime of network.

Source-location privacy through dynamic routing (Li, Y., & Ren, J. 2010) was proposed for wireless sensor networks. The major objective of the proposed system was protecting the source-location privacy by using the two-phase routing process and also routing to the single randomly selected intermediate node and developing the two multi-intermediate nodes selection strategies for the SLP method. In this paper, the SLP method was proposed by using routing to the randomly selected intermediate nodes before the message was forwarded to the sink node. Moreover, the routing via multiple selected intermediate nodes was presented according to the angle and quadrant for further improving the global source location privacy.

Quantification of anonymity (Moe, M. E. G. 2009) was investigated for mobile ad-hoc networks. In this paper, a probabilistic system framework was proposed for anonymous ad-hoc routing protocols by considering the prior knowledge about the adversary. The information theoretical entropy measure was discussed for quantification of the anonymity of the system as the adversary captures an increasing the number of nodes in the network. However, the performance of the algorithm was not analyzed for different number of adversarial nodes.

2.2 CHAPTER SUMMARY

In this chapter, the previous researches and packet scheduling algorithms in wireless networks are studied. In addition, different source location privacy and anonymity algorithms are also discussed in detail. Therefore, the proposed secure aware packet scheduling algorithm is provided based on the issues in the previous algorithms.



CHAPTER - 3

A NOVEL SERVICE-LEVEL SECURITY-AWARE PACKET SCHEDULING IN MOBILE AD-HOC NETWORK

A NOVEL SERVICE-LEVEL SECURITY-AWARE PACKET SCHEDULING IN MOBILE AD-HOC NETWORK

This chapter provides the detailed information about the service-level based security-aware packet scheduling algorithm in mobile ad-hoc networks for reducing the delay based on the consideration of the packet dependencies. This chapter describes how service-level based security-aware packet scheduling algorithm reduces the delay and communication overhead according to the dependencies of packets.

3.1 INTRODUCTION

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 (Zhu, X., et al. 2012) is introduced based on the dynamic Security-Aware Packet Scheduling (SPSS) algorithm (Qin, X., et al. 2008).

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 research, dependent relations are considered in ISAPS algorithm by discovering the service dependencies in mobile ad-hoc networks. In this chapter, service-level security-aware packet scheduling algorithm is explained in brief.

3.2 SERVICE-LEVEL SECURITY-AWARE PACKET SCHEDULING ALGORITHM

In this section, 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 section, these two types of dependencies are explained and detection of dependencies, representation of dependencies and construction the representation are also described.

3.2.1 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 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).

3.2.2 Scheduler Model

An improved scheduler model is considered in which each node is having the single transmitter and the single receiver. Normally, the single transmitter and the single receiver are combined in the single transceiver on the mobile node and the scheduler is implemented for the wireless networks.

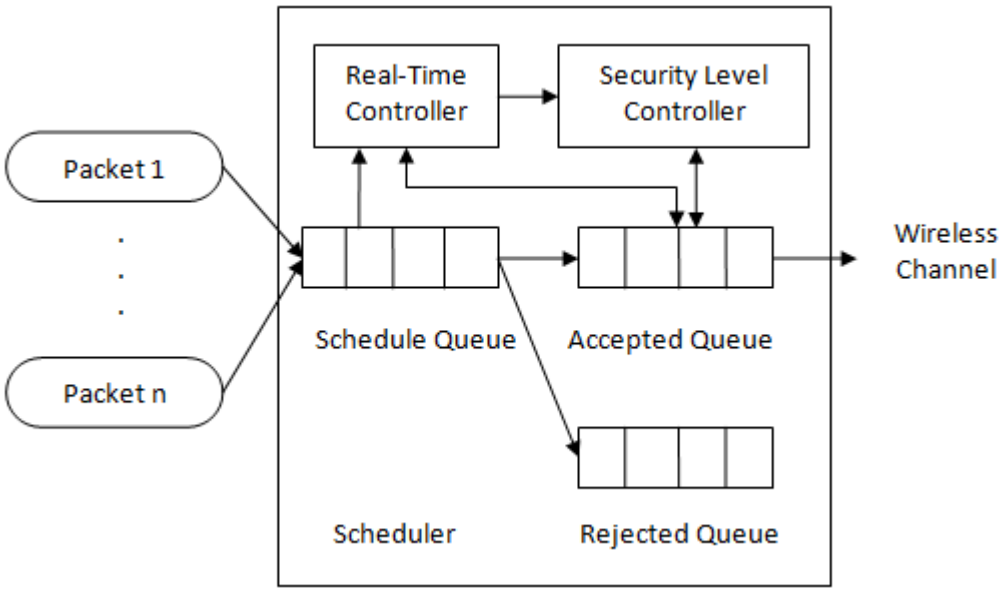


Figure.3.1 Improved Packet Scheduler Model

Figure 1 illustrates that an improved packet scheduler located between transmitters and receivers. When a new packet is arrived, initially it is given to the schedule queue in order to wait for scheduling and the lowest security level assigned. The real-time controller in the scheduler is used to get the new packet from the schedule queue according to the Earliest Deadline First (EDF) policy and the new packet is determined whether it is accepted or not. The real-time controller is consists of both the new packet and the packets waiting in the accepted queue for maximizing the schedulability. If the new packet is not accommodated then it is dropped into the rejected queue otherwise it is transformed into the accepted queue. The security level controller is notified for functioning by the real time controller after the new packet is allocated to the accepted queue. The security level controller is provided for the increasing the security level of packets in the accepted queue which utilizes the system resource for enhancing the security of packets in wireless networks effectively.

3.2.3 Packet Model

Consider a set of soft real-time packets $P = \{p_1, p_2, \dots, p_m\}$ which are transmitting from the target service T_s and clients are represented as $C = \{1, \dots, |C|\}$. Different client services related to the target service T_s is denoted as $C_s = \{c_1, c_2, \dots, c_n\}$. The security levels of each packet are denoted by $S = \{s_1, s_2, \dots, s_n\}$. The dependencies of packet are denoted as $D = \{d_1, d_2, \dots, d_k\}$. For a given packet $p_i \in P$, the arrival time, deadline and finish time are represented as a_i, d_i and f_i respectively. Moreover, consider $Z = \{z_1, z_2, \dots, z_m\}$ is the binary set where $z_i = 1$ if p_i is allocated successfully, otherwise $z_i = 0$.

3.2.4 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.

The size of DG is reduced by the short time duration but some significant service interactions are missed. The complete record of dependencies is provided by the long time duration. The service dependency graph is the directed graph which is denoted as $DG = < S, D >$, where S is the finite set of services $S = \{s_1, s_2, \dots, s_n\}$ and n is the number of services $(n \geq 2)$ and E is the finite set of dependencies among services $D = \{d_1, d_2, \dots, d_k\}$ where k is the number of dependencies $(k \geq 1)$.

3.2.5 Service Dependence Matrix

The DG is represented by using the dependence matrix. Every service in the dependence matrix is represented by the column and row. A cell in the matrix is used for representing the potential dependence between the source service of the column and the target service of the row. For a given service dependency graph DG, two services are considered such that $x, y \in S$ and the service dependency matrix is represented as $DM = [dm_{ij}]$ and the following conditions are used for discovering the services such as,

- $dm_{ii} = I$; I is known as Intra-Dependency value.
- $dm_{ij} = ID \ (i \neq j)$ If there is a dependency $d \in D$ for $x \rightarrow y$, otherwise $d\ m_{ij} = 0$; ID is known as Inter-Dependency value.

After constructing the service dependency graph, the corresponding matrix is also constructed. The service dependency matrix is shown in Table 3.1.

Table.3.1 Service Dependency Matrix

	S1	S2	S3	S4	S5
S1	I	0	0	0	0
S2	ID	I	0	0	0
S3	0	ID	I	0	0
S4	0	0	ID	I	0
S5	0	0	0	ID	I

Each element in the service dependency matrix is defined for representing the dependency whose direction is from column service to row service. Each I value in the matrix represents the self-dependency of the service which denotes the inter-service relations. Each ID in the matrix represents that there is dependency between services from the column service to the row service. In addition, every 0 in the matrix indicates that there is no dependency between two services.

The inter-intra service dependency matrix is constructed as follow:

For a given service dependency graph DG, two services $x = \{e_1, e_2, \dots, e_m\}, y = \{e_1, e_2, \dots, e_n\} \in S, x \neq y$ and a dependency $d \in D$ for $x \rightarrow y$ and the following definitions are defined as,

- The intra-service relation matrix is denoted for the service x is as follows:

$$P_x = [p_{ij}], 1 \leq i, j \leq m$$

Here, $p_{ij} = 1$ if e_i has a relation with e_j, $e_i \in x, e_j \in y$; otherwise $p_{ij} = 0$.

- The inter-service relation matrix is represented for dependency d is as follows:

$$Q_{x \to y} = [q_{ij}], 1 \leq i \leq m, 1 \leq j \leq n$$

Here, $q_{ij} = 1$ if e_i has a relation with e_j, $e_i \in x, e_j \in y$; otherwise $q_{ij} = 0$.

Table.3.2 Intra and Inter-Service Dependence Matrix

	e1	e2	e3	e4	e5
e1	1	0	0	0	0
e2	1	1	0	0	0
e3	1	0	1	0	0
e4	0	0	0	1	0
e5	0	0	0	1	1

The table 3.2 shows that the intra and inter-service relations for client service and target service. This matrix is constructed by filling 1 or 0 which represents the intra or inter relations. The established matrix representation is used for capturing inter and intra-dependencies easily. The proposed service dependency detection approach utilizes the distributed set of monitoring agents which provide the information to the centralized dependence discovery component which is shown in figure 3.2.

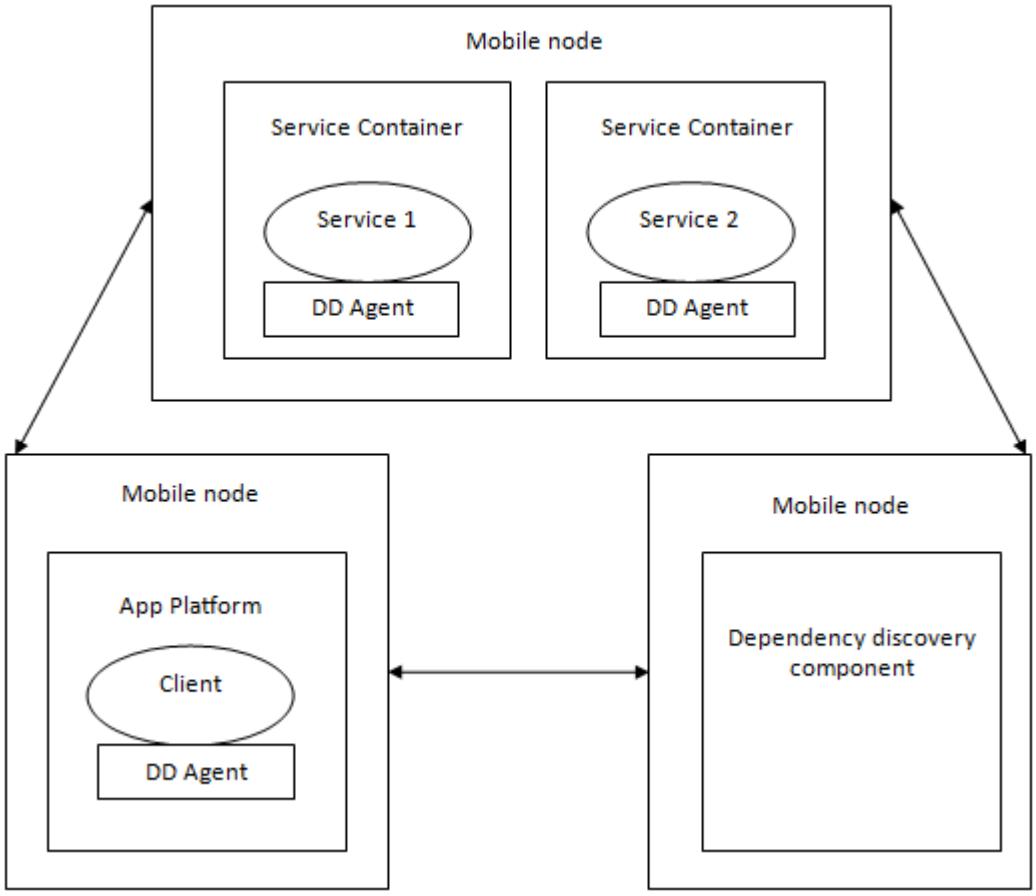


Figure.3.2 Architecture of Dependence Discovery

The most common case of DG construction is for a client. The DG consists of the set of services where the clients are depending upon directly or indirectly. Theoretically, the data are harvested by the walk rooted at the monitoring agent connected to the client. For specific analyses, the dependence discovery is limited to the specific conversation which is utilized in fault localization. This can be achieved by adjusting the time duration of the DG.

The accuracy of DG construction is depending upon the time duration and workload. Some significant dependencies with short time duration and small workload are not observed so these are missed. The obsolete and irrelevant dependencies with long time duration and large workload are included. In addition, the number of monitoring agents are also affected the accuracy of DG.

3.2.6 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_s) 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.

The following condition must be satisfied for scheduling real time packet.

$$st_i + pt_i \leq dl_i \tag{3.1}$$

$$\forall p_q, o_q < o_i,\ w_q = 1:\ st_q + pt_q \leq dl_q \tag{3.2}$$

In equations (3.1) and (3.2), st_i is the starting time of i^{th} packet in P, pt_i is the processing time of i^{th} packet in P, and dl_i is the deadline of i^{th} packet in P. Also, p_q is q^{th} packet in P, o_q is the transmission order of packet p_q, and $w_q = 1$ is the packet p_q waiting in the accepted queue. The security overhead so_i is expressed as the additional processing time and the total processing time pt_i are given as,

$$so_i = t_i \times (s_i/|S|) \tag{3.3}$$

$$pt_i = t_i + so_i = t_i \times (1 + s_i/|S|) \tag{3.4}$$

In the above equation, a_i is the arrival time of the packet p_i, and r is the remaining transmission time of the transmitting packet on the wireless channel. When clustering is performed on incoming packets P, number of clusters are formed and denoted as l.

$$Cl_s: \{1, \ldots, m\} \rightarrow \{1, \ldots, l\} \tag{3.5}$$

The packets related to the target service are assigned to the intra-service dependence clusters Cl_I and the packets which are irrelevant to the target service are assigned as inter-service dependence clusters Cl_{ID}. Consider number of nodes represented as $U = \{u_1, u_2, \ldots, u_z\}$. The packets p_i entered into the node u_i are based on the Euclidean distance measure between similarities of target service packets and client service packets.

$$D(U) = \sqrt{\sum_{s=1}^{n} |p(T_s) - p(C_s)|^2} \tag{3.6}$$

In equation (3.7), $p(T_s)$ are the target service packets, and $p(C_s)$ are the client service packets. Therefore, the starting time st_i of the packet p_i is denoted as,

$$st_i = a_i + \sum_{o_k<o_i, w_k=1} pt_k + r \quad (3.7)$$

The total processing time is rewritten based on the service dependence discovery method as follows,

$$pt_i = t_i + dt_i + so_i \quad (3.8)$$

In equation (3.8), t_i is the transmission time of the packet p_i, and dt_i is the dependence discovery time of the packet p_i. The security overhead so_i is also rewritten as follows,

$$so_i = t_i \times \left(\frac{s_i}{|S|}\right) \quad (3.9)$$

Where, s_i refers the security level of the packet p_i. According to the limits of security levels defined by the users, the relevant packets must be maximized under timing constraints.

$$\max_{p_i \in p(T_s)} \sum_{i=1}^{m} z_i \quad (3.10)$$

After the packets from related services are obtained, the security levels are required to be maximized.

$$\max_{p_i \in p(T_s)} \{\sum_{i=1}^{m} z_i \, s_i / \sum_{i=1}^{m} z_i\} \quad (3.11)$$

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 (3.1) and (3.2)
2. Clustering the real time service packets based on similarity measurement calculated by (3.6)
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 (3.7)
5. Calculate the total processing time of packets with respect to deadline time using (3.8)
6. Provide security level to each packets using (3.10) and (3.11)
7. Scheduling the packets

3.2.7 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 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. At this moment, the similarity S_{ID} between packets among inter-service dependence cluster is calculated. It is measured as,

$$S_{ID} = \min(Euclidean\ distance\ between\ two\ packets\ from\ each\ cluster) \quad (3.12)$$

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 (3.1) and (3.2)
2. Clustering the real time service packets based on similarity measurement calculated by (3.6)
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 (3.12)
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 (3.7)
7. Calculate the total processing time of packets with respect to deadline time using (3.8)
8. Provide security level to each packets using (3.10) and (3.11)
9. Scheduling the packets

3.3 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.

3.3.1 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

A). Deadline versus Guarantee Ratio (%)

The comparison of deadline versus guarantee ratio is shown in Table 3.3.

Table.3.3 Comparison of Guarantee Ratio based on Deadline

Deadline	ISAPS	ISDSPS	IISDSPS
100	41%	43%	46%
300	58%	62%	65%
500	70%	73%	76%
700	85%	88%	91%
900	90%	92%	94%

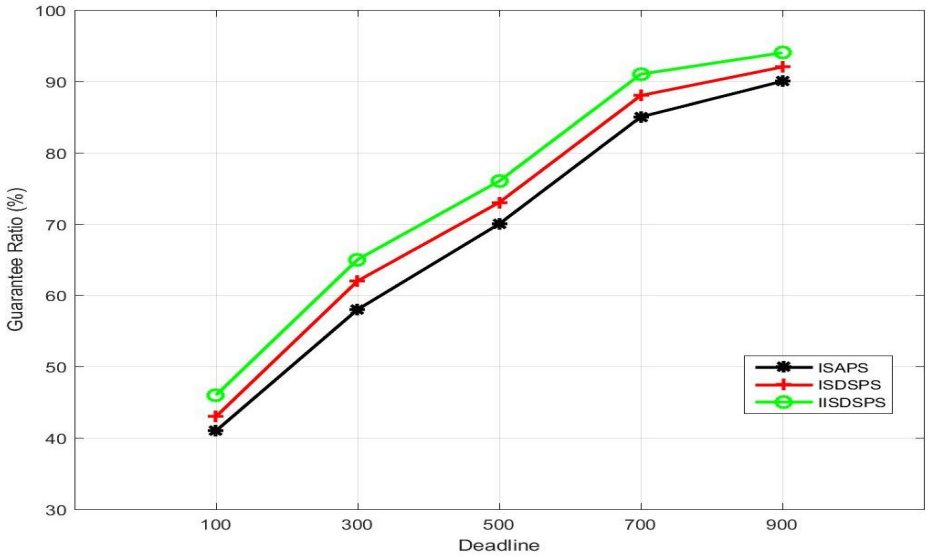


Figure.3.3 Deadline versus Guarantee Ratio (%)

Figure 3.3 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 IISDSPS has higher guarantee ratio than the other algorithms.

B). Arrival Rate versus Guarantee Ratio (%)

The comparison of arrival rate versus guarantee ratio is shown in Table 3.4.

Table.3.4 Comparison of Guarantee Ratio based on Arrival Rate

Arrival Rate	ISAPS	ISDSPS	IISDSPS
10	95%	88%	81%
30	81%	72%	64%
50	70%	59%	51%
70	58%	43%	36%
90	41%	38%	30%

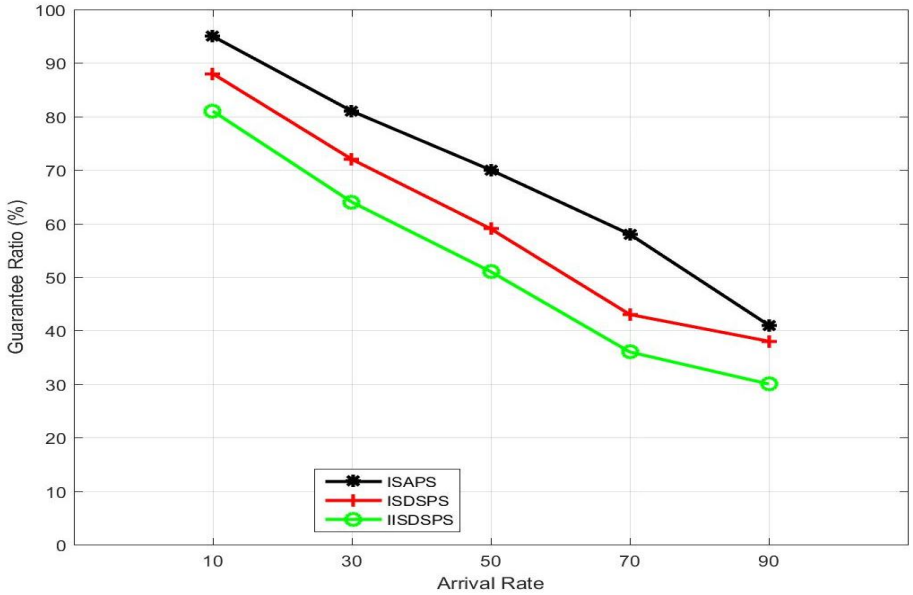


Figure.3.4 Arrival Rate Vs Guarantee Ratio (%)

Figure 3.4 shows that the result of guarantee ratio comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the guarantee ratio (%) is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Then, the packets arriving later increases the probability of missing deadlines. Thus, the guarantee ratio is decreased. The proposed IISDSPS has higher guarantee ratio that is IISDSPS has the ability for enhancing the schedulability than the other algorithms while the system workload is high.

3.3.2 Average Security Level

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

A). Deadline versus Average Security Level

The comparison of deadline versus average security level is shown in Table 3.5.

Table.3.5 Comparison of Average Security Level based on Deadline

Deadline	ISAPS	ISDSPS	IISDSPS
100	2.7	3.2	3.6
300	3.1	3.7	4.1
500	3.5	4.1	4.6
700	3.8	4.5	5.0
900	4.1	4.8	5.3

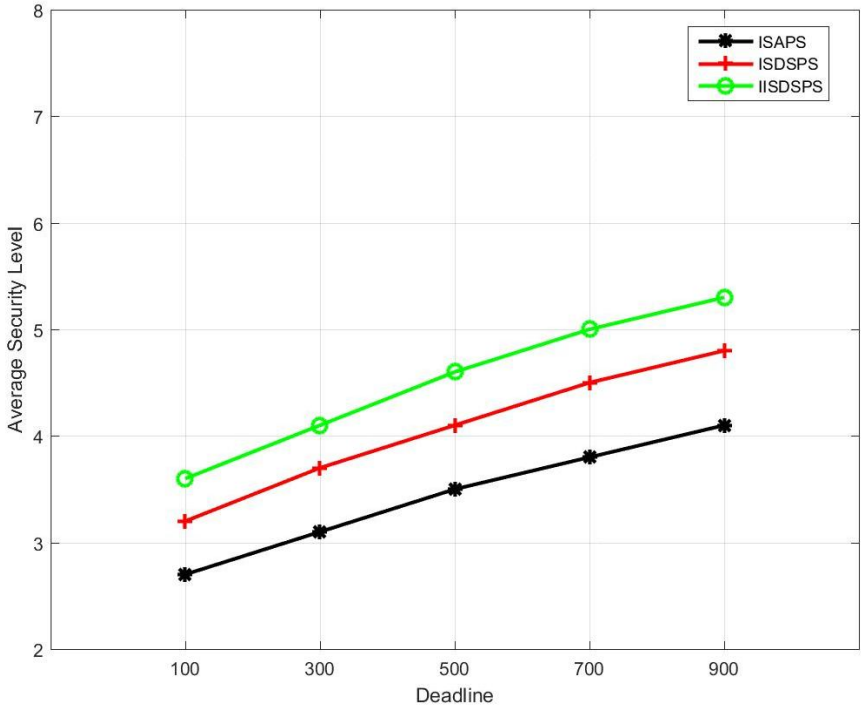


Figure.3.5 Deadline Vs Average Security Level

Figure 3.5 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.

B). Arrival Rate versus Average Security Level

The comparison of arrival rate versus average security level is shown in Table 3.6.

Table.3.6 Comparison of Average Security Level based on Arrival Rate

Arrival Rate	ISAPS	ISDSPS	IISDSPS
10	4.7	4.4	3.9
30	4.2	4.0	3.4
50	3.7	3.6	3.0
70	3.4	3.2	2.6
90	2.9	2.5	2.2

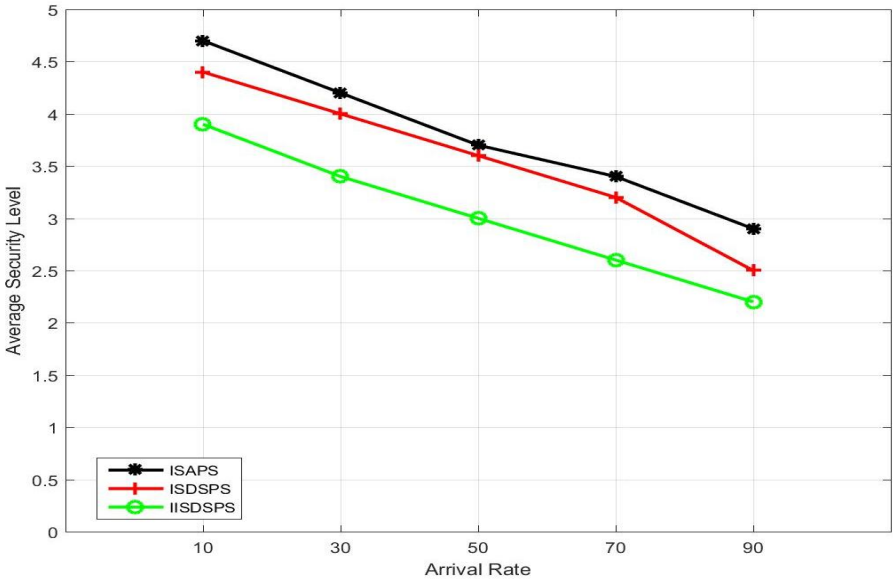


Figure.3.6 Arrival rate Vs Average Security Level

Figure 3.6 shows that the result of average security level comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the average security level is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Therefore, the security level of packets waiting in queue is degraded for improving the schedulability. Thus, the average security level is decreased. The proposed IISDSPS has higher average security level than the other algorithms by satisfying the security requirements of the users while the system workload is high.

3.3.3 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,

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

The comparison of packet delivery ratio is shown in Table 3.7.

Table.3.7 Comparison of Packet Delivery Ratio

Number of Nodes	ISAPS	ISDSPS	IISDSPS
20	0.48	0.52	0.57
40	0.54	0.58	0.64
60	0.60	0.63	0.69
80	0.66	0.69	0.75
100	0.72	0.75	0.81

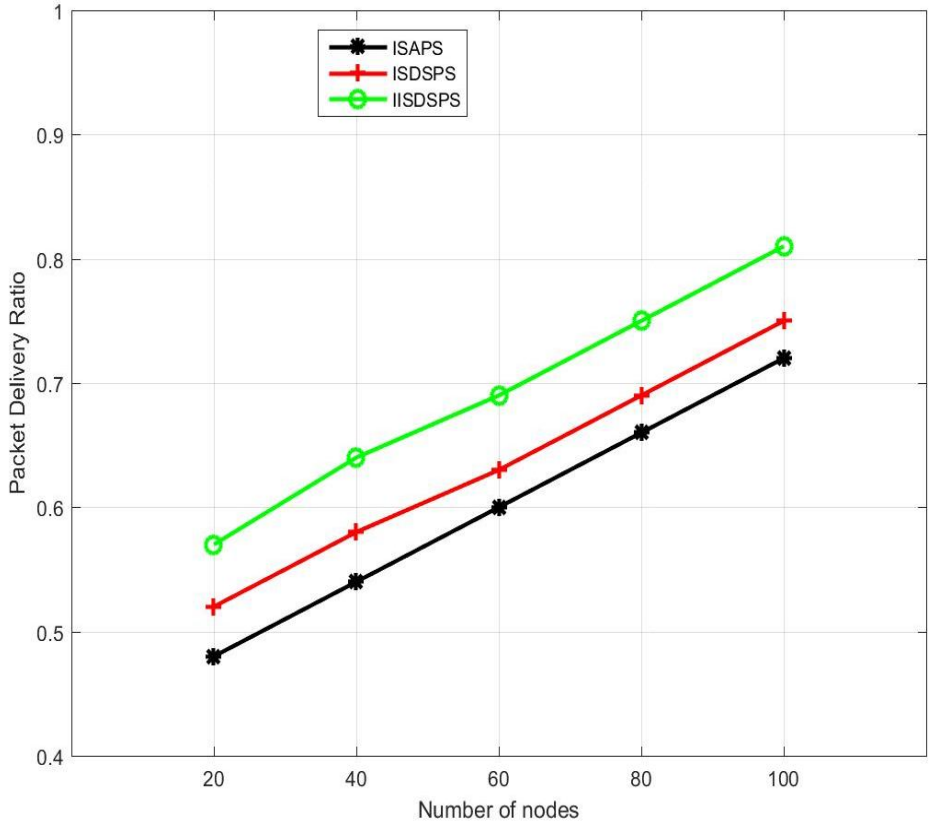


Figure.3.7 Number of Nodes versus Packet Delivery Ratio

Figure 3.7 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 IISDSPS has higher packet delivery ratio than the other algorithms.

3.3.4 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,

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

The comparison of end-to-end delay is shown in Table 3.8.

Table.3.8 Comparison of End-to-End Delay (seconds)

Number of Nodes	ISAPS	ISDSPS	IISDSPS
20	42	38	35
40	51	43	39
60	58	49	44
80	65	53	50
100	70	59	55

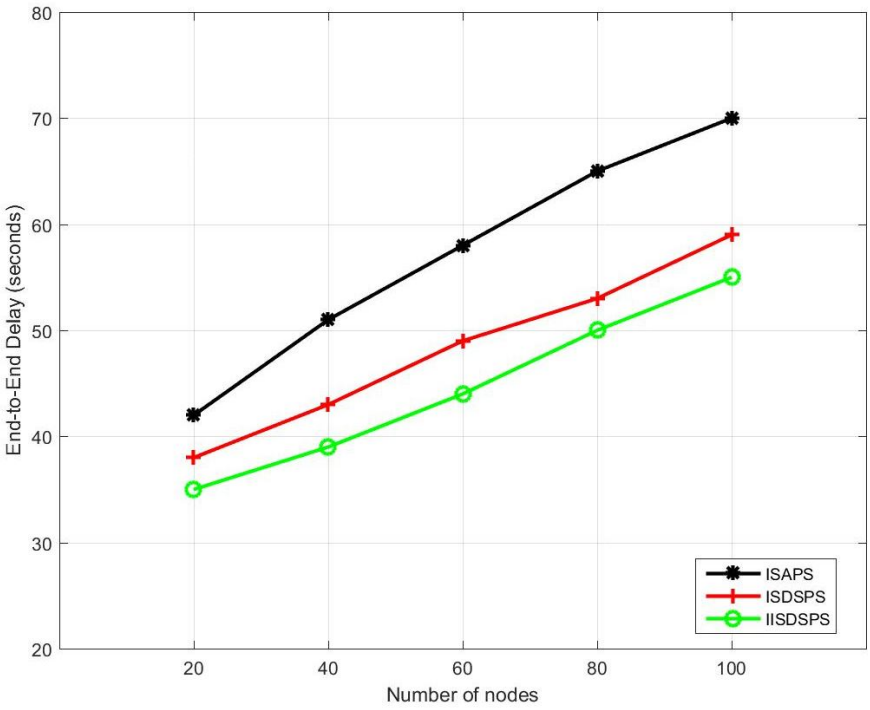
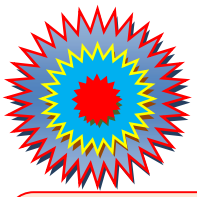


Figure.3.8 Number of Nodes Vs End-to-End Delay (Seconds)

Figure 3.8 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.

3.4 CHAPTER SUMMARY

In this chapter, 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.



CHAPTER - 4

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

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

This chapter provides the detailed information about the multiple layer based service-level dependent security-aware packet scheduling algorithm in mobile ad-hoc networks for reducing degradation of the performance of packet scheduling algorithm based on the consideration of the packet dependencies among multiple layers. This chapter describes how multiple layer based service dependent security-aware packet scheduling algorithm improves the correlation of packet dependencies between multiple layers and enhancing the packet level security.

4.1 INTRODUCTION

Nowadays, dynamic networks like MANET are mostly used for providing various services. In these networks, the performance degradation of services plays an important role for managing the services efficiently. The dynamic security mechanisms are provided for transmitting the data packets securely by using scheduling algorithms. In our previous research, service level security-aware packet scheduling algorithms are proposed. In which, inter and intra-service dependencies between the packets along with security level are considered for packet transmission. For this purpose, ISDSPS and IISDSPS algorithms are proposed effectively with less latency and communication overhead. However, the performance of services is affected due to time duration across different layers of networks. The correlation of the dependencies between the packets across multiple layers is not considered in multiple layer scenarios. Therefore, the correlation of the dependencies across multiple layers is required for reducing the packet scheduling performance degradation. Hence, in this research, multiple layer based service dependent security-aware packet scheduling algorithm is proposed including with the inter-intra service dependencies of packets. In this approach, a causality graph is constructed based on the Service-Layer Dependency Graph (SLDG) for evaluating the fault propagation among different services. In addition, the scalability issue is addressed by using the network tomography method. In addition, the spatial correlation is utilized between services to effectively narrow down the possible states of individual services. In this chapter, intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is described in brief.

4.2 NETWORK TOMOGRAPHY MODEL

The network tomography is utilized for fault diagnosis at the network layer level (Lawrence, E., et al. 2006). The major objective of the network tomography is inferring the link-level properties from the network topology and e2e client-service measurements. The faults are diagnosed by the large linear system which represents the relation between path and link properties must be solved. The problem is formulated based on the spatial correlation as,

$$Y = AX \tag{4.1}$$

Where, Y is the e2e client-service measurements matrix, A is the routing matrix, and X is the internal states of the links. However, the issue in network tomography is that fundamentally underconstrained such that in the network-level performance diagnosis there exists in the system whose status cannot be determined uniquely. Therefore, the proposed model of dependencies among different services and the measured service performance are described in terms of their success probabilities perceived by clients. Hence, the proposed approach is designed based on the network tomography model.

4.3 INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (IIMLSDSPS)

In this section, our proposed inter-intra and multiple layer based service dependent security-aware packet scheduling algorithm is described. Initially, the ISAPS algorithm is performed based on the dependence discovery method by using dependence graph model. These algorithms are explained briefly in Chapter 3. In this section, the proposed IIMLSDSPS approach is explained briefly.

4.3.1 System Model

In our proposed system, the set of clients, $C = \{1, \ldots, |C|\}$ are monitored for their successes or failures while accessing different services. For service dependencies, two system-level graphs are

utilized such as Directed Acyclic Graph (DAG) and Service-Layer Dependency Graph (SLDG). The Directed Acyclic Graph (DAG) is provided for representing the local dependency graph for client services. This model is described briefly in Chapter 3 and section 3.2.4.

4.3.2 Service-Level Dependency Graph (SLDG)

The Service-Level Dependency Graph (SLDG) is utilized for representing the global dependency graph for client services. The global SLDG $SLDG =< S, D >$ is defined as the union of all local dependency graphs $(DG =< S_i, D_i)$ for clients i. Here, $S = \bigcup_{i \in C} S_i$, and $D = \bigcup_{i \in C} D_i$ are represents the all possible service dependencies required for all requests of clients. The model of SLDG is given in figure 4.1.

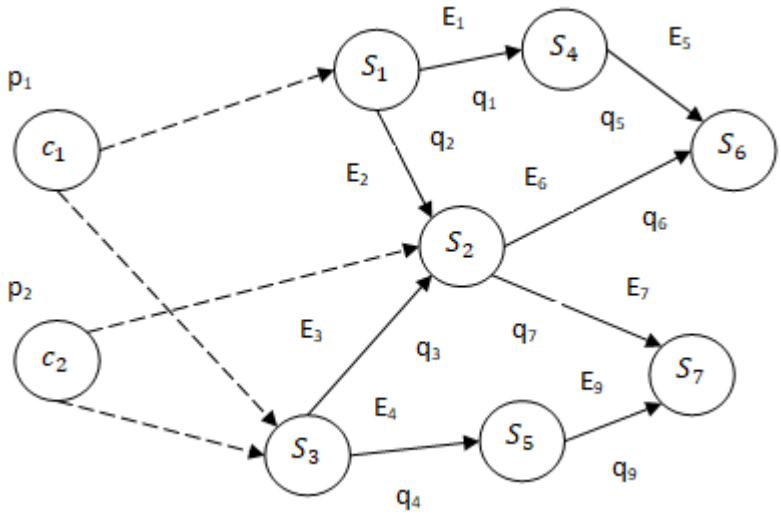


Figure.4.1 Example of SLDG

4.3.3 Monitoring Model

The measurements are gathered for evaluating the following probabilities.

- p_i for $i \in C$ is the success probability of e2e client-service dependency i. The vector of all p_i represents the monitored values.
- q_j for $j = (x, y) \in D$ is the success probability of the inter-service dependency between the services x and y. The vector of all q_j represents the internal states.

The client request is satisfied by assuming the all inter-service dependencies in the local dependency graph are successful. Hence, $p_i = 1 - \prod_{j \in D_i}(1 - q_j)$ and for all $i \in C$, $y_i = ln(1 - p_i)$ is defined and for all $j \in D$, $x_j = ln(1 - q_j)$ is defined. Hence, we have $Y = (y_1, \ldots, y|C|)$ and $X = (x_1, \ldots, x|D|)$.

4.3.4 Tomography based Algorithm

The proposed algorithm has two steps such as one is used for building the hypotheses list and the other is used for rating those dependencies of packets for determining the internal states of services efficiently (Tati, S., et al. 2011). In the first step, the network tomography is used for enumerating the all possible dependencies of packets for reducing the performance degradation in services. The linear equation $Y = AX$ is used for providing solution for our proposed approach. The $(|C| \times 1)Y$ matrix is used for representing success probabilities of clients; the element $\{a_{ij}\}$ in the $(|C| \times |D|)$ dependency matrix A is 1 if $j \in D_i$ otherwise zero, and the $(|D| \times 1)$ matrix X is used for representing the internal states of the services. Consider, the linear system is underconstrained.

Therefore, number of solutions is obtained for a given input. These solutions are listed as possible dependencies of packets in the hypotheses list.

In the second step, these possible dependencies of packets are ranked by using particular characteristics of services and the other constraints at the service layer. One of the characteristics that the spatial correlation of the nodes is used which provides the services. The second possible constraint is the policies which are deployed across the networks. These policies are precluded the particular services from running on certain nodes or precluded two services from interacting. The different dependencies of packets are ranked in the hypotheses list by using these additional constraints.

Therefore, the highly correlated dependencies of packets are collected and the high security level is provided for packet transmission. Thus, the packets are scheduled based on the proposed IIMLSDSPS approach which reduces the performance degradation of the algorithm.

Algorithm: IIMLSDSPS

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

1. Check the schedulability condition

$$st_i + pt_i \leq dl_i$$

$$\forall p_q, o_q < o_i,\ w_q = 1:\ st_q + pt_q \leq dl_q$$

2. Clustering the real time service packets based on similarity measurement

$$D(U) = \sqrt{\sum_{s=1}^{n} |p(T_s) - p(C_s)|^2}$$

2. Prioritizing intra dependency clusters and packets within the intra dependency cluster
3. Find correlation of dependencies of packets using spatial correlation approach

$$Y = AX$$

4. Find the probability of e2e client-service measurements and inter-service dependencies of packets
5. Check whether there is any packet in inter service dependency cluster is related to intra service dependency cluster

$$S_{ID} = \min(Euclidean\ distance\ between\ two\ packets\ from\ each\ cluster)$$

6. If yes, then give same priority as that of intra service dependency cluster packets
7. Calculate the start time of each prioritized packets intra service dependency

$$st_i = a_i + \sum_{o_k < o_i, w_k = 1} pt_k + r$$

8. Calculate the total processing time of packets with respect to deadline time

$$pt_i = t_i + dt_i + so_i$$

9. Provide security level to each packets

$$\max_{p_i \in p(T_s)} \sum_{i=1}^{m} z_i$$

$$\max_{p_i \in p(T_s)} \left\{ \sum_{i=1}^{m} z_i \, s_i / \sum_{i=1}^{m} z_i \right\}$$

8. Scheduling the packets

4.4 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 ISDSPS, IISDSPS, and IIMLSDSPS.

4.4.1 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

A). Deadline versus Guarantee Ratio (%)

The comparison of deadline versus guarantee ratio is shown in Table 4.1.

Table.4.1 Comparison of Guarantee Ratio based on Deadline

Deadline	ISDSPS	IISDSPS	IIMLSDSPS
100	43%	46%	50%
300	62%	65%	68%
500	73%	76%	79%
700	88%	91%	93%
900	92%	94%	96%

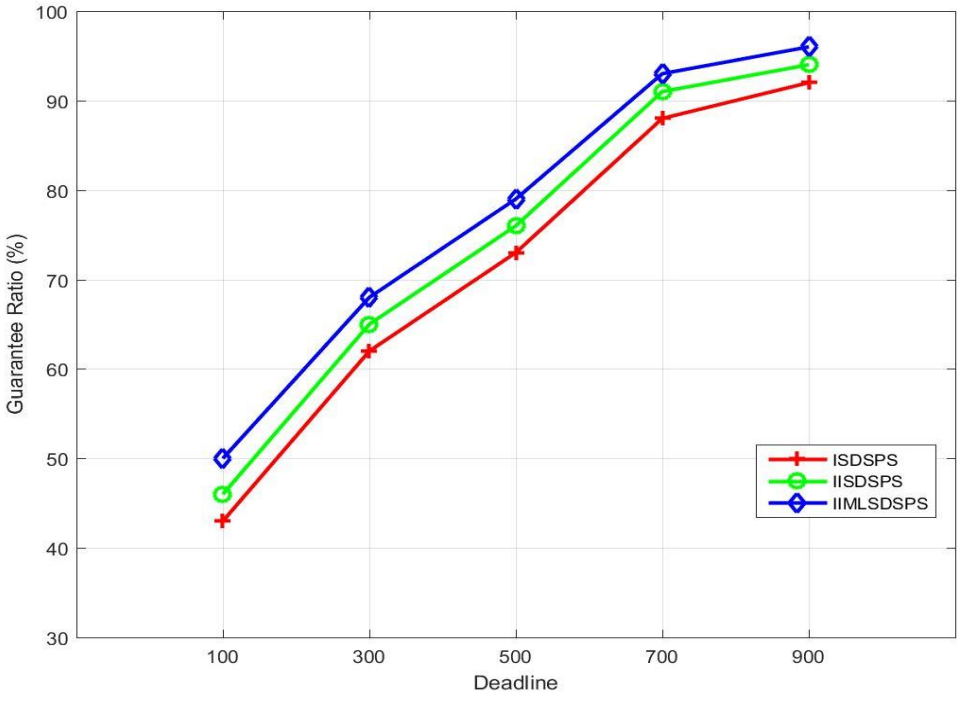


Figure.4.2 Deadline versus Guarantee Ratio (%)

Figure 4.2 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 IIMLSDSPS has higher guarantee ratio than the other algorithms.

B). Arrival Rate versus Guarantee Ratio (%)

The comparison of arrival rate versus guarantee ratio is shown in Table 4.2.

Table.4.2 Comparison of Guarantee Ratio based on Arrival Rate

Arrival Rate	ISDSPS	IISDSPS	IIMLSDSPS
10	88%	81%	76%
30	72%	64%	59%
50	59%	51%	45%
70	43%	36%	30%
90	38%	30%	24%

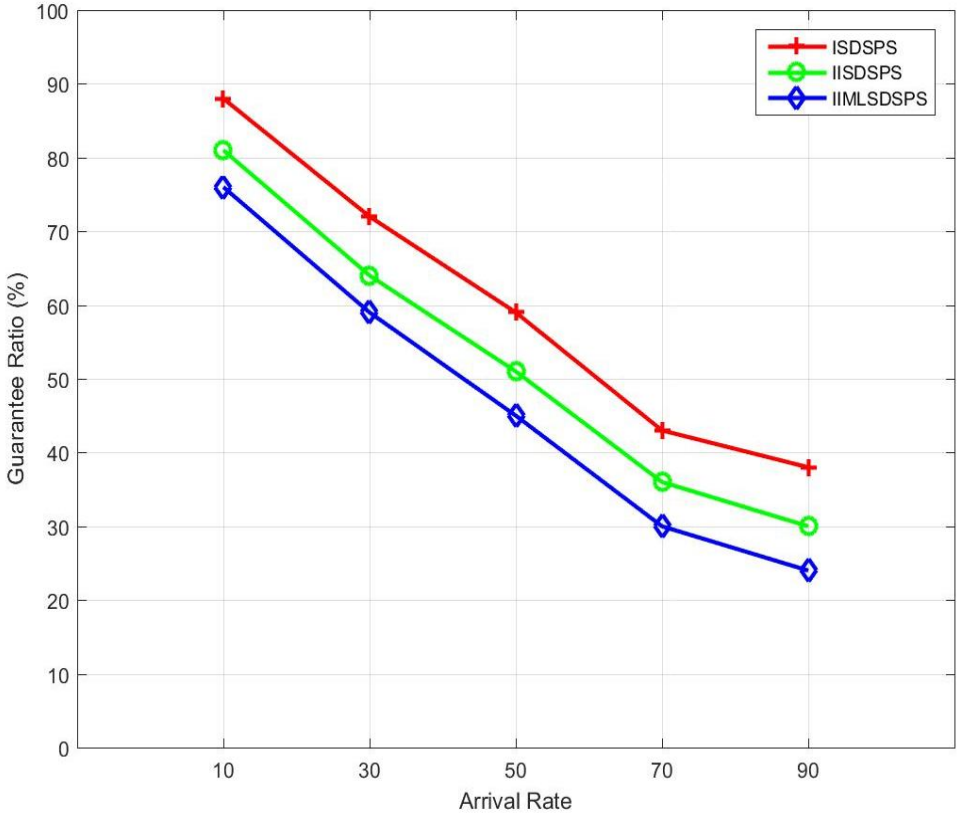


Figure.4.3 Arrival Rate versus Guarantee Ratio (%)

Figure 4.3 shows that the result of guarantee ratio comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the guarantee ratio (%) is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Then, the packets arriving later increases the probability of missing deadlines. Thus, the guarantee ratio is decreased. The proposed IIMLSDSPS has higher guarantee ratio that is IIMLSDSPS has the ability for enhancing the schedulability than the other algorithms while the system workload is high.

4.4.2 Average Security Level

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

A). Deadline versus Average Security Level

The comparison of deadline versus average security level is shown in Table 4.3.

Table.4.3 Comparison of Average Security Level based on Deadline

Deadline	ISDSPS	IISDSPS	IIMLSDSPS
100	3.2	3.6	4.0
300	3.7	4.1	4.4
500	4.1	4.6	4.7
700	4.5	5.0	5.2
900	4.8	5.3	5.6

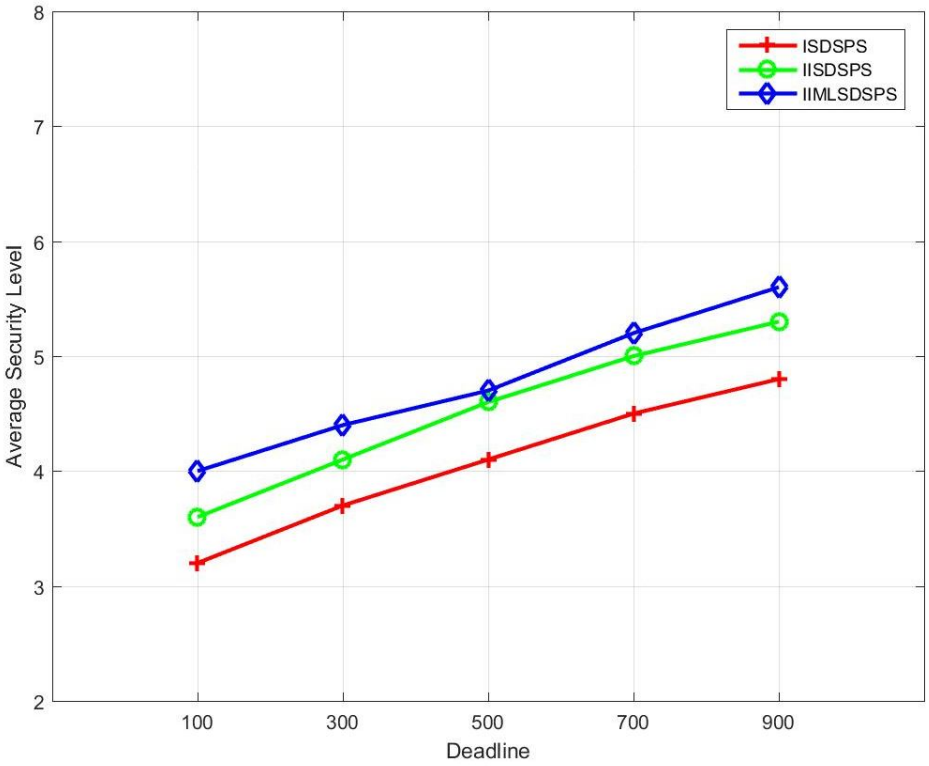


Figure.4.4 Deadline versus Average Security Level

Figure 4.4 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 ISDSPS 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 IIMLSDSPS has higher security levels than the other algorithms by satisfying the user's requirements.

B). Arrival Rate versus Average Security Level

The comparison of arrival rate versus average security level is shown in Table 4.4.

Table.4.4 Comparison of Average Security Level based on Arrival Rate

Arrival Rate	ISDSPS	IISDSPS	IIMLSDSPS
10	4.4	3.9	3.5
30	4.0	3.4	2.9
50	3.6	3.0	2.5
70	3.2	2.6	2.1
90	2.5	2.2	1.6

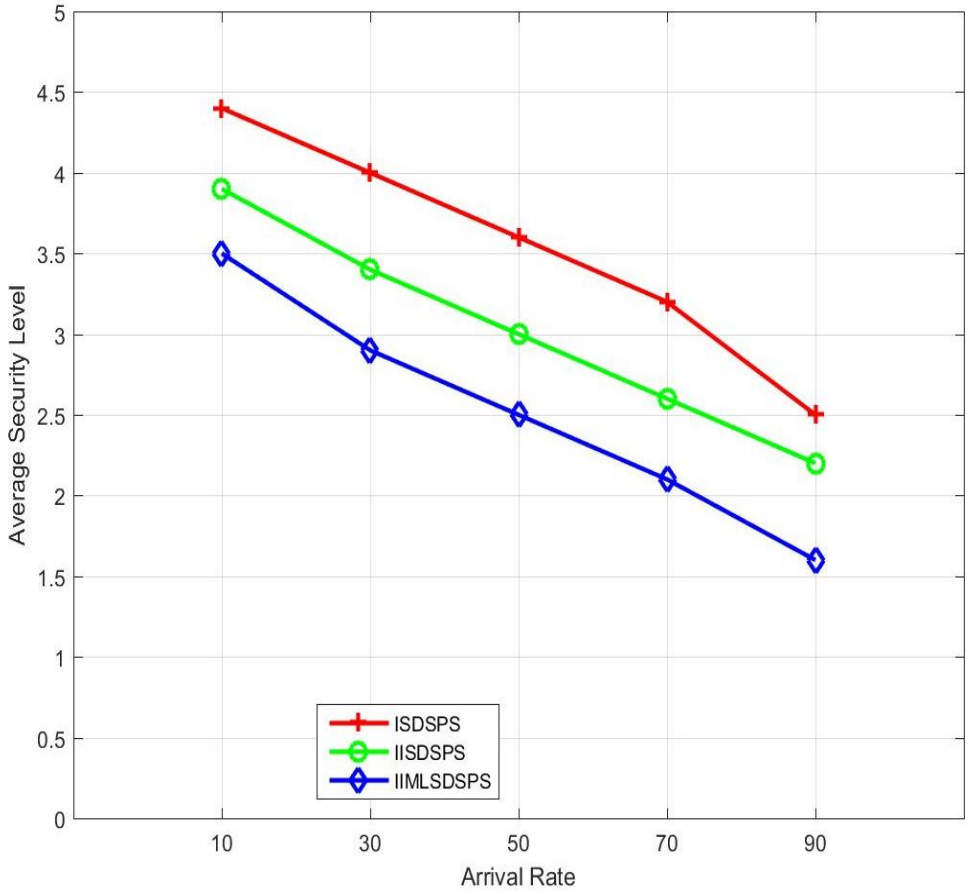


Figure.4.5 Arrival rate versus Average Security Level

Figure 4.5 shows that the result of average security level comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the average security level is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Therefore, the security level of packets waiting in queue is degraded for improving the schedulability. Thus, the average security level is decreased. The proposed IIMLSDSPS has higher average security level than the other algorithms by satisfying the security requirements of the users while the system workload is high.

4.4.3 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,

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

The comparison of packet delivery ratio is shown in Table 4.5.

Table.4.5 Comparison of Packet Delivery Ratio

Number of Nodes	ISDSPS	IISDSPS	IIMLSDSPS
20	0.52	0.57	0.61
40	0.58	0.64	0.66
60	0.63	0.69	0.72
80	0.69	0.75	0.79
100	0.75	0.81	0.85

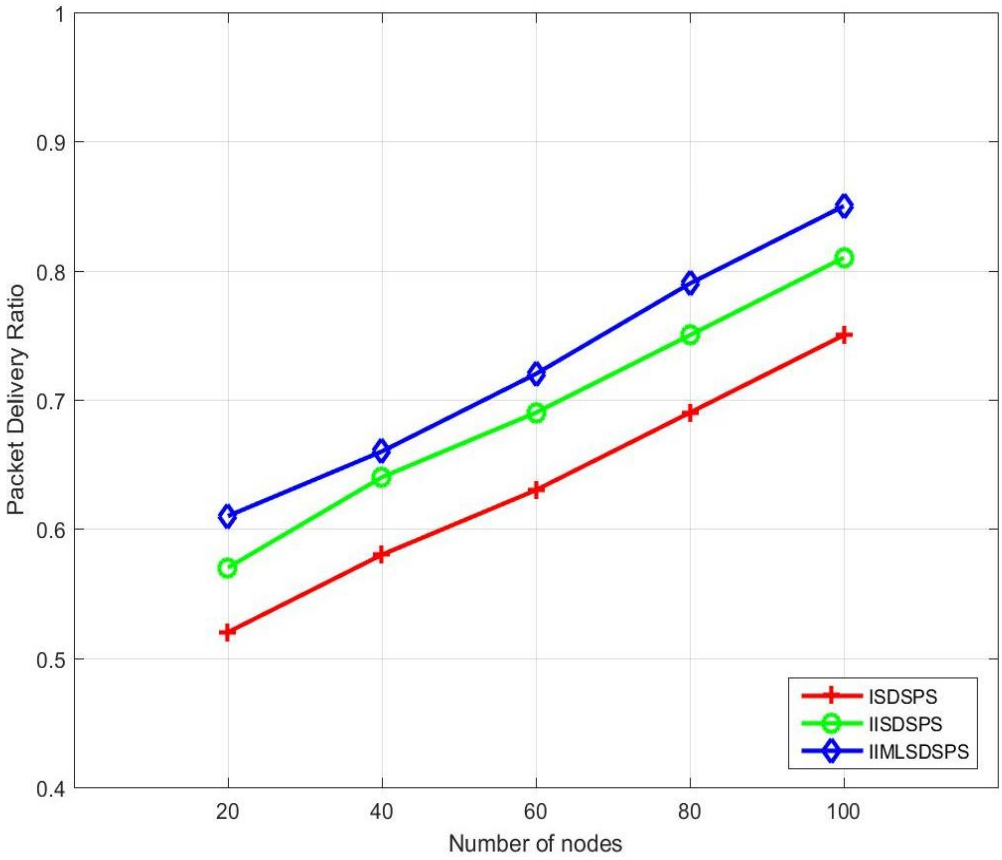


Figure.4.6 Number of Nodes versus Packet Delivery Ratio

Figure 4.6 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 IIMLSDSPS has higher packet delivery ratio than the other algorithms.

4.4.4 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,

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

The comparison of end-to-end delay is shown in Table 4.6.

Table.4.6 Comparison of End-to-End Delay (seconds)

Number of Nodes	ISDSPS	IISDSPS	IIMLSDSPS
20	38	35	31
40	43	39	36
60	49	44	41
80	53	50	47
100	59	55	52

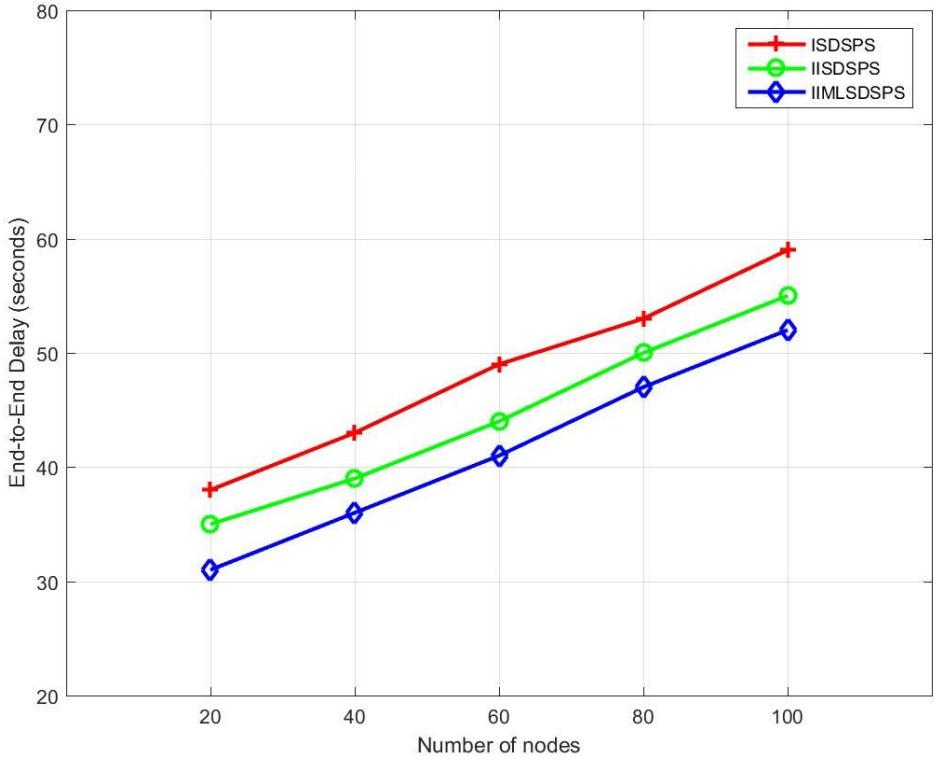
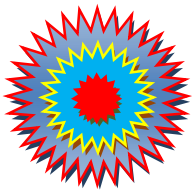


Figure.4.7 Number of Nodes versus End-to-End Delay (Seconds)

Figure 4.7 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 IIMLSDSPS has less end-to-end delay than the other algorithms.

4.5 CHAPTER SUMMARY

In this chapter, the issues of the correlation of dependencies of packets which are coming from multiple layers in mobile ad-hoc networks by using security-aware packet scheduling algorithm are considered. These issues are removed by introducing the multiple-layer based service-dependence discovery method which is combined with inter and intra-service dependence discovery algorithm and the service dependencies of packets are achieved by using service-level dependence graph (SLDG) as global dependency graph instead of dependence graph (DG). Moreover, the constraints for correlation of dependencies of packets are solved by constructing the hypothesis list and the correlation of dependencies are rated for improving the packet scheduling performance. Hence, the proposed IIMLSDSPS algorithm performs better than the IISDPS based algorithm. The experimental results are proved that the proposed IIMLSDSPS has better performance than the other algorithms.



CHAPTER - 5

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

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

This chapter provides the detailed information about the anonymity based multiple layer service-level dependent security-aware packet scheduling algorithm in mobile ad-hoc networks for improving the efficiency of security-aware packet scheduling algorithm by using anonymity of source-location. This chapter describes how source-location anonymity protocol improves the obscurity of mobile ad-hoc networks and enhancing the packet level security.

5.1 INTRODUCTION

In mobile ad-hoc networks, 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.

The series of service packets are reported to the base station that impostors eavesdropping on the network may backtrack to the source through traffic analysis and RF localization techniques. This provides the degradation in effectiveness of the mobile ad-hoc networks. The unreliability of wireless links and the broadcast property of physical layer provide the potential for an impostor in order to overhear the network. In some cases, source-location information leakage is exposed the locations of monitored agents and therefore the relevant information is utilized by an impostors. The impostor can overhear the service packet while it is transmitted to the destination or base station and the source location is determined through RF positioning technique. It continues until the service packet reaches the source hop-by-hop. Such issues may degrade the performance of security-aware packet scheduling algorithm.

Therefore, in this research, an anonymity-based source-location privacy method is proposed which is incorporated into the intra-inter and multiple layer service dependent security-aware packet scheduling algorithm. The proposed approach utilizes the fake source-location method for introducing the fake sources in the network in order to bewilder the impostors. These fake sources are utilized for constructing the different fake paths to transmit the packets according to the scheduling. In this chapter, an anonymity based intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is explained in brief.

5.2 NETWORK AND THREAT MODEL

In this section, anonymity-based intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is explained. The AIIMLSDSPS algorithm is developed by considering the source-location anonymity. After scheduling the packets by using IIMLSDSPS which is explained briefly in Chapter 4, anonymity scheme is introduced for transmitting the packets from source to destination securely. The network and threat model are described in below.

5.2.1 Network Model

In mobile ad-hoc networks, the number of sensor nodes is homogeneously distributed in the large region. Various base stations are deployed in the network for collecting and processing the sensed data from the lightweight sensor nodes. The base stations are secure along with high computational capability. Hence, it is considered to be impossible for filching any information from them. The major objective of employing the base stations is guaranteeing each sensor node can deliver its data to at least one base station not far away. However, in our proposed system, only one base station is considered in the network.

Then, client-service packets are generated and scheduled based on the service dependencies and also transmitted to the base station regularly. The packets with contextual information such as node ID and time stamp are forwarded to the base station in order to know about where and when the monitored agents are presented. Encryption algorithm is used for ensuring that an impostor cannot know about

the information of client-service packets. In addition, only one source node is considered in the network for reducing the data packet redundancy and also reporting the services all time period.

5.2.2 Threat Model

The sensor node is communicated with its neighbors in the radio transmission range. It broadcasts or discards the service packets while it receives the packets. The impostors are eavesdropping on the communications between the sensors. The adversary is assumed that it has similar eavesdropping range as radio communication range of the sensor nodes. Though, an impostor cannot obtain the accurate information of the packets intercepted, the direct sender of the packets is determined by using traffic analysis or RF localization techniques. The adversaries are overhearing at the base station. While intercepting the packet, it moves to the location where the packet transmitted from. Then, it eavesdrops on the communication between the present node and its neighboring nodes until backtracking to the source hop-by-hop.

In the proposed system, adversaries are considered to be record each location for avoiding the circulations generated by fake sources in the networks. The circulations provide it difficult for adversaries for tracking the source. At this situation, a sophisticated impostor is utilized for checking the historical locations after determining where the packets coming from. Only if the packet comes from the completely new sensor, the adversary is travelled to that node. Otherwise, the packets are discarded and an adversary is keep listening at the current location. It is possible that the patient adversary cannot overhear anything for long time duration. In this case, the adversary can roll back to the latest one among the recorded locations. Then, this location is eliminated from the record of the historical locations.

The local eavesdroppers are the adversaries who have only the local view of network traffic. The global eavesdroppers are the adversaries who eavesdrop on the entire network and complete view of network traffic. The global eavesdropper is easily infer the locations of monitored agents since the sensor nodes which initiate the communication along with the base station are normally close to the monitoring agents.

5.3 PATH EXTENSION METHOD

In the proposed approach, the source-location privacy is achieved by introducing the novel method which is called as Path Extension Method (PEM) in order to provide the robust protection (Tan, W., et al. 2014). Here, fake sources are introduced dynamically instead of fixed fake sources. The series of fake sources are provided the different fake paths and an impostor is induced farther away from the source if it is entrapped by any of them, which is significantly prolonging the safety duration. The generation of fake sources and path extension are described in below.

5.3.1 Generation of Initial Fake Sources

In the proposed method, different fake sources are generated while the real source initiates the packets transmission to the base station. The PEM method is illustrated in figure 5.1.

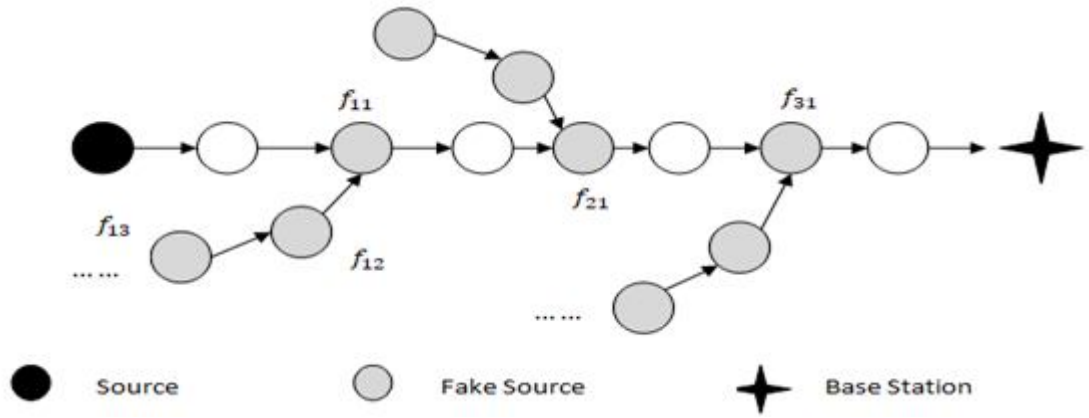


Figure.5.1 Proposed PEM Method

In figure 5.1, the first batch of the fake sources is selected from the nodes on the path between the real source and the base station which is known as initial fake sources. When the monitored agent is occurred in the network, the sensor node closest to it becomes the source. Then, it transmits the client-service packets to the base station regularly through the shortest path which significantly decays the packet delay. This shortest routing path is called as the real path. Once the node on the real path receives the packet from the source, it generates the random number n which is uniformly distributed over the range $[0,1]$. If $n < \gamma$, then the node will acts as an initial fake source. The system parameter γ is used for governing the number of initial fake sources which has the positive correlation with the length of the real path and is neither smaller than the constant number N_α, nor greater than the constant number N_β. The system parameter γ is given as follows,

$$\gamma = \begin{cases} \frac{N_\alpha}{l} & l \le l_\alpha, \\ \gamma_o \quad l_\alpha < l < l_\beta, \quad \gamma_o = \frac{\frac{N_\beta - N_\alpha}{l_\beta - l_\alpha}(l - l_\alpha) + N_\alpha}{l}. & \\ \frac{N_\beta}{l} & l_\beta \le l, \end{cases} \tag{5.1}$$

In equation (5.1), N_α and N_β are the system parameters, l_α and l_β are two thresholds values, and l is the length of the real path from source to base station. Consider the number of initial fake sources on the real path is fs. Then the probability for selecting the correct path to the source for an adversary is follows,

$$P_{correct} = \left(\frac{1}{k+1}\right)^{fs} \tag{5.2}$$

In equation (5.2), fs is smaller than the length of the real path l, and k is the number of fake paths that branch from an initial fake source. The greater value of k provides stronger security protection and consumes more energy. Consider the probability of the sensor node on the real path which is selected as an initial fake source is ρ. Then the expectation of number of initial fake sources on the real path fs is given as,

$$E(fs) = l \times \rho \tag{5.3}$$

5.3.2 Path Extension

Once the initial fake sources are determined, then new fake sources are selected from each of them based on its neighbors without including the two on the real path for transmitting the fake service-packets to it. The routing path of fake service-packets is called as fake path. The fake source transmits the packets simultaneously along with the fake path for a period of δ and then the new fake source is selected from its neighbors, thus longer fake path is generated. In addition, the new fake source cannot be neighbor of any node on the real path otherwise an adversary residing at this new fake source may be pulled back to the real path by packets routing through it. The adversary is escaped from the fake path. The extension of the fake path is terminated if the current fake source cannot select the qualified successor from its neighbors.

The locations of the fake sources are carefully considered and keep distance from the real source. Also, an adversary is assumed that it has an unlimited storage space and the more exquisite attack model is employed. If an impostor is located in the visible region of the real source, then the considered monitored agent is captured. Hence, the fake paths are not passed through the visible region of the real source. The visible region is represented by the system parameter h_v, such as hops

from the real source. It is assured that the fake path will never get into the visible region of the real source and the initial fake sources are not in the visible region either. This is achieved by introducing the limited flooding by means of the source. Nodes which receive this flooding packet are not fake sources.

The fake messaging rate is the most significant while the node is selected as fake source. If the fake source transmits the packets at higher rate than the real source then the impostor will be drawn towards the fake source and vice versa. Therefore, the fake messages are injected into the network at the equivalent rate as the real messages for improving the balance between safety period and energy consumption. However, the fake sources are generated in PEM dynamically and the fake paths are extended longer at the same time duration. Therefore, the fake messages along with the fake path are designed to be transmitted fast at beginning and then the speed is decreased. Faster delivery rate at the beginning is utilized for inducing the adversaries for dropping into the fake paths and slower transmitting rate is utilized for saving energy.

5.3.3 Combination of Fake Paths

Many fake paths are overlapped for providing the length of fake paths and saving the energy. The path combination is shown in figure 5.2.

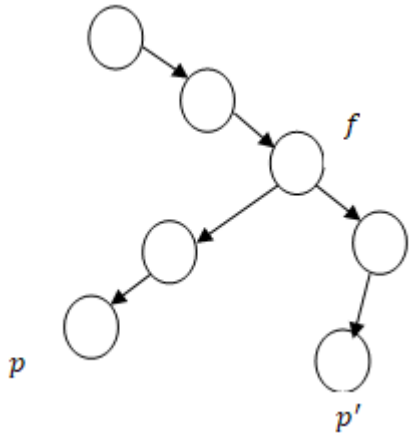


Figure.5.2 Combination of Fake Paths

In figure 5.2, the fake paths p and p' are congregated at the fake source f, after they converged into the single path. While f receives the packet, the packet is delivered to the two fake paths by f. If f is on path p before it joins path p', then the fake messaging rate of f is determined by its location on fake path p. The fake sources are selected from almost all sensors in the network based on fake path convergence strategy. Though, it does not permit that the fake source selected its successor on the same fake paths with itself. Therefore, the fake source f cannot select its successor on path p or p'. If not, it will generate the cycle, which provides an impostor realize that it is entrapped by fake paths by inspecting its recorded locations. The fake path is represented by the initial fake source from which it originates and each fake source memories which paths it is on. When the fake path p' is encountered p at the fake source f, successors of f and itself is modified their memory recording which paths they are on.

Algorithm: AIIMLSDSPS

//Strategy utilized by Sophisticated Impostors

1. An impostor travels from node A to node B after it overhears the message or packet.
2. Initialize the timer by an impostor and set the timeout interval δ'
3. While (keep listening at node B) do

4. If (overhear the message/packet) then
5. Determine which node it is from, Consider C.
6. If (C=A or C=B or historicalLocations.find(C)) then
7. Drop the message or packet
8. Else
9. historicalLocations.push(C)
10. Move to node C
11. Break
12. End if
13. Else if (timer timeout) then
14. Node X=historicalLocations.top()
15. Move to node X
16. Break
17. Else
18. Do nothing
19. End if
20. End while

//Limited flooding by the Source

21. For all sensor nodes to be true do
22. Set the variable canBeFakeSource
23. Generate the message $msg\_h_v = h$ by the source
24. Broadcast the generated message
25. Receive the flooding message by source
26. If ($msg_{h_v} > 0$) then
27. canBeFakeSource=false
28. $msg\_h_v = msg\_h_v - 1$
29. Transmit the modified message
30. Else
31. Drop the received message
32. End if

//Fake Source Discovery Process

33. bool fake_source_discovery_process()
34. //n refers the number of neighbors of the current fake source
35. For i=0 to n do
36. If (neighbor[i] is on the real path) then
37. Continue;

38. End if
39. If (neighbor[i].canBeFakeSource==false) then
40. Continue;
41. End if
42. If (Current fake source is an initial fake source) then
43. new_fake_source = neighbor[i];
44. If (neighbor[i].is_fake_source==true) then
45. Combine the two fake paths;
46. Else
47. neighbor[i].is_fake_source=true;
48. Inform neighbor[i] is new fake source;
49. neighbor[i] transmits the fake messages along the extensive fake path;
50. End if
51. Return true;
52. Else
53. If (neighbor[i] is neighbor of any node on the real path) then
54. Continue;
55. End if
56. If (neighbor[i].is_fake_source==true) then
57. If (neighbor[i] is on the same path with the current source) then
58. Continue;
59. End if
60. new_fake_source = neighbor[i];
61. Combine the two fake paths;
62. Else
63. new_fake_source = neighbor[i];
64. neighbor[i].is_fake_source==true;
65. Inform neighbor[i] is new fake source;
66. neighbor[i] transmits the fake messages along the extensive fake path;
67. End if
68. Return true;
69. End if
70. End for
71. Return false;

//Extension of Fake Paths

72. The current_fake_source transmits the fake event packets through fake_path for time duration δ

73. If (fake_source_discovery_process()==false) then
74. Do nothing
75. Else
76. current_fake_source=new_fake_source
77. fake_path=current_fake_source+fake_path
78. End if

5.4 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 IIMLSDSPS, and AIIMLSDSPS.

5.4.1 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

A). Deadline versus Guarantee Ratio (%)

The comparison of deadline versus guarantee ratio is shown in Table 5.1.

Table.5.1 Comparison of Guarantee Ratio based on Deadline

Deadline	IIMLSDSPS	AIIMLSDSPS
100	50%	53%
300	68%	71%
500	79%	81%
700	93%	95%
900	96%	97.5%

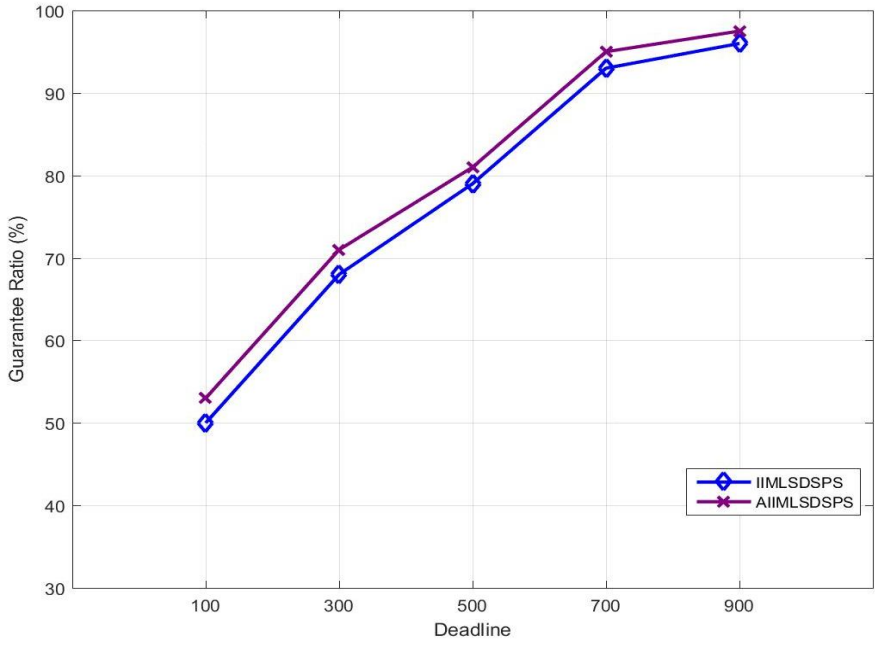


Figure.5.3 Deadline versus Guarantee Ratio (%)

Figure 5.3 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 algorithms.

B). Arrival Rate versus Guarantee Ratio (%)

The comparison of arrival rate versus guarantee ratio is shown in Table 5.2.

Table.5.2 Comparison of Guarantee Ratio based on Arrival Rate

Arrival Rate	IIMLSDSPS	AIIMLSDSPS
10	76%	71%
30	59%	52%
50	45%	38%
70	30%	24%
90	24%	18%

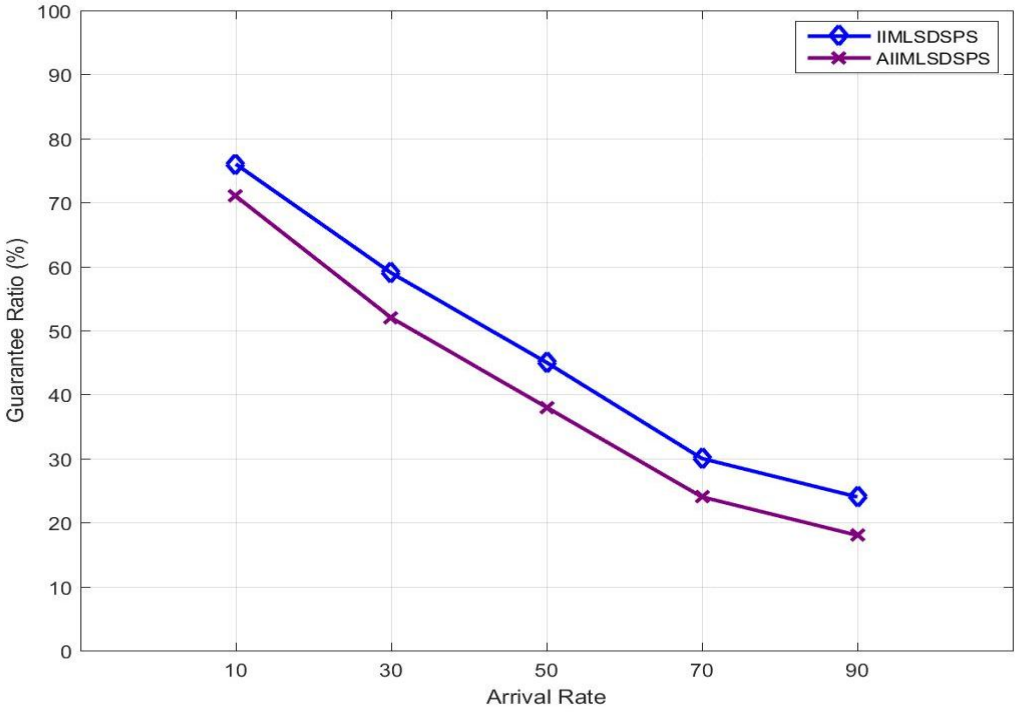


Figure.5.4 Arrival Rate versus Guarantee Ratio (%)

Figure 5.4 shows that the result of guarantee ratio comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the guarantee ratio (%) is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Then, the packets arriving later increases the probability of missing deadlines. Thus, the guarantee ratio is decreased. The proposed AIIMLSDSPS has higher guarantee ratio that is AIIMLSDSPS has the ability for enhancing the schedulability than the other algorithms while the system workload is high.

5.4.2 Average Security Level

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

A). Deadline versus Average Security Level

The comparison of deadline versus average security level is shown in Table 5.3.

Table.5.3 Comparison of Average Security Level based on Deadline

Deadline	IIMLSDSPS	AIIMLSDSPS
100	4.0	4.3
300	4.4	4.7
500	4.7	5.1
700	5.2	5.5
900	5.6	5.9

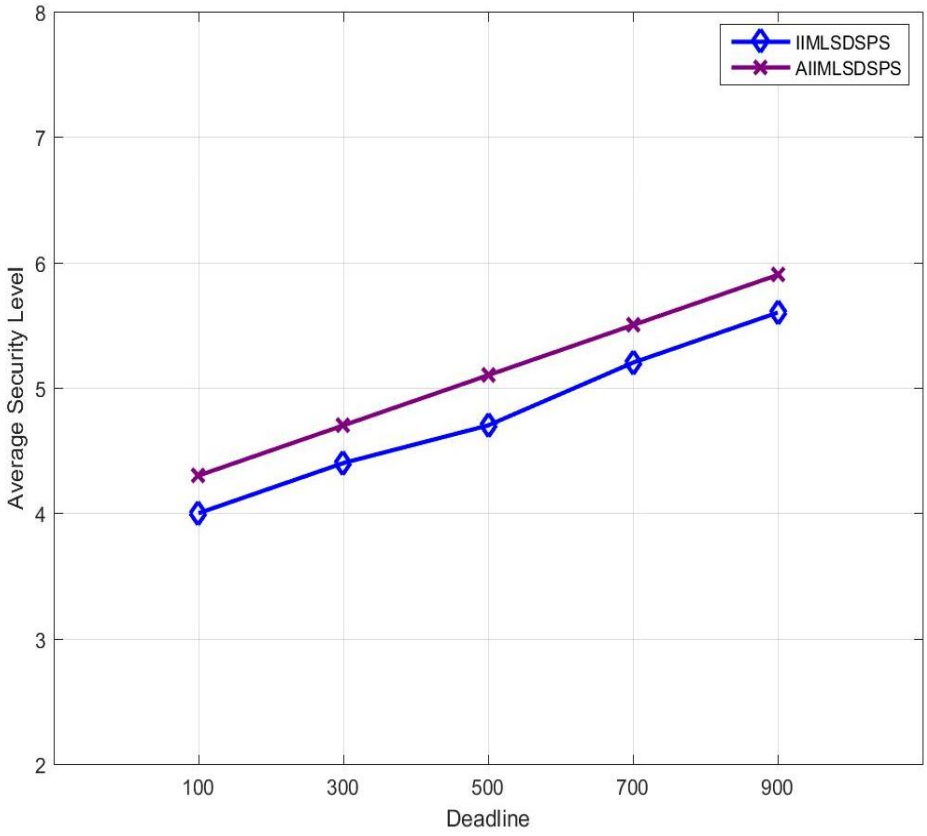


Figure.5.5 Deadline versus Average Security Level

Figure 5.5 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 algorithms by satisfying the user's requirements.

B). Arrival Rate versus Average Security Level

The comparison of arrival rate versus average security level is shown in Table 5.4.

Table.5.4 Comparison of Average Security Level based on Arrival Rate

Arrival Rate	IIMLSDSPS	AIIMLSDSPS
10	3.5	3.1
30	2.9	2.7
50	2.5	2.2
70	2.1	1.7
90	1.6	1.1

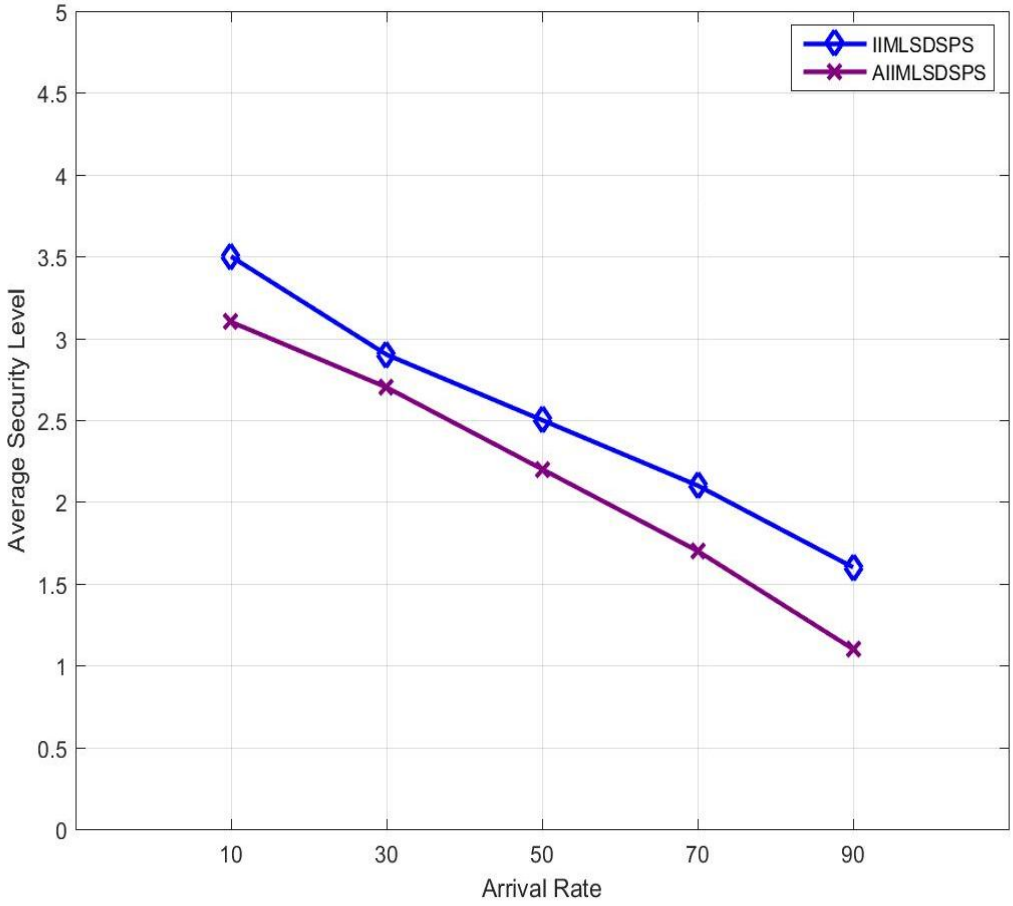


Figure.5.6 Arrival rate versus Average Security Level

Figure 5.6 shows that the result of average security level comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the average security level is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Therefore, the security level of packets waiting in queue is degraded for improving the schedulability. Thus, the average security level is decreased. The proposed AIIMLSDSPS has higher average security level than the other algorithms by satisfying the security requirements of the users while the system workload is high.

5.4.3 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,

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

The comparison of packet delivery ratio is shown in Table 5.5.

Table.5.5 Comparison of Packet Delivery Ratio

Number of Nodes	IIMLSDSPS	AIIMLSDSPS
20	0.61	0.65
40	0.66	0.71
60	0.72	0.78
80	0.79	0.85
100	0.85	0.91

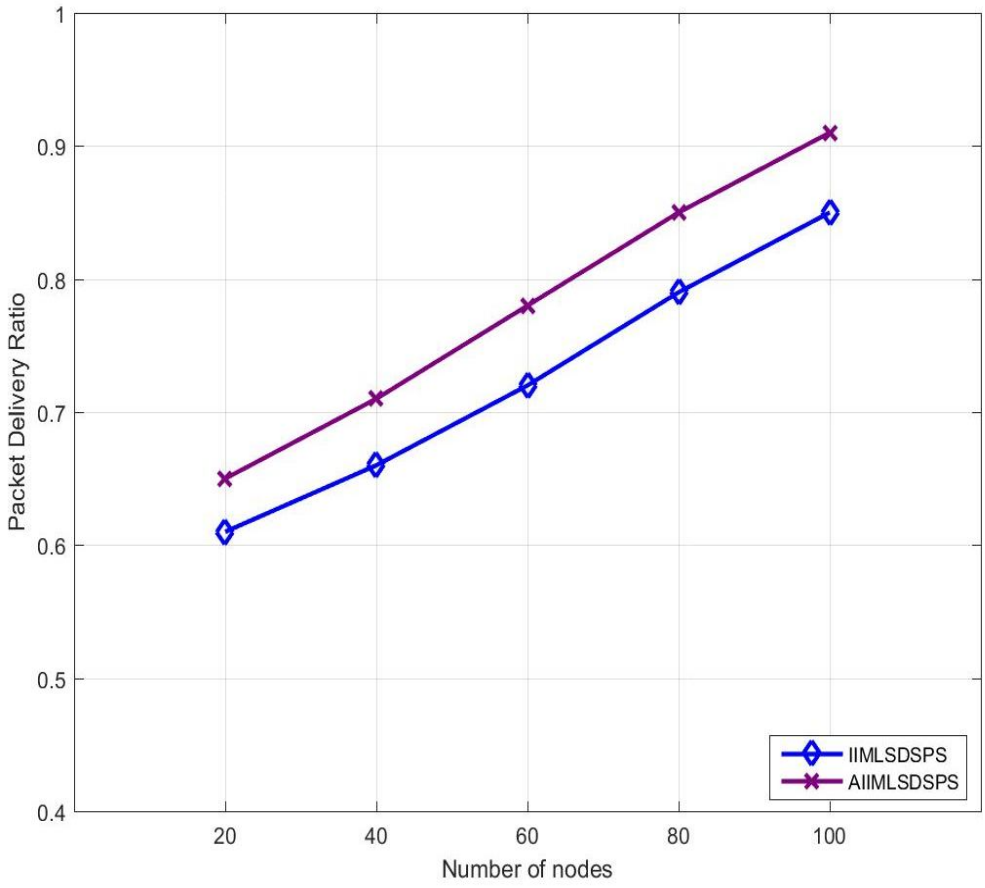


Figure.5.7 Number of Nodes versus Packet Delivery Ratio

Figure 5.7 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 algorithms.

5.4.4 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,

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

The comparison of end-to-end delay is shown in Table 5.6.

Table.5.6 Comparison of End-to-End Delay (seconds)

Number of Nodes	IIMLSDSPS	AIIMLSDSPS
20	31	28
40	36	32
60	41	39
80	47	43
100	52	48

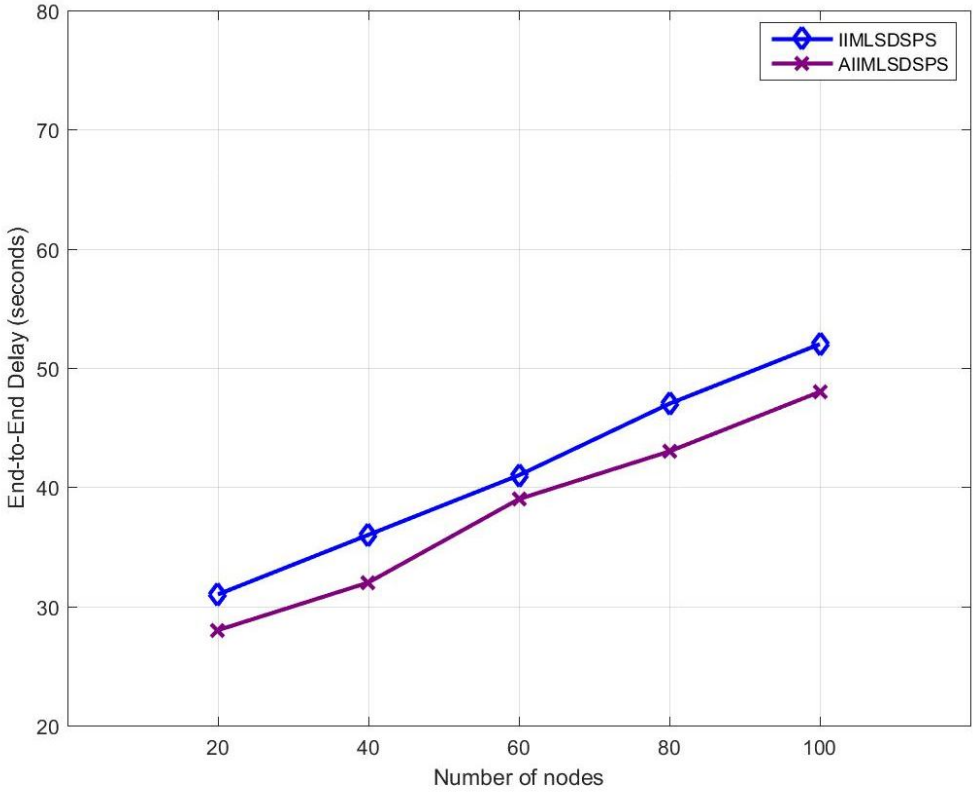
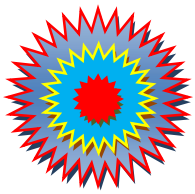


Figure.5.8 Number of Nodes versus End-to-End Delay (Seconds)

Figure 5.8 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 algorithms.

5.5 CHAPTER SUMMARY

In this chapter, 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 algorithm performs better than the IIMLSDSPS based algorithm. The experimental results are proved that the proposed AIIMLSDSPS has better performance than the other algorithms.



CHAPTER - 6

ANONYMITY-BASED FLEXIBLE ROUTING PROTOCOL WITH INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (AFIIMLSDSPS)

ANONYMITY-BASED FLEXIBLE ROUTING PROTOCOL WITH INTRA-INTER AND MULTIPLE LAYER SERVICE DEPENDENT SECURITY-AWARE PACKET SCHEDULING ALGORITHM (AFIIMLSDSPS)

This chapter provides the detailed information about the anonymity based flexible routing protocol with intra-inter and multiple layer service-level dependent security-aware packet scheduling algorithm in mobile ad-hoc networks for reducing the energy consumption due to path extension process in security-aware packet scheduling algorithm based on the anonymity of source-location. This chapter describes how routing protocol reduces the energy consumption of path discovery and extension process in mobile ad-hoc networks and enhancing the packet level security.

6.1 INTRODUCTION

Over the past few years, the coupling of advanced techniques and distributed computing paradigms were introduced in wireless communication networks. These are expected that the broad spectrum of remote-sensing applications ranging from collecting the data with concerning the highway traffic to monitoring cardiologic data for at risk heart patients since the effectiveness of energy-efficient sensors. However, due to the open nature of sensor technology, adversaries are having the ability to easily gain the access to communication. These privacy issues are removed by source location privacy based distributed anonymity algorithm. These location-privacy techniques are particularly constructed by using network security methods such as the anonymity provided by the additional communication, memory and communicational overhead which are unaffordable for utilization of resource-constrained environments. As a result, full-fledged privacy solutions are not suitable and light-weight, resource-efficient alternatives must be explored.

Therefore, this issue is removed by the proposed anonymity-based source location privacy algorithm which is based on the fake source discovery process. However, the energy consumption is high due to the flooding process and path extension process. Hence, the new routing technique is proposed in order to reduce the energy consumption of flooding process in mobile ad-hoc networks. In addition, a concrete metric is provided for measuring the location privacy in MANET by using the privacy measure called as privacy period. The issue of energy consumption is reduced by routing protocol named phantom routing which is flexible and having the capability for preventing the adversaries from tracking the location of source. In this chapter, an anonymity-based flexible routing protocol with intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is explained in brief.

6.2 NETWORK AND ADVERSARY MODEL

In this section, anonymity-based flexible routing protocol with intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is explained. The AFIIMLSDSPS algorithm is developed by considering the phantom routing protocol with source-location anonymity. After scheduling the packets by using AIIMLSDSPS which is explained briefly in Chapter 5, flexible routing protocol is provided for transmitting the packets from source to destination securely with less energy consumption. The network and adversary model are described in below.

6.2.1 Network Model

The proposed network consists of the source node, phantom node, base station, few fake source nodes and large number of homogeneous sensor node which is randomly deployed for monitoring the quality such as Panda in Panda Hunter game (Ozturk, C., et al. 2004). The source node, phantom node and fake source nodes are also having the similar capabilities like other homogeneous nodes. The source node is defined as the node which senses the event such as the presence of panda. The phantom node is referred as the node which is used for forwarding the packets to the base station on behalf of source node. The fake source nodes are utilized for generating the fake packets which are identical to the real packets generated by the real source node.

6.2.2 Adversary Model

The adversaries are trying to find the location of the source node as passive attacker and it is considered for having the following characteristics.

- The adversary identifies the location of the base station and determines the location of the source node from the instance of the packets it overhears. Initially, the adversary is started from the base station and hearing radius of an adversary is identical to the transmission radius of the nodes. Consequently, the adversary is used for monitoring only the traffic area around the node and not the entire network.
- The adversary is resource-rich. It is travelled from one sensor to another physically and has an unlimited number of energy. The adversary does not interfere with the proper functioning of the network like destroying the sensor nodes or adjusting the packets for not triggering the other security methods. It can remember all packets it has overhear and decide if the packet is new or it is the similar with another it has already overheard. Since, similar packets are following the different paths towards the destination and utilizing the similar nodes in different time slots.

6.2.3 Panda-Hunter Game

In Panda-Hunter game, the large array of panda-detection sensor nodes is deployed by using the Save-The-Panda Organization for monitoring the vast habitat for pandas. Once the panda is observed, the corresponding source node will provide observations and report the data regularly to the sink node through multi-hop routing techniques. The game also having the hunter as an adversary for trying to find the panda by back-tracing the routing path until it reaches the source. Subsequently, the privacy-cautious routing protocol is used for preventing the hunter from locating the source during the data delivery to the sink.

The major objective for the operator of the sensor network is security of the panda. Therefore, keeping the location of the source of the sensor reading an unknown to the hunter is the major privacy target. Hence, in this game, the panda pops up at the random location and stays there until it is captured by the hunter. Once the hunter is nearly to the panda such that within δ hops from the panda, the panda is assumed to be captured and the game is terminated. The source generates the new packet each T periods until the simulation is ended. The packets are having the identical length and encrypted and the hunter cannot break the encryption process.

The hunter is assumed to as mobile with unlimited number of energy and limited number of memory. The hunter is initiated at the sink's location where it is assured that sensor packets should ultimately arrive. The hunter is in the listening or receiving mode regularly. The node among its neighborhood is identified after the initial packet is heard by the hunter and it is travelled to the transmitting sensor node. Once the new packet is heard, the hunter provides another move to its sender. If no new messages are heard within the certain time period T_{listen}, the hunter is informed that the current node is not on the routing path and must return to the former location.

In the proposed system, three major performance metrics are measured in order to develop the routing strategies such as follows:

- Privacy conservation level or safety period which is measured by the amount of new packets that the source has transmitted before the panda is captured.
- Energy efficiency which is measured by the amount of packets that transmitted by the entire network.
- The quality of delivery which is measured by delivery latency and delivery ratio.

6.3 PHANTOM ROUTING PROTOCOL

The main objective of the phantom routing protocol (Gu, C., et al. 2015) is enticing the hunter away from the source towards the phantom source (Kamat, P., et al. 2005). In phantom routing, two phases are provided for delivering the packets or messages such as,

- Random walk phase which is either pure random walk or directed walk and refers to direct the message to the phantom source.
- Subsequent flooding or single-path routing phase refers to deliver the message to the sink.

When the source node sends the message, the message is broadcasted in the random manner for the total number of h_{walk} hops. In phantom flooding, after h_{walk} hops the message is flooded by using probabilistic flooding. In phantom single-path routing, after h_{walk} hops the message transmission is switched to single-path routing.

The ability of phantom technique is improving the privacy based on the ability of the random walk for locating the phantom source at the location far from the real source node. Consider the network of sensors N is arrayed on the two-dimensional integer grid with the source and asset A is located at $(0,0)$. Assume the random walk selects randomly from moving north, south, east or west such as from $\{(1,0),(-1,0),(0,1),(0,-1)\}$ along with equivalent probability and that the random walk can visit the node more than once. The probability is estimated that after h_{walk} hops, the phantom source is within the distance $d < h_{walk}$ of the real source node. The mobility consists of h_{walk} steps, wherein each step is an independent random variable X_j with vector values such as $\{(1,0),(-1,0),(0,1),(0,-1)\}$. After h_{walk} steps, the location of the random walk $D_{h_{walk}}$ is given as,

$$D_{h_{walk}} = X_1 + X_2 + \cdots + X_{h_{walk}} \quad (6.1)$$

Then, by using the central limit theorem, $D_{h_{walk}}/\sqrt{h_{walk}}$ converges in distribution to the bivar Gaussian with mean $\mu = (0,0)$ and covariance matrix $\left(1/2\right) I$. As result, $D_{h_{walk}} \sim N\left(\mu, \frac{h_{walk}}{2} I\right)$ Consider $B = B(\mu, d)$ is the ball of radius d centered at (0, The asymptotic probability of the phantom source's location $D_{h_{walk}}$ is within the distance d of real source node, after h random walk steps is given as,

$$P(D \in B) = \frac{1}{h\pi} \int_B e^{-\frac{(x^2+y^2)}{h_{walk}}} dxdy$$

$$= \frac{1}{h\pi} \int_0^d \int_0^{2\pi} e^{-r^2/h_{walk}} r \, d\theta \, dr$$

$$P(D \in B) = 1 - e^{-d^2/h_{walk}} \quad (6.2)$$

By using the equation (6.2), the likelihood of the phantom's source is examined within 20% of h_{walk} from the real source node after h_{walk} steps such as $d = h_{walk}/5$. The probability is denoted as $p = 1 - e^{-h_{walk}/25}$. When h_{walk} is increased, the probability tend to 1 which is indicating that the amount of energy consumption moving the message around and remain clustered around the real source's location. Thus, the purely random walk is inefficient at providing the phantom source far from the real source. Hence, for reasonable h_{walk} values the location-privacy is not significantly increased. In order to avoid random walks cancelling each other, the bias is introduced into the walking process.

Therefore, directed walk is proposed for providing the source-location privacy. The directed walk is achieved based on the two approaches such as sector-based directed random walk and hop-based directed random walk.

- **Sector-based Directed Random Walk:** In this approach, each sensor node should have the ability to partition the 2-dimensional plane into two half planes. For example, once the network is deployed then the west-most node is marked. Consider that node is initiated the flood all over network. For a random node i in the network, if it transmits the packet to its neighbor j before it receives the identical packet from j, then it is concluded that j is to the east; otherwise j is to the west. By using this method, each node can partition its neighbors into two sets such as S_0 and S_1. Before the source initiates the directed random walk, it flips the coin and determines whether it is going to use S_0 or S_1. Then, within the first h_{walk} hops, each node that receives the packet randomly selects the neighbor node from the selected set of that packet.
- **Hop-based Directed Random Walk:** In this approach, every node should know about the hop count between itself and the sink. This is achieved by the sink initiating the flood throughout the network. After the node receives the packet, it increases the hop count and passes the packet to its neighbors. After the flood phase, neighbors update each other with their own hop counts. Consequently, node i can partition its neighbors into two sets such as S_0 and S_1, in which S_0 includes the all neighbors whose hop counts are lesser than or equal to i^{th} hop count and S_1 includes the all neighbors with larger hop count. In the sector-based directed random walk, each new message is selected a random set after the two sets are formed and each node in the walk is selected the random neighbor from its corresponding set.

The safety period is increased by the phantom technique since each message may take the different shortest path for reaching any node within the network. Therefore, after the adversary hears the message i, it may take long time before it receives $i + 1$. While it receives message $i + 1$, the immediate sender of that message may provide the adversary farther away from the source. The privacy protection is improved by both phantom flooding and phantom single-path routing since the path diversity between different messages. The energy consumed by the phantom routing is governed by two factors such as walk distance h_{walk} and type of flooding or single-path routing phase used.

The random walk phase automatically introduces the h_{walk} transmissions which are not present in the probability cases. However, the predominant energy utilization for flooding-based techniques under flooding phase and usually, $h_{walk} \ll n$. Therefore, the increased energy consumption is negligible. Moreover, for single-path routing mechanisms, it introduces at most $2h_{walk}$ extra transmissions to the shortest path between the source and the sink, and the total energy consumption of this approach is minimized.

Algorithm: AFIIMLSDSPS

//Strategy utilized by Sophisticated Impostors

1. An impostor travels from node A to node B after it overhears the message or packet.
2. Initialize the timer by an impostor and set the timeout interval δ'
3. While (keep listening at node B) do
4. If (overhear the message/packet) then
5. Determine which node it is from, Consider C.
6. If (C=A or C=B or historicalLocations.find(C)) then
7. Drop the message or packet
8. Else
9. historicalLocations.push(C)
10. Move to node C

11. Break
12. End if
13. Else if (timer timeout) then
14. Node X=historicalLocations.top()
15. Move to node X
16. Break
17. Else
18. Do nothing
19. End if
20. End while

//Phantom flooding for patient adversary

21. next_location=sink;
22. While (next_location!=source) do
23. Listen(next_location);
24. msg=ReceiveMessage();
25. If (IsNewMessage(msg)) then
26. next_location-CalculateImmediateSender(msg);
27. MoveTo(next_location);
28. End
29. End

//Phantom flooding for cautious adversary

30. prev_location=sink;
31. next-location-sink;
32. While (next_location!=source) do
33. reason=TimedListen(next_location, interval);
34. If (reason==MSG_ARRIVAL) then
35. msg=ReceiveMessage();
36. If (IsNewMessage(msg)) then
37. next_location=CalculateImmediateSender(msg);
38. MoveTo(next_location);
39. End if
40. Else
41. next_location=prev_location;
42. prev_location=LookUpPrevLocation(prev_location);
43. MoveTo(next_location);
44. End if
45. End

6.4 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 AIIMLSDSPS, and AFIIMLSDSPS.

6.4.1 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

A). Deadline versus Guarantee Ratio (%)

The comparison of deadline versus guarantee ratio is shown in Table 6.1.

Table.6.1 Comparison of Guarantee Ratio based on Deadline

Deadline	AIIMLSDSPS	AFIIMLSDSPS
100	53%	56%
300	71%	73%
500	81%	84%
700	95%	97%
900	97.5%	99%

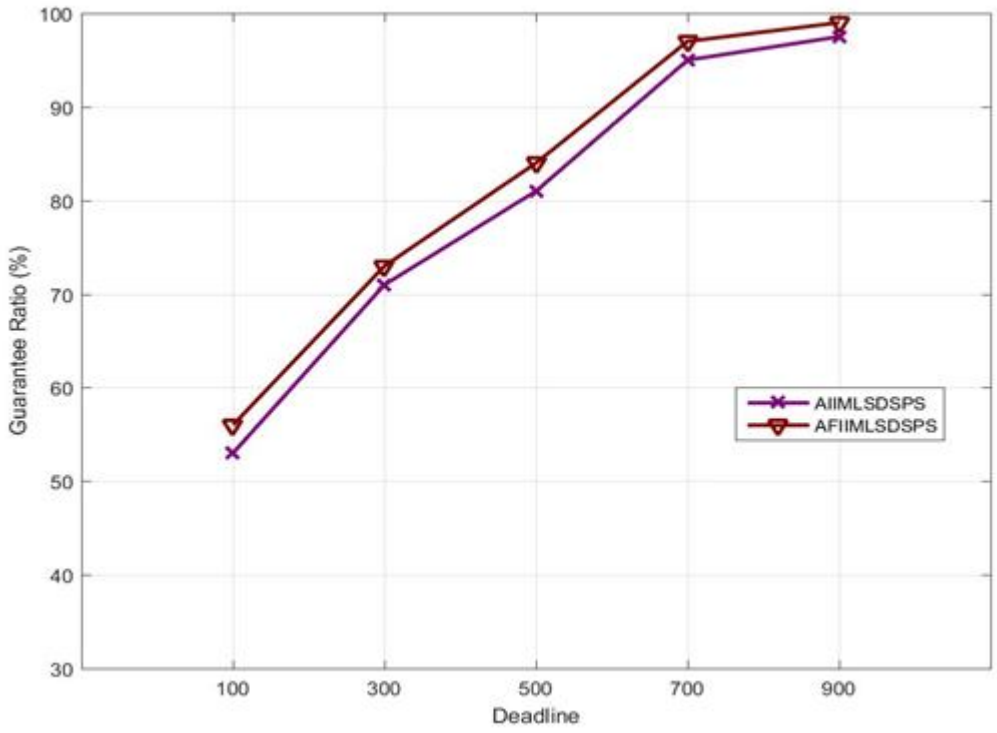


Figure.6.1 Deadline versus Guarantee Ratio (%)

Figure 6.1 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 AFIIMLSDSPS has higher guarantee ratio than the other algorithms.

B). Arrival Rate versus Guarantee Ratio (%)

The comparison of arrival rate versus guarantee ratio is shown in Table 6.2.

Table.6.2 Comparison of Guarantee Ratio based on Arrival Rate

Arrival Rate	AIIMLSDSPS	AFIIMLSDSPS
10	71%	65%
30	52%	46%
50	38%	31%
70	24%	17%
90	18%	12%

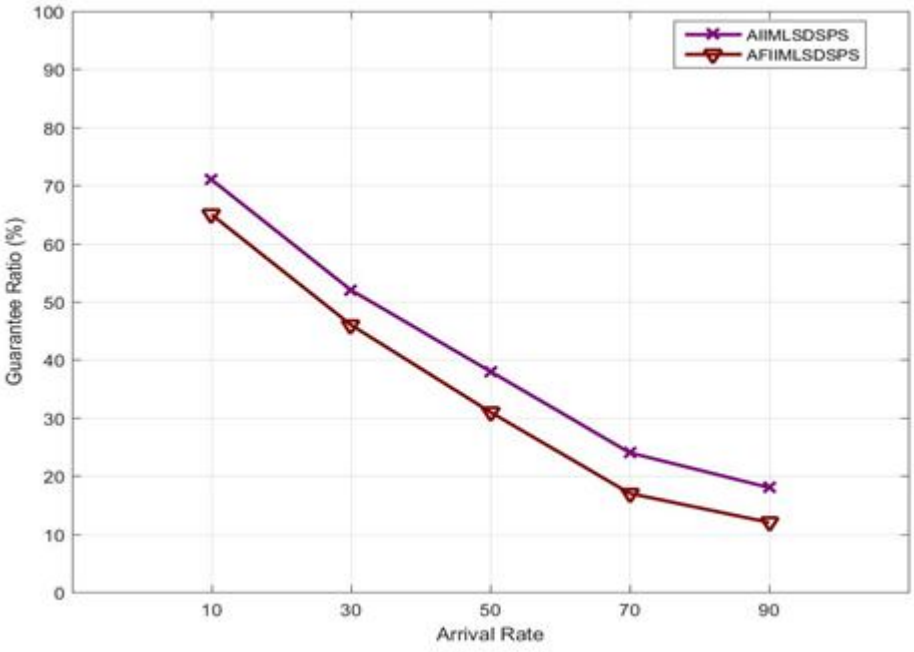


Figure.6.2 Arrival Rate versus Guarantee Ratio (%)

Figure 6.2 shows that the result of guarantee ratio comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the guarantee ratio (%) is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Then, the packets arriving later increases the probability of missing deadlines. Thus, the guarantee ratio is decreased. The proposed AFIIMLSDSPS has higher guarantee ratio that is AFIIMLSDSPS has the ability for enhancing the schedulability than the other algorithms while the system workload is high.

6.4.2 Average Security Level

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

A). Deadline versus Average Security Level

The comparison of deadline versus average security level is shown in Table 6.3.

Table.6.3 Comparison of Average Security Level based on Deadline

Deadline	AIIMLSDSPS	AFIIMLSDSPS
100	4.3	4.7
300	4.7	5.2
500	5.1	5.8
700	5.5	6.2
900	5.9	6.7

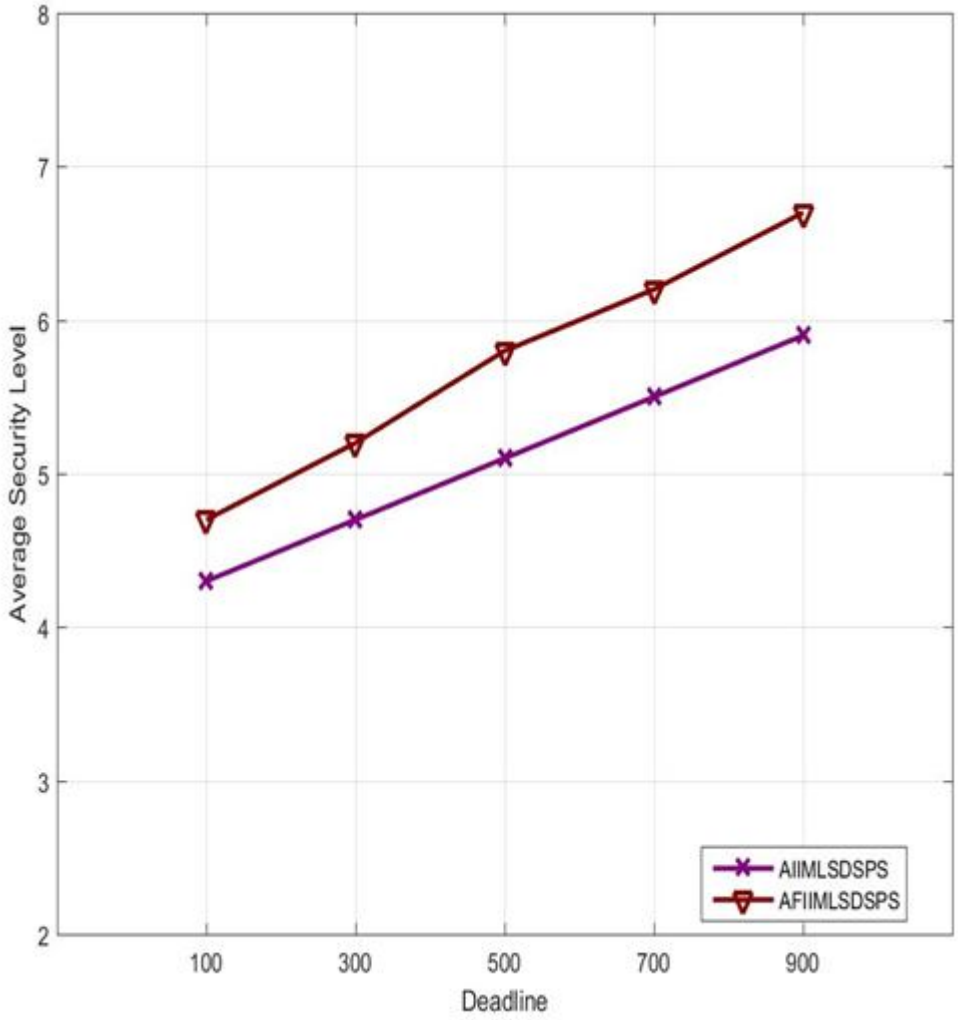


Figure.6.3 Deadline versus Average Security Level

Figure 6.3 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 AIIMLSDSPS 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 AFIIMLSDSPS has higher security levels than the other algorithms by satisfying the user's requirements.

B). Arrival Rate versus Average Security Level

The comparison of arrival rate versus average security level is shown in Table 6.4.

Table.6.4 Comparison of Average Security Level based on Arrival Rate

Arrival Rate	AIIMLSDSPS	AFIIMLSDSPS
10	3.1	2.8
30	2.7	2.3
50	2.2	1.6
70	1.7	1.0
90	1.1	0.4

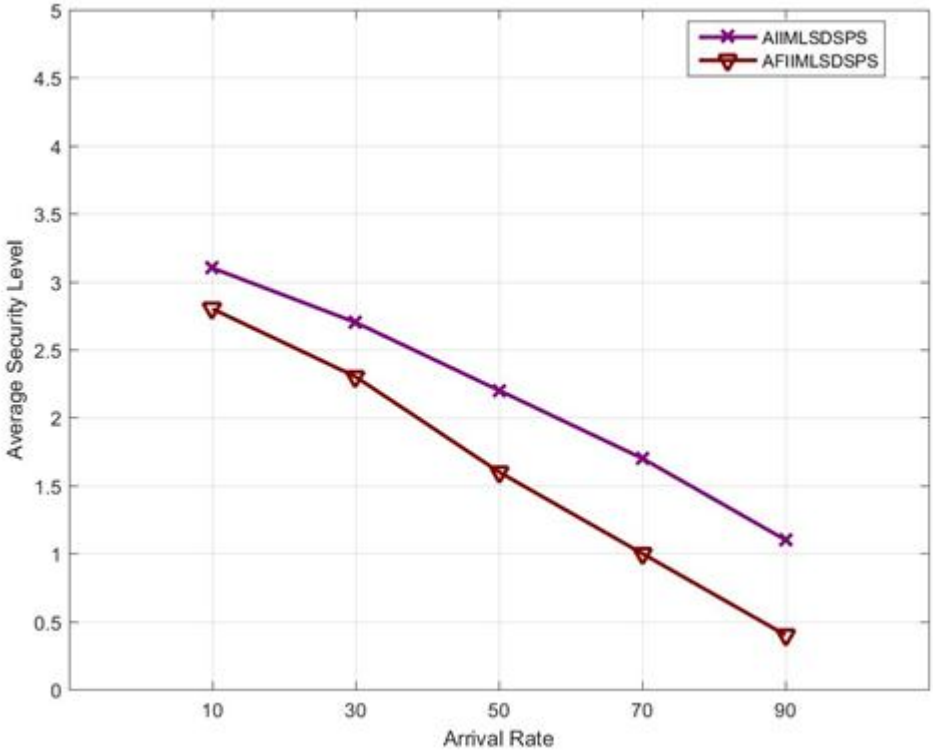


Figure.6.4 Arrival rate versus Average Security Level

Figure 6.4 shows that the result of average security level comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the average security level is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Therefore, the security level of packets waiting in queue is degraded for improving the schedulability. Thus, the average security level is decreased. The proposed AFIIMLSDSPS has higher average security level than the other algorithms by satisfying the security requirements of the users while the system workload is high.

6.4.3 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,

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

The comparison of packet delivery ratio is shown in Table 6.5.

Table.6.5 Comparison of Packet Delivery Ratio

Number of Nodes	AIIMLSDSPS	AFIIMLSDSPS
20	0.65	0.70
40	0.71	0.77
60	0.78	0.83
80	0.85	0.89
100	0.91	0.95

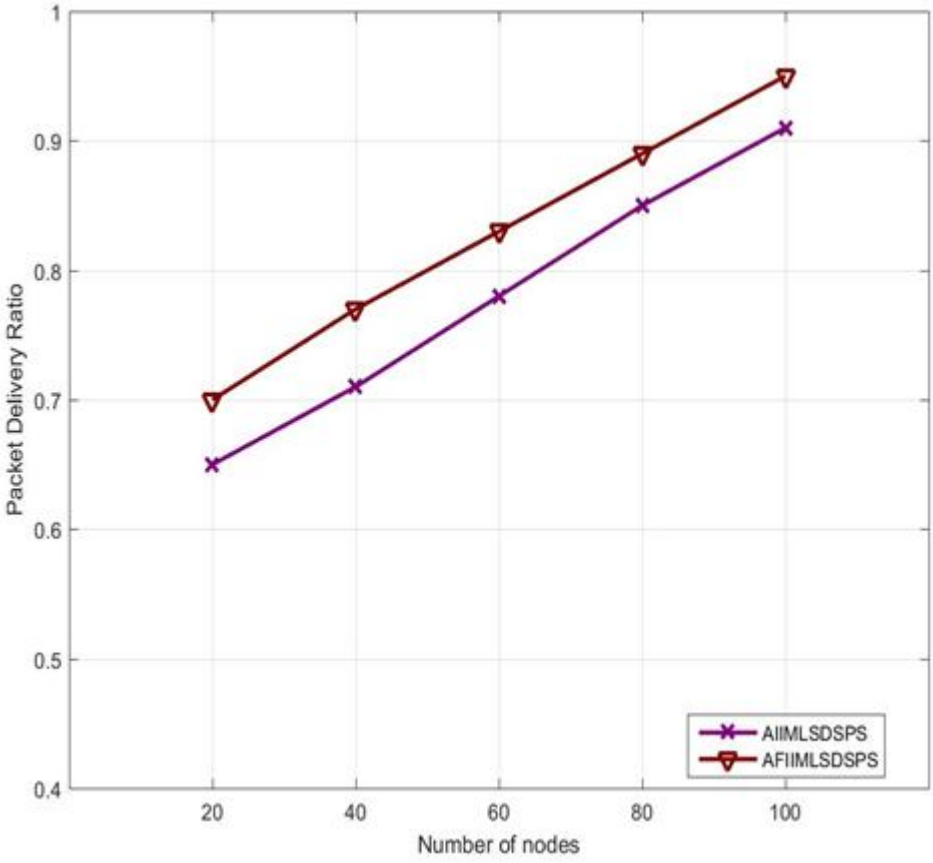


Figure.6.5 Number of Nodes versus Packet Delivery Ratio

Figure 6.5 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 AFIIMLSDSPS has higher packet delivery ratio than the other algorithms.

6.4.4 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,

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

The comparison of end-to-end delay is shown in Table 6.6.

Table.6.6 Comparison of End-to-End Delay (seconds)

Number of Nodes	AIIMLSDSPS	AFIIMLSDSPS
20	28	24
40	32	29
60	39	33
80	43	38
100	48	42

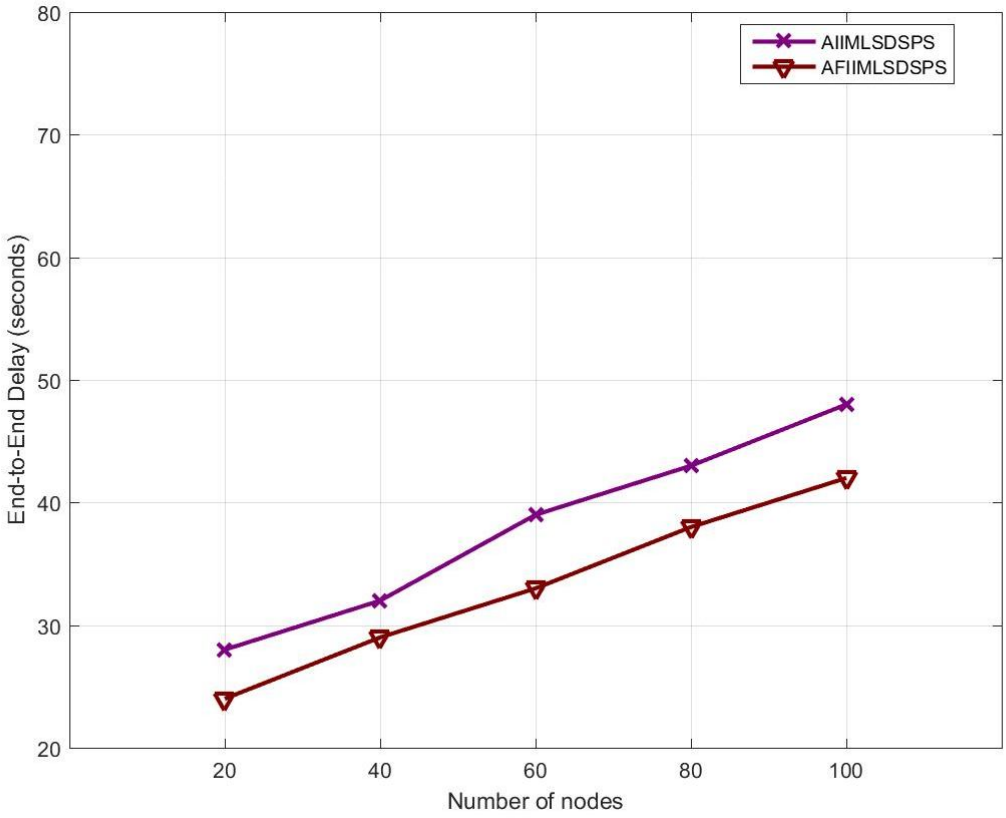
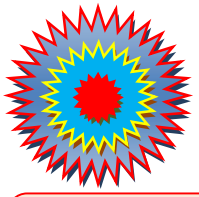


Figure.6.6 Number of Nodes versus End-to-End Delay (Seconds)

Figure 6.6 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 AFIIMLSDSPS has less end-to-end delay than the other algorithms.

6.5 CHAPTER SUMMARY

In this chapter, the issues of the energy consumption during flooding process in mobile ad-hoc networks by using security-aware packet scheduling algorithm are considered. These issues are removed by introducing the flexible routing protocol named phantom routing protocol which is integrated with the anonymity-based intra-inter and multiple-layer service-dependence discovery method. The phantom routing protocol is provided for flooding process based on the directed walk along with the random direction followed by the routing from the phantom source to the sink. The proposed phantom flooding is utilized for distributing the messages to different locations of the network. Thus, the attacker cannot receive the messages for tracking the real source node. Hence, the proposed AFIIMLSDSPS algorithm performs better than the AIIMLSDSPS based algorithm. The experimental results are proved that the proposed AFIIMLSDSPS has better performance than the other algorithms.



CHAPTER - 7

RESULTS AND DISCUSSION

RESULTS AND DISCUSSION

This chapter provides the detailed information about the overall performance of different proposed approaches such as ISAPS, ISDSPS, IISDSPS, IIMLSDSPS, AIIMLSDSPS, and AFIIMLSDSPS.

7.1 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, IISDSPS, IIMLSDSPS, AIIMLSDSPS, and AFIIMLSDSPS

7.2 Guarantee Ratio (%)

The Guarantee Ratio (GR) is computed as follows,

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

A). Deadline versus Guarantee Ratio (%)

The comparison of deadline versus guarantee ratio is shown in Table 7.1.

Table.7.1 Comparison of Guarantee Ratio based on Deadline

Deadline	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
100	41%	43%	46%	50%	53%	56%
300	58%	62%	65%	68%	71%	73%
500	70%	73%	76%	79%	81%	84%
700	85%	88%	91%	93%	95%	97%
900	90%	92%	94%	96%	97.5%	99%

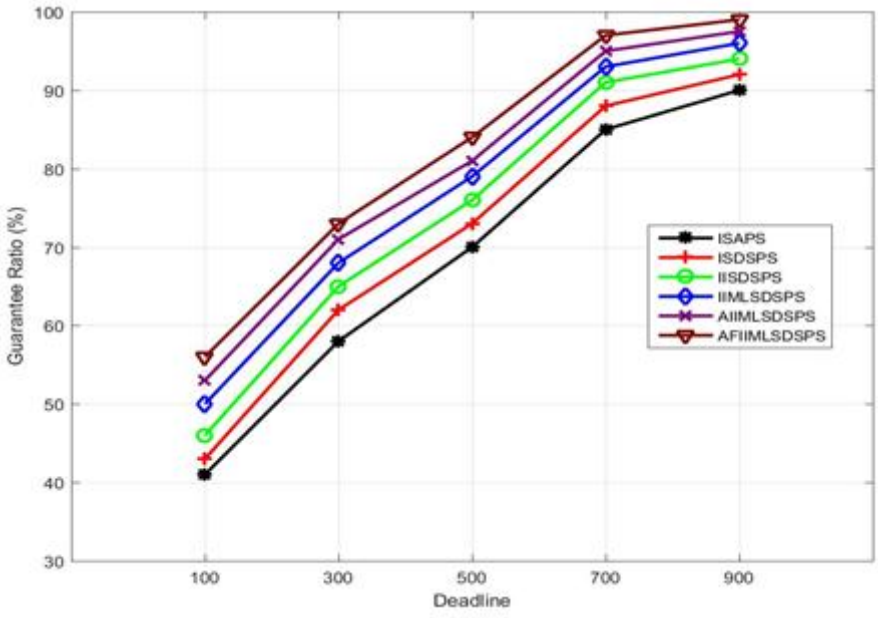


Figure.7.1 Deadline versus Guarantee Ratio (%)

Figure 7.1 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 AFIIMLSDSPS has higher guarantee ratio than the other algorithms.

B). Arrival Rate versus Guarantee Ratio (%)

The comparison of arrival rate versus guarantee ratio is shown in Table 7.2.

Table.7.2 Comparison of Guarantee Ratio based on Arrival Rate

Arrival Rate	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
10	95%	88%	81%	76%	71%	65%
30	81%	72%	64%	59%	52%	46%
50	70%	59%	51%	45%	38%	31%
70	58%	43%	36%	30%	24%	17%
90	41%	38%	30%	24%	18%	12%

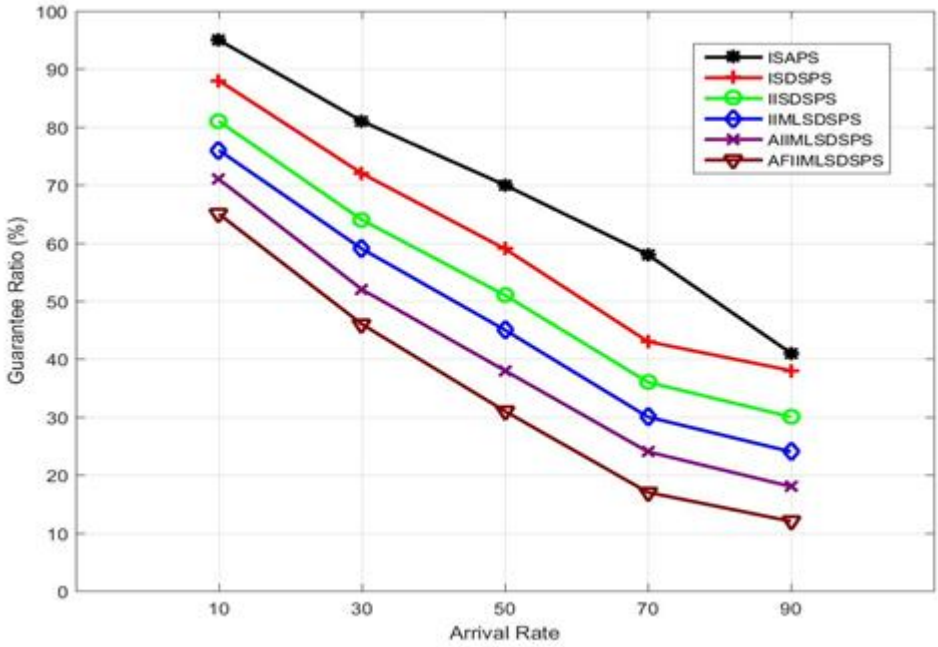


Figure.7.2 Arrival Rate versus Guarantee Ratio (%)

Figure 7.2 shows that the result of guarantee ratio comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the guarantee ratio (%) is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Then, the packets arriving later increases the probability of missing deadlines. Thus, the guarantee ratio is decreased. The proposed AFIIMLSDSPS has higher guarantee ratio that is AFIIMLSDSPS has the ability for enhancing the schedulability than the other algorithms while the system workload is high.

7.3 Average Security Level

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

A). Deadline versus Average Security Level

The comparison of deadline versus average security level is shown in Table 7.3.

Table.7.3 Comparison of Average Security Level based on Deadline

Deadline	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
100	2.7	3.2	3.6	4.0	4.3	4.7
300	3.1	3.7	4.1	4.4	4.7	5.2
500	3.5	4.1	4.6	4.7	5.1	5.8
700	3.8	4.5	5.0	5.2	5.5	6.2
900	4.1	4.8	5.3	5.6	5.9	6.7

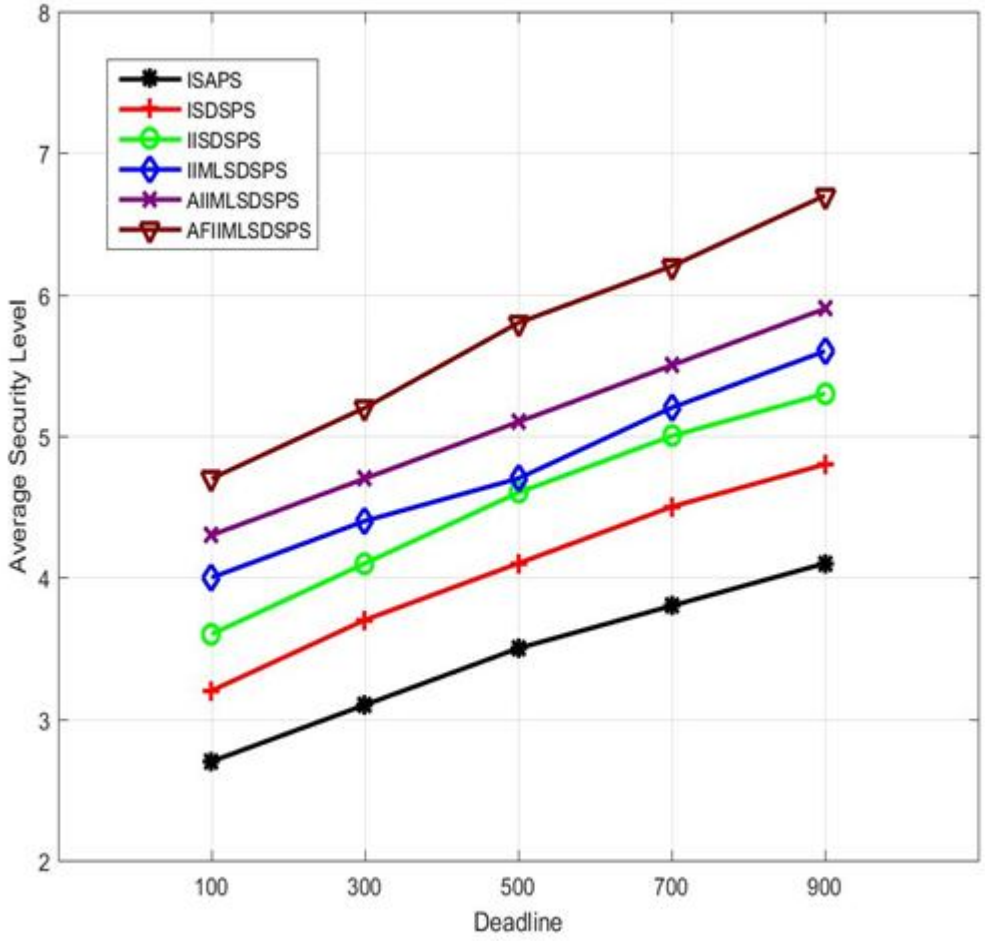


Figure.7.3 Deadline versus Average Security Level

Figure 7.3 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 AFIIMLSDSPS has higher security levels than the other algorithms by satisfying the user's requirements.

B). Arrival Rate versus Average Security Level

The comparison of arrival rate versus average security level is shown in Table 7.4.

Table.7.4 Comparison of Average Security Level based on Arrival Rate

Arrival Rate	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
10	4.7	4.4	3.9	3.5	3.1	2.8
30	4.2	4.0	3.4	2.9	2.7	2.3
50	3.7	3.6	3.0	2.5	2.2	1.6
70	3.4	3.2	2.6	2.1	1.7	1.0
90	2.9	2.5	2.2	1.6	1.1	0.4

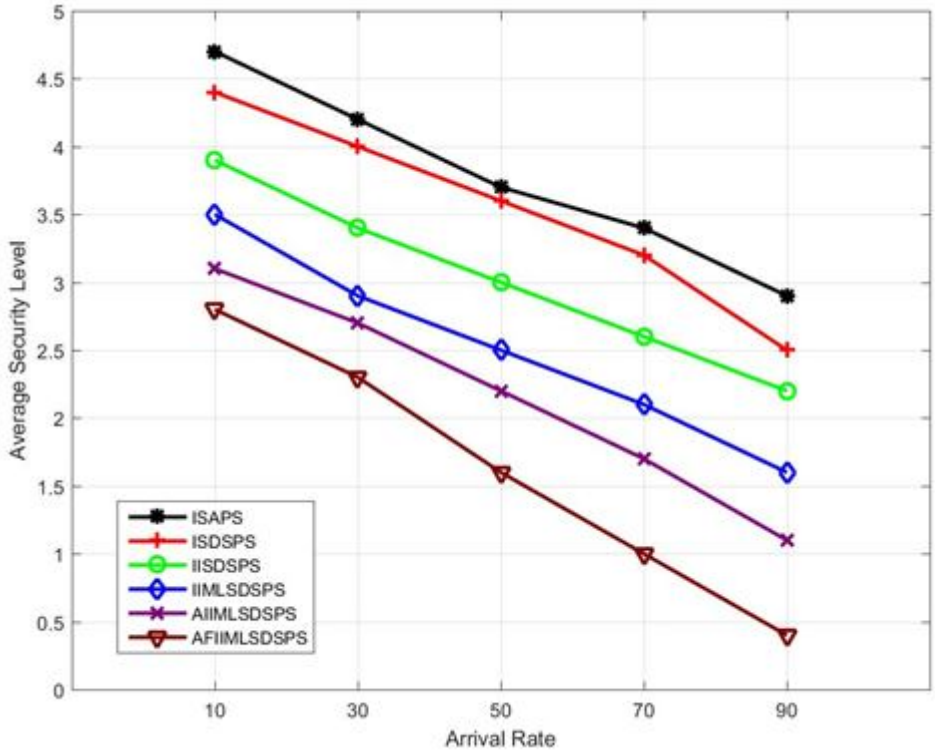


Figure.7.4 Arrival rate versus Average Security Level

Figure 7.4 shows that the result of average security level comparison in terms of arrival rate of packets. From the graph, it is proved that, if the arrival rate of packets increases then the average security level is decreases. The major reason for this result is that when arrival rate of packets is increasing the system workload is also increasing which provides more number of packets wait in the accepted queue. Therefore, the security level of packets waiting in queue is degraded for improving the schedulability. Thus, the average security level is decreased. The proposed AFIIMLSDSPS has higher average security level than the other algorithms by satisfying the security requirements of the users while the system workload is high.

7.4 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,

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

The comparison of packet delivery ratio is shown in Table 7.5.

Table.7.5 Comparison of Packet Delivery Ratio

Number of Nodes	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
20	0.48	0.52	0.57	0.61	0.65	0.70
40	0.54	0.58	0.64	0.66	0.71	0.77
60	0.60	0.63	0.69	0.72	0.78	0.83
80	0.66	0.69	0.75	0.79	0.85	0.89
100	0.72	0.75	0.81	0.85	0.91	0.95

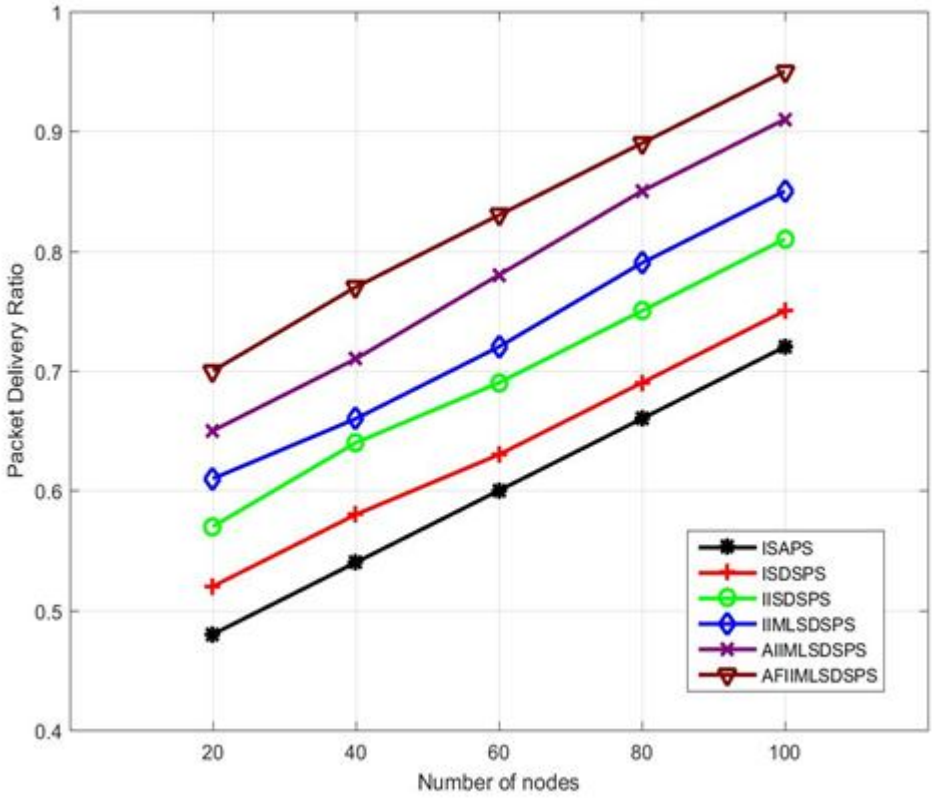


Figure.7.5 Number of Nodes versus Packet Delivery Ratio

Figure 7.5 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 AFIIMLSDSPS has higher packet delivery ratio than the other algorithms.

7.5 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,

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

The comparison of end-to-end delay is shown in Table 7.6.

Table.7.6 Comparison of End-to-End Delay (seconds)

Number of Nodes	ISAPS	ISDSPS	IISDSPS	IIMLSDSPS	AIIMLSDSPS	AFIIMLSDSPS
20	42	38	35	31	28	24
40	51	43	39	36	32	29
60	58	49	44	41	39	33
80	65	53	50	47	43	38
100	70	59	55	52	48	42

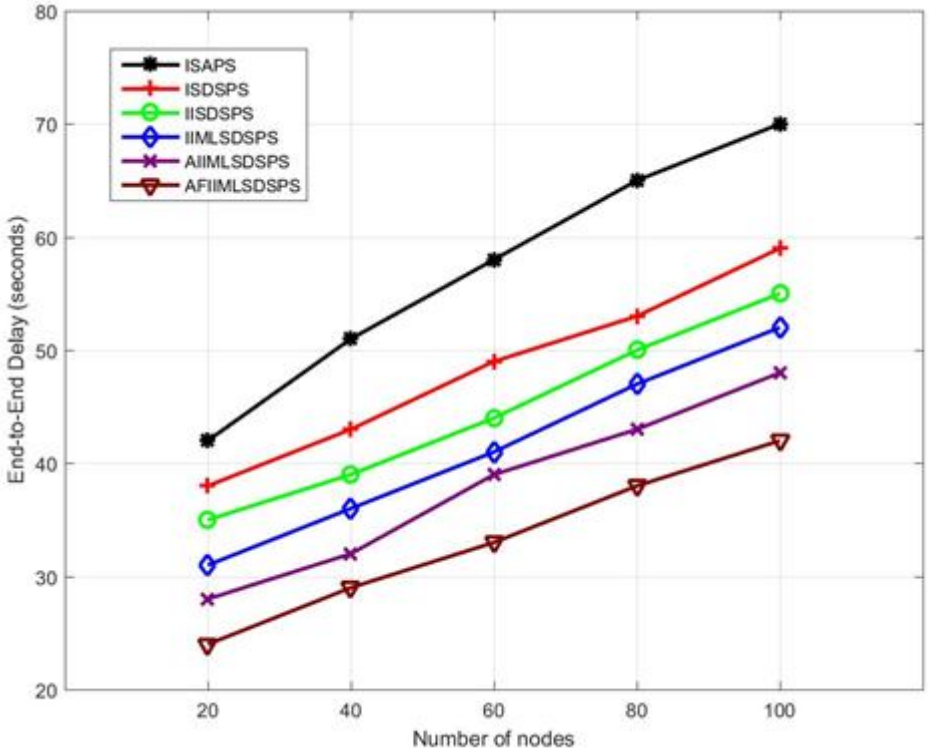


Figure.7.6 Number of Nodes versus End-to-End Delay (Seconds)

Figure 7.6 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 AFIIMLSDSPS has less end-to-end delay than the other algorithms.

8.1 CONCLUSION

The major objective of this research is to enhance the improved security-aware packet scheduling algorithm in mobile ad-hoc networks. In mobile ad-hoc networks, the service dependency and anonymity issues due to the packet scheduling algorithms are not significantly removed. In this research, these issues are removed by considering the dependence and anonymity algorithms effectively. Therefore, an anonymity-based flexible routing protocol with intra-inter and multiple layer service dependent security-aware packet scheduling algorithm is proposed to deal with this crisis.

In the first part of the research, two types of service dependencies algorithms namely Intra-Service Dependent Security-aware Packet Scheduling (ISDSPS) and Inter-Service Dependent Security-aware Packet Scheduling (IISDSPS) are proposed for considering the packets are dependent to each other. In this proposed approach, the dependencies data are collected by the monitoring agents in the mobile hosts based on the message traffic interception between services. The service and their dependencies are represented by using the dependence graph (DG) model and dependence matrix. Hence, the proposed approach detects the packet service dependencies accurately with less latency and communication overhead.

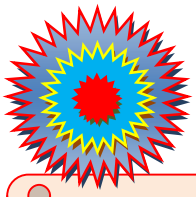
In the second part of the research, the correlation of the dependencies among multiple layers is considered. Here, service layer dependence graph (SLDG) model is proposed whereas it is utilized as global dependency graph. The directed cyclic graph is also used as the local dependency graph model. In the proposed approach named IIMLSDSPS, the constraints for correlation of dependencies are solved by constructing the hypothesis list and rating the constraints in order to improve the performance of the system. In addition, e2e client-service measurements are considered in the dynamic networks for evaluating the internal states of the services. Hence, the proposed approach improves the correlation of dependencies across multiple layers in the network for improving the security of the packet level during transmission.

In the third part of the research, the anonymity-based algorithm called AIIMLSDSPS is proposed for improving the anonymity in mobile ad-hoc networks by using security-aware packet scheduling algorithms. In the proposed approach, fake source-location based algorithm is proposed for generating the fake sources for confusing the impostors in order to avoid the tracking the real source node by the attacker. The generated fake sources are also utilized the fake routing paths in the network which are far away from the real source. Therefore, the attacker cannot find the real source through the transmitted packets. Hence, the proposed anonymity-based approach increases the privacy and security level of the nodes and reduces the latency and packet loss.

In the fourth part of the research, flexible routing protocol with anonymity named AFIIMLSDSPS is proposed for reducing the energy consumption during the flooding process. The proposed phantom routing protocol is based on both flooding and single-path classes for enhancing the privacy protection with less energy consumption. In addition, shortest path between source and sink are also identified for directing the messages to different locations of the network. The phantom flooding protocol is provided for distributing the similar insights as baseline or probabilistic flooding. Thus, the attacker cannot receive the messages for tracking the real sources. Hence, the proposed anonymity and flexible routing protocol based security-aware packet scheduling algorithm improves the security of packets in MANET with low energy consumption and high efficiency. The experimental results are proved that the proposed AFIIMLSDSPS has better performance than the other security-aware packet scheduling algorithms.

8.2 FUTURE WORK

In future, the proposed AFIIMLSDSPS based packet scheduling algorithm will be implemented on different wireless network routers and analyzed their effectiveness through experimental evaluation. In addition, the congestion control will be reduced by introducing the user popularity-based improved packet scheduling. Hence, the overhead on the mobile ad-hoc network will be decreased. Moreover, the proposed AFIIMLSDSPS algorithm will be enhanced by considering the method for processing the packets with expired deadline instead of packet dropping.



REFERENCES

REFERENCES

1. Nasir, H. J. A., & Ku-Mahamud, K. R. (2016). Wireless Sensor Network: A Bibliographical Survey. *Indian Journal of Science and Technology*, *9*(38).
2. Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: Applications and challenges. *Journal-Communications Network*, *3*(3), 60-66.
3. Cheng, X., Huang, X., & Du, D. Z. (Eds.). (2013). *Ad hoc wireless networking* (Vol. 14). Springer Science & Business Media.
4. Aarti, D. S., & Tyagi, S. S. (2013).Study Of Manet: Characteristics, challenges, application and security attack. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5), 252-257.
5. Kumar, M., & Mishra, R. (2012). An overview of MANET: history, challenges and applications. *Indian Journal of Computer Science and Engineering*, *1*(3), 121-125.
6. Chitkara, M., & Ahmad, M. W. (2014). Review on MANET: characteristics, challenges, imperatives and routing protocols. *International Journal of Computer Science and Mobile Computing*, *3*(2), 432-437.
7. Bang, A. O., & Ramteke, P. L. (2013). Manet: history, challenges and applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *2*(9), 249-251.
8. Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*, 32-37.
9. Raja, M. L., & Baboo, C. D. S. S. (2014). An Overview of MANET: Applications, Attacks and Challenges. *International Journal of Computer Science and Mobile Computing (IJCSMC)*, *3*(1), 408-417.
10. Orozco, A. L. S., Matesanz, J. G., Villalba, L. J. G., Diaz, J. D. M., & Kim, T. H. (2012). Security Issues in Mobile Ad Hoc Networks. *International Journal of Distributed Sensor Networks*.
11. Kumar, S., & Dutta, K. (2014). Security issues in mobile ad hoc networks: A survey. *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, 176-221.
12. Stieglitz, S., & Fuchß, C. (2011). Challenges of MANET for mobile social networks. *Procedia computer science*, *5*, 820-825.
13. Raza, N., Aftab, M. U., Akbar, M. Q., Ashraf, O., & Irfan, M. (2016). Mobile Ad-Hoc Networks Applications and Its Challenges. *Communications and Network*, *8*(03), 131.
14. Gupta, P. (2016). A Literature Survey of MANET. *International Research Journal of Engineering and Technology (IRJET)*, *3*(2), 95-99.
15. Rana, A., & Gupta, S. (2013). Review on MANETs Characteristics, Challenges, Application and Security Attacks. *International Journal of Science and Research (IJSR)*, *4*(2), 2203-2208.
16. Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security Issues in Mobile Ad Hoc Networks. *International Conference on Intelligent Computing, Communication & Convergence (ICCC)*, 329-335.
17. 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.
18. 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.

19. Gupta, A., & Ranga, S. P. (2012). Various Routing Attacks in Mobile AD-HOC Networks. *International Journal of Computing and Corporate Research*, *2*(4).

20. 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.

21. Garg, K., & Singh, R. (2012). Scheduling Algorithms in Mobile Ad Hoc Networks. *International Journal of Computer Science & Applications (TIJCSA)*, *1*(5).

22. Jandaeng, C., Suntiamontut, W., & Elz, N. (2011). PSA: the packet scheduling algorithm for wireless sensor networks. *arXiv preprint arXiv:1110.1590*.

23. Tsai, T. Y., Chung, Y. L., & Tsai, Z. (2010). *Introduction to packet scheduling algorithms for communication networks* (pp. 263-271). Sciyo.

24. Børve, B. H. (2008). *Packet Scheduling Algorithms for Wireless Networks*.

25. Raj, A., & Prince, P. B. (2013). Round robin based secure-aware packet scheduling in wireless networks. *International Journal of Engineering Science and Technology*, *5*(3), 570.

26. Chen, X., Jones, H. M., & Jayalath, D. (2011). Channel-aware routing in MANETs with route handoff. *IEEE Transactions on Mobile computing*, *10*(1), 108-121.

27. Sridhar, K. N., & Chan, M. C. (2008, June). Channel-aware packet scheduling for MANETs. In *World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a* (pp. 1-9). IEEE.

28. Saleh, M., & Dong, L. (2013). Real-time scheduling with security enhancement for packet switched networks. *IEEE Transactions on Network and Service Management*, *10*(3), 271-285.

29. Deshmukh, A., & Vaze, R. (2016). Online energy efficient packet scheduling for a common deadline with and without energy harvesting. *arXiv preprint arXiv:1602.01560*.

30. Wu, J., Yuen, C., Cheng, B., Wang, M., & Chen, J. Adaptive Flow Assignment and Packet Scheduling for Delay-Constrained Traffic over Heterogeneous Wireless Networks.

31. Zhang, Z., Chen, X., Zhang, Y., Zhong, C., & Wang, W. (2015). Energy-Efficient Opportunistic Packet Scheduling in Mobile Relay Systems. In *IEEE Transactions on Vehicular Technology, 65*(7), 5327-5336.

32. Yantong, W., & Sheng, Z. An Enhanced Dynamic Priority Packet Scheduling Algorithm in Wireless Sensor Networks. *UKSim-AMSS 18th International Conference on Computer Modelling and Simulation,* Cambridge, United Kingdom, 311-316.

33. Mishra, A., & Venkitasubramaniam, P. (2016). Anonymity and Fairness in Packet Scheduling: A Quantitative Tradeoff. *IEEE/ACM Transactions on Networking*, *24*(2), 688-702.

34. Yu, Q., Znati, T., & Yang, W. (2015, December). Energy-efficient, Delay-aware packet scheduling in high-speed networks. In *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)* (pp. 1-8). IEEE.

35. Kongsili, L., Fujimoto, A., & Uchio, F. (2015). Packet Scheduling and Access Priority Control for QoS and Fairness in Wireless LAN. *Procedia Computer Science*, *60*, 1788-1797.

36. Li, F. (2013). A comprehensive study of an online packet scheduling algorithm. *Theoretical Computer Science*, *497*, 31-38.

37. Hung, T. Y., Chen, Z., & Tan, Y. P. (2011). Packet scheduling with playout adaptation for scalable video delivery over wireless networks. *Journal of Visual Communication and Image Representation, 22*(6), 491-503.

38. Sharifkhani, A., & Beaulieu, N. C. (2009, November). Packet transmission scheduling algorithm for dense wireless sensor networks with mobile sink. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* (pp. 1-8). IEEE.

39. Lakshmi, S., & Radha, S. (2012, April). Selfish aware queue scheduler for packet scheduling in MANET. In *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on* (pp. 343-348). IEEE.

40. Karim, L., Nasser, N., Taleb, T., & Alqallaf, A. (2012, June). An Efficient Priority Packet Scheduling Algorithm for Wireless Sensor Network. In *2012 IEEE International Conference on Communications (ICC)* (pp. 334-338). IEEE.

41. Kumar, R. A., & Varshini, K. M. (2014). Multilevel Priority Packet Scheduling Scheme for Wireless Networks. *International Journal of Distributed and Parallel Systems*, *5*(1-3), 69.

42. Rewadkar, D. N., & Khot, S. (2014). Real Time Scheduling for Security of Packet Switched Network. *International Journal of Computer Technology & Applications (IJCTA), 5*(3), 1188-1193.

43. Achir, N., & Muhlethaler, P. (2014, November). Optimal sinks deployment and packet scheduling for Wireless Sensor Networks. In *2014 IFIP Wireless Days (WD)* (pp. 1-6). IEEE.

44. Tiwari, G., & Mishra, D. (2016). A Study on Real-Time Packet Scheduling Algorithm in WLAN with Security Awareness. *International Journal of Research in Engineering and Technology (IJRET), 5*(7), 428-432.

45. Wan, Z., Ren, K., Zhu, B., Preneel, B., & Gu, M. (2010). Anonymous user communication for privacy protection in wireless metropolitan mesh networks. *IEEE transactions on vehicular technology*, *59*(2), 519-532.

46. Torabzadeh, M., & Ajib, W. (2010). Packet scheduling and fairness for multiuser MIMO systems. *IEEE Transactions on Vehicular Technology*, *59*(3), 1330-1340.

47. Tsai, M. F., Chilamkurti, N., Park, J. H., & Shieh, C. K. (2010). Multi-path transmission control scheme combining bandwidth aggregation and packet scheduling for real-time streaming in multi-path environment. *IET communications*, *4*(8), 937-945.

48. Tajima, T., & Okabe, Y. (2016, June). Optimizing Packet Transmission Scheduling for Enhanced Web QoE in Wireless LAN. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual* (Vol. 2, pp. 312-318). IEEE.

49. Ooshita, F., Kawai, S., Kakugawa, H., & Masuzawa, T. (2014). Randomized Gathering of Mobile Agents in Anonymous Unidirectional Ring Networks. *IEEE Transactions on Parallel and Distributed Systems*, *25*(5), 1289-1296.

50. Huang, S., Izquierdo, E., & Hao, P. (2016, November). Multi-generation packet scheduling for live streaming with network coding. In *Visual Communications and Image Processing (VCIP), 2016* (pp. 1-4). IEEE.

51. Chan, M. C., Tseng, C. C., & Yen, L. H. (2016, April). Jitter-aware packet scheduler for concurrent multipath transmission in heterogeneous wireless networks. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE* (pp. 1-7). IEEE.

52. Jandaeng, C., Suntiamontut, W., & Elz, N. (2011). PSA: the packet scheduling algorithm for wireless sensor networks. *arXiv preprint arXiv:1110.1590*.

53. Dang, L., Xu, J., Li, H., & Dang, N. (2010, December). DASR: distributed anonymous secure routing with good scalability for mobile ad hoc networks. In *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific* (pp. 454-461). IEEE.

54. Gunasekaran, M., & Premalatha, K. (2012, July). Trust-Based Anonymous Communication for malicious user disclosure in Mobile Ad Hoc Networks. In *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on* (pp. 1-9). IEEE.

55. Jiang, R., & Xing, Y. (2012, October). Anonymous on-demand routing and secure checking of traffic forwarding for mobile ad hoc networks. In *Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on* (pp. 406-411). IEEE.

56. Gunasekaran, M., & Premalatha, K. (2013). TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks. *IET Information Security*, *7*(3), 203-211.

57. Lo, N. W., Chiang, M. C., & Hsu, C. Y. (2015, May). Hash-based anonymous secure routing protocol in mobile ad hoc networks. In *Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on* (pp. 55-62). IEEE.

58. Malwe, S. R., & Biswas, G. P. (2015, October). Location aware sector-based routing in wireless ad hoc networks. In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on* (pp. 154-159). IEEE.

59. Schellenberg, S., Saliminia, A., Krug, S., Seitz, J., Finke, T., & Schroeder, J. (2014, February). Routing-based and location-aware service discovery in mobile ad-hoc networks. In *Information Networking (ICOIN), 2014 International Conference on* (pp. 7-12). IEEE.

60. Sheklabadi, E., & Berenjkoub, M. (2011, February). An anonymous secure routing protocol for mobile ad hoc networks. In *Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on* (pp. 142-147). IEEE.

61. Singh, K., Sharma, A., & Singh, N. K. (2015, December). Linear Regression Based Energy Aware Location-Aided Routing Protocol for Mobile Ad-Hoc Networks. In *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on* (pp. 114-121). IEEE.

62. Kathrine, J. W., & Raj, A. (2012, October). Packet Scheduling Algorithms in Different Wireless Networks A Survey. In *International Journal of Engineering Research and Technology* (Vol. 1, No. 8 (October-2012)). ESRSA Publications.

63. Wang, Z. J., Pei, H. R., & Wang, Y. (2013, December). Sampling Traffic Analysis of Anonymous Communications in Mobile Ad Hoc Networks. In *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on* (pp. 233-239). IEEE.

64. Annadurai, C. (2011). Review of packet scheduling algorithms in mobile ad hoc networks. *International Journal of Computer Applications*, *15*(1), 7-10.

65. Chennakesavula, P., Ebenezer, J., Murty, S. S., & Jayakumar, T. (2013, February). Real-time packet scheduling for real-time wireless sensor networks. In *Advance Computing Conference (IACC), 2013 IEEE 3rd International* (pp. 273-276). IEEE.

66. Gomathi, R., & Mahendran, N. (2015, February). An efficient data packet scheduling schemes in wireless sensor networks. In *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on* (pp. 542-547). IEEE.

67. Jain, V., Agarwal, S., & Goswami, K. (2014, July). Dynamic multilevel priority packet scheduling design for WSN. In *Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on* (pp. 86-90). IEEE.

68. Mansouri, W., Zarai, F., Mnif, K., & Kamoun, L. (2011, April). New scheduling algorithm for wireless mesh networks. In *Multimedia Computing and Systems (ICMCS), 2011 International Conference on* (pp. 1-6). IEEE.

69. Natarajan, A., Ning, P., Liu, Y., Jajodia, S., & Hutchinson, S. E. (2012). *NSDMiner: Automated discovery of network service dependencies* (pp. 2507-2515). IEEE.

70. Saleh, M., & Dong, L. (2012, January). Real-time scheduling with security awareness for packet switched networks. In *Radio and Wireless Symposium (RWS), 2012 IEEE* (pp. 391-394). IEEE.

71. Singh, S. (2014, December). Improve real-time packet scheduling algorithm with security constraint. In *India Conference (INDICON), 2014 Annual IEEE* (pp. 1-6). IEEE.

72. Tsou, Y. T., Lu, C. S., & Kuo, S. Y. (2013). MoteSec-aware: a practical secure mechanism for wireless sensor networks. *IEEE Transactions on Wireless Communications*, *12*(6), 2817-2829.

73. Lupia, A., & Marano, S. (2016, July). A dynamic monitoring for energy consumption reduction of a trust-based intrusion detection system in mobile Ad-hoc networks. In *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2016 International Symposium on* (pp. 1-5). IEEE.

74. Nuruzzaman, M. T., & Ferng, H. W. (2016, May). A low energy consumption routing protocol for mobile sensor networks with a path-constrained mobile sink. In *Communications (ICC), 2016 IEEE International Conference on* (pp. 1-6). IEEE.

75. Ouchitachen, H., Hair, A., & Idrissi, N. (2015, October). Minimizing energy consumption in mission-specific mobile sensor networks by placing sensors and base station in the best locations: Genetic algorithms approach. In *Wireless Networks and Mobile Communications (WINCOM), 2015 International Conference on* (pp. 1-7). IEEE.

76. Cai, X., Duan, Y., He, Y., Yang, J., & Li, C. (2015). Bee-Sensor-C: an energy-efficient and scalable multipath routing protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *11*(3), 976127.

77. Samar, P., Pearlman, M. R., & Haas, Z. J. (2004). Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks. *IEEE/ACM Transactions on Networking (TON)*, *12*(4), 595-608.

78. Chen, K., & Shen, H. (2016). FaceChange: Attaining Neighbor Node Anonymity in Mobile Opportunistic Social Networks with Fine-Grained Control. *IEEE/ACM Transactions on Networking*.

79. Bradbury, M., Leeke, M., & Jhumka, A. (2015, August). A dynamic fake source algorithm for source location privacy in wireless sensor networks. In *Trustcom/BigDataSE/ISPA, 2015 IEEE* (Vol. 1, pp. 531-538). IEEE.

80. Jhumka, A., Bradbury, M., & Leeke, M. (2012, June). Towards understanding source location privacy in wireless sensor networks through fake sources. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 760-768). IEEE.

81. Liu, J., Yang, Z., & Liu, Y. (2012, December). Ad-hoc anonymity: Privacy preservation for location-based services in mobile networks. In *Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on* (pp. 197-204). IEEE.

82. Thomason, A., Leeke, M., Bradbury, M., & Jhumka, A. (2013, July). Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 667-674). IEEE.

83. Vijayan, A., & Thomas, T. (2014, April). Anonymity, unlinkability and unobservability in mobile ad hoc networks. In *Communications and Signal Processing (ICCSP), 2014 International Conference on* (pp. 1880-1884). IEEE.

84. Wang, Y., Xu, D., & Li, F. (2016). Providing location-aware location privacy protection for mobile location-based services. *Tsinghua Science and Technology*, *21*(3), 243-259.

85. Bai, L., Li, L., Qian, S., & Zhang, S. (2016, August). Random selection false source-based algorithm for protecting source-location privacy in WSNs. In *Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2016 12th International Conference on* (pp. 2064-2069). IEEE.

86. Niu, X., Wei, C., Feng, W., & Chen, Q. (2014, April). OSAP: Optimal-cluster-based source anonymity protocol in delay-sensitive wireless sensor networks. In *Wireless Communications and Networking Conference (WCNC), 2014 IEEE* (pp. 2880-2885). IEEE.

87. Gurjar, A., & Patial, A. R. (2013). B. Evaluating the privacy measure of the source location privacy scheme in a wireless sensor network. *Int J Comput Eng Res*, *3*, 10-13.

88. Dong, M., Ota, K., & Liu, A. (2015, October). Preserving source-location privacy through redundant fog loop for wireless sensor networks. In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on* (pp. 1835-1842). IEEE.

89. Li, Y., & Ren, J. (2010, March). Source-location privacy through dynamic routing in wireless sensor networks. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1-9). IEEE.

90. Moe, M. E. G. (2009). Quantification of anonymity for mobile ad hoc networks. *Electronic Notes in Theoretical Computer Science*, *244*, 95-107.

91. 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.

92. 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).

93. 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.

94. 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.

95. Lawrence, E., Michailidis, G., Nair, V., & Xi, B. (2006). Network tomography: A review and recent developments. *Ann Arbor*, *1001*(48), 109-1107.

96. Tati, S., Novotny, P., Ko, B. J., Wolf, A., Swami, A., & La Porta, T. (2011). Performance diagnosis of services in scalable and dynamic networks. *System*, *5*, 1.

97. Tan, W., Xu, K., & Wang, D. (2014). An anti-tracking source-location privacy protection protocol in WSNs based on path extension. *IEEE Internet of Things Journal*, *1*(5), 461-471.

98. Ozturk, C., Zhang, Y., & Trappe, W. (2004, October). Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 88-93). ACM.

99. Kamat, P., Zhang, Y., Trappe, W., & Ozturk, C. (2005, June). Enhancing source-location privacy in sensor network routing. In *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on* (pp. 599-608). IEEE.

100. Gu, C., Bradbury, M., Jhumka, A., & Leeke, M. (2015, November). Assessing the performance of phantom routing on source location privacy in wireless sensor networks. In *Dependable Computing (PRDC), 2015 IEEE 21st Pacific Rim International Symposium on* (pp. 99-108). IEEE.

ABOUT THE AUTHOR

Dr. R. Nandakumar worked as Assistant Professor in the Department of Computer Science, R. V. Government College, University of Madras, India. His Research Interests are Network Security, Information Retrieval and web search. He has Published more than 15 research articles in International journals and Conferences.

ABOUT THE BOOK

In modern years, the most developed wireless networks are Mobile Ad-hoc Networks (MANET) which is referred as the collection of independent, self-configuring devices such as mobile nodes connected through the wireless links. Due to the open nature, several challenges and issues were occurred. However, the major challenge in MANET was the packet level security in multiple levels. The network performance was degraded due to contravene in packet level security which causes high packet loss. To overcome this challenge, an Improved Security-Aware Packet Scheduling (ISAPS) algorithm was proposed for achieving high level security and effective packet scheduling. However, in ISAPS, the packets from the multiple nodes were considered as independent to each other. In addition, the computational complexity and energy consumption were high. The correlation of the multiple dependency packets were degraded the network performance due to representing the dependencies and scalability. The efficiency of security was less since the source node and their packets were easily identified by the attacker. Therefore, in this research, these issues are avoided by proposed inter and intra service dependencies based ISAPS algorithm. Furthermore, the anonymity concept is included with the security-aware packet scheduling algorithm for improving the efficiency of security by secure routing protocol.

Empyreal Publishing House

ISBN 978-81-946373-9-4