Journal of Computer Science

Original Research Paper

Secure and Efficient Transmission in Mobile Ad hoc Network to Identify the Fake ID's Using Fake ID Detection Protocol

[1]Gopalakrishnan, S. and [2]P. Ganeshkumar

[2]Department of ECE, PSNA College of Engineering and Technology, Dindigul, India
[1]Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, India

Article history
Received: 13-06-2014
Revised: 27-08-2014
Accepted: 10-09-2014

Corresponding Author:
Gopalakrishnan, S.
Department of ECE, PSNA College of Engineering and Technology, Dindigul, India
Email: lapog.gopal@gmail.com

Abstract: Mobile Ad hoc Network (MANET) is a frequent infrastructure less self- coordinating network, in which each and every mobile node works as a source, destination and a wireless relay. Such pattern of wireless network is produced by dynamic mobile nodes without any centralized or fixed or existing network infrastructure. In MANET, however, there is no static network infrastructure and mobile nodes do not possess accession to a centralized host to assume IDs or IP addresses. Moreover, owing to mobility of node, network partitions and combines are quick occurrences. These occurrences produce the possibility of fake addresses inside the network. Thus, a centralized scheme cannot be employed in those networks; a dispersed and dynamic mechanism is required for mobile nodes to adopt and preserve a unique ID or IP address in mobile networks. In this study, we proposed two protocols namely Fake ID Detection (FIDD) and Path Selection Routing protocol (PSR) in which the FIDD protocol is used to detect the fake id i.e., the duplicate packets and PSR protocol is used to select the alternate path when the current path became busy or failure and it frequently chooses an alternate path to continue the transmission without any interruption. Hence, the efficiency and life-time of the network can be increased. Finally, the overall performance of the network can be increased.

Keywords: Mobile Ad hoc Network, FIDD Protocol, PSR Protocol, OAIH and BAIH

Introduction

Mobile Ad hoc Network (MANET) is a type of wireless ad hoc network in which entire transferable nodes can directly communicate with each other without reckon on a centralized or fixed network infrastructure. Here, forwarding and routing of packets are accomplished by intermediate or neighbor nodes. By considering the routing protocols, the routing path is adopted while a sender wants to transmit data packets to the destination (Camp *et al*., 2002; Basagni *et al*., 2004; Chlamtac *et al*., 2003). To transmit and receive packets within two nodes, they must possess its unique IP address in that network. Because IP is also employed in mobile ad hoc networks and a unique IP address must be allotted to each and every node. Thus, IP address auto configuration approaches have formulated to eliminate the manual configuration overhead. Generally, we can classify the IP assignment results to be either reactive protocol or proactive protocol. Reactive protocols necessitate a consensus among entire nodes of that network on the novel IP address which is to be allotted, where in the proactive routing scheme; each and every node can severally allotted a novel IP address without demanding permission from any other mobile node in the mobile network. Mobility is the major causes for partitioning of the ad hoc network. While a mobile node possessing unique IP address in a partition, proceeds into other partition and there may be

an increase a probability of fake of the node ID or IP address. Because, IP address accepts to be a unique one, address disputes require to be discovered through a Fake ID Detection (FIDD) protocol.

Fake ID Detection (FIDD) protocol is the type of methodology inserted for supervising the delivery of ID or IP addresses by the private nodes by themselves. In this study, we presented a reactive ID or IP address appointment approach with FIDD for address dispute discovery for the mobile ad hoc network. The configuration of network parameter which is needed to be unique for each and every node in the mobile network is their ID or IP address. Our dispersed protocol with FIDD mechanism assures which no two nodes in the mobile network adopt the same ID or IP address. We depict improvements to the result which can address the troubles that may develop owing to node failures, packet losses, node mobility, or multiple simultaneous launchings of node configuration and the partitioning network and combiner. Here, the FIDD protocol has three phases namely detection of fake ID, Node initialization and node registration. In first phase, fake IDs are detected and in second phase nodes are initialized and in third phase nodes are registered in the network. Our aim is make the network more efficient. If the path is busy or became failure the packets which are needed to be transmitted could not able to transmit. For that reason we propose another protocol called Path Selection Routing (PSR) protocol which is used to choose alternate path when the current transmission path is busy (packet transmission takes place) or it became failure. If any of the paths are busy or it contains high packet dropping ratio due to some other factors like channel noise, it quickly chooses another one as an alternate path in order to continue the transmission without any interruption. Thus, the efficiency and life-time of the network can be increased. Finally, the overall performance of the network can be increased.

The rest of the chapter is organized as follows. Section 2 presents the related work. In section 3 proposed protocols are discussed in a detailed manner. Section 4 covers the algorithms for FIDD protocol and PSR protocol with their description. Section 5 presents the comparison table for existing and proposed protocols with its description. Section 6 provides the experimental results and section 7 summarizes the chapter with future work.

Related Work

In a self-directed mobile ad hoc mobile network the mobile nodes can be unambiguously discovered by an IP address with the exclusively introduce that such address should be dissimilar from that whatever other node in that ad hoc network. The process of configuration is the set of phases by which a single node receives their IP address inside the network. There are three mechanisms (Villalba *et al*., 2011) are present to set addresses like stateful and stateless and hybrid.

Rather than the addresses assignment along an instant entity, stateless auto-contour appropriates the mobile nodes to build addresses by themselves, normally established on the ID of hardware or some random number. Mobility is the cause for zoning of the mobile network. While a mobile node experiencing unique IP address in single zone, proceeds into another zone and there may be originate a probability of IP address duplication. Later on, the IP address accepts to be unique, address disputes necessitate to be discovered by a Duplicate Address Detection (DAD) procedure. Duplicate Address Detection (DAD) is one of the approaches proposed for supervising the delivery of IP addresses through the single mobile nodes themselves. Zahoor ul Huq *et al*. (2010) Ganeshkumar and Thyagarajah (2010) Proposed the value of sensing of IP address disputes and various approaches presented for the process of detection.

Weak DAD, proposed in (Vaidya, 2002; Velayutham and Manimegalai, 2014), is a type of methodology to keep a packet from routing to a incorrect destination, even if there is any duplicate addresses subsist. Mobile nodes in the ad hoc network are distinguished not only by their IP addresses, but in addition to a key that can be established on an ID of hardware or some random number. If a mobile node delivers a packet comprising an IP address which is kept in their routing table, but on a dissimilar key, an address dispute is discovered and it will merely function with the proactive one which updates or informs the routes invariably, but with a reactive one there may be mobile nodes which could not discover the IP addresses duplicity. It has no need to contribute extras overhead to the routing protocol, but then, it actually contributes to the overhead through transmitting ever the key along with each IP address.

By considering the Strong Duplicated Address Detection (SDAD) approach (Perkins *et al*., 2001; Gopalakrishnan and Ganeshkumar, 2014) the mobile node prefers two IP addresses name namely temporary and tentative addresses. It will merely utilize the temporary address for the process of initialization when it discovers if the provisional one is unique or not. The discovery approach comprises of transmitting a message Internet Control Message Protocol (ICMP) intended instantly to such address. If it obtains a reply, such IP address is being utilized so the

operation will be summarized. If this process does not deliver a reply, the message will be transmitted a particular number of times to make a point which the address is the unique one. It will not function for temporary disjuncture or dropping of the mobile network. Furthermore, while the network is so long and merely some free IP addresses persist, it enhances the overhead till it encounters a unique IP addresses. In address auto-configuration with Address Reservation and Optimistic Duplicated address detection (AROD) (Kim *et al*., 2007), the address reservation is based on the existence of nodes that have an IP address reserved to deliver it to the new nodes that enter. Two types of nodes will exist. Type 1: Agents type 1 with a reserved IP address, apart from the IP address that has its network interfaces. When a node joins the network, this reserved IP will be assigned to it immediately. Type 2: Agents type 2, which do not have reserved IP addresses. If a node that joins newly asks one of these for an IP address, this node borrows the reserved address of one of its neighbors who is of type 1 and it is assigned to the new one immediately. If the possibility of changing the reserved IP address number to the node type, number increases, the latency of IP address assignment is minor, but on the contrary the overhead increases due to having had to undergo more DAD processes and vice versa.

Hybrid Centralized Query-based Auto configuration (HCQA) (Sun and Belding-Royer, 2003) is a dynamic address configuration protocol for mobile ad hoc networks that provides address assignment to mobile nodes during the formation and maintenance of a network. The protocol assigns unique addresses and can be combined with a variety of routing schemes. Further, the address authority aids in the detection of duplicate addresses and handles address resolution after network partitions and merges. It has two main problems, firstly the overhead produced by the SDAD process and periodic messages of Address Authority and secondly, the network depends on a central entity with which all nodes must communicate directly in order to register its IP address, so that much latency is added at the joining of nodes to the network.

Mohsin and Prakash (2002) propose a stateful protocol which uses multiple disjoint allocation tables. In this approach every node has a disjoint set of IP addresses that can be assigned to new nodes, is said that as node owns these pool of IP addresses hence no quorum is required to make a decision. This approach uses a proactive scheme for dynamic allocation of IP addresses in MANETs. This protocol employs the approach described in MANET to solve network partitioning. The major drawback of this protocol is that the synchronization depends on the existence of a reliable broadcast and such a thing does not exist in a distributed mobile environment, thus one can question the robustness of this protocol.

An improvement of (Mohsin and Prakash, 2002) can be found in (Thoppian and Prakash, 2006), where Thoppian and Prakash propose a dynamic address assignment based on a so-called buddy system that manages mobility of nodes during address assignment, message loss and network partitioning and merging. However, the IP address allocation can generate a high overhead of control messages while it does a global search and the address recovery (to avoid missing addresses) requires diffusion messages by a flooding process. In addition, union and partition may incur in high overhead because of the global nature of this protocol.

Extensible MANET Auto-configuration Protocol (EMAP) (Ros *et al*., 2010) is based on the idea of a protocol of REQUEST/REPLAY messages. The main advantage of this protocol is the possibility of doing it extensible, i.e., it can include new functionalities in the future that are analyzed in a theoretical way, such as Domain Name Server (DNS). The route discovery mechanism among nodes is similar to the Ad hoc On-Demand distance Vector (AODV) (Perkins and Royer, 1999) protocol.

Proposed Protocol

In this study, we presented two protocols one is Fake ID Detection (FIDD) protocol which the FIDD protocol is used to detect the fake id i.e., the duplicate packets and another one is Path Selection Routing (PSR) protocol which is used to select the alternate path when the current path became busy or failure. In this section the proposed work is discussed detailed manner.

Fake ID Detection (FIDD) Protocol

Fake ID detection protocol has three following phases through which the fake or duplicate packets are detected at the sender side. This protocol includes the following three steps.

Step 1: Detection of Fake ID

A main effect of auto configuration of address is Fake ID Detection (FIDD). Fake addresses may originate during the initialization process of nodes because the nodes may contain multiple hops and cannot heed each other at once. Besides during combining of two nodes may assume same address.

Consider the nodes which are needed to combine are denoted as A and B. Nodes A and B receive the same ID, A, severally from dissimilar networks. A source or sender node in the network starts a session and transmission with node A through any of the routing path. Such path contains a length of two. While the two networks proceed towards one another and subsequently combine, node B moves into the direct range of transmission of the source node. Therefore, if proactive routing protocols are employed, after obtaining the routing information of periodic update, the sender node must update their routing initiation for ID or IP address A to the straight path to node B with length of the path as one. If the reactive routing protocols are used, novel path discovery processes will consequence in the path to address A to the novel path. Hence, the erroneous routing keeps the sender from communication with the right destination. So, FIDD is very essential. As we have considered WDAD (Vaidya, 2002) and SDAD (Perkins *et al*., 2001) protocols that both induce its own restrictions. In WDAD if a novel node connects the network with no knowledge of the routing data and the identifier and it cannot differentiate those two nodes merely by ID or IP addresses. Therefore, this will guide to erroneous routing. In SDAD, if a mobile node is disjointed for very long time, it would not deliver the packet which can be addressed as partition.

Step 2: Node Initialization

A mobile node getting in a network, broadcast Address Request Message (ARM) by setting their randomly selected candidate ID or IP address apart from their address of the hardware for the reply message. Node commences its respond timer, if respond timer runs out and it does not acquire any ARM, it duplicates the step for threshold number of time than which resolves that it can prefer the address for the process of communication. But ahead of registration process it cannot employ it for communication, thus it awaits for Original Address Information Holder (OAIH) ask_reg unicast message transmitted instantly at its developed ID or IP address, if anyway the node employing the candidate ID or IP address ARM as well as OAIH ARM message does not accomplish to the novel node then even fake address will be discovered and novel node will take over the above process again and again. If the network does not deliver any ask_reg message for ask_t where ask_t> n*ask_reg_t then the network will arrive to experience that it is the only node in this network and it will determine the mobile ad hoc network and announce itself as OAIH.

Step 3: Node Registration

Since extending all the three level of fake ID detection the novel node with their assumed ID or IP address, their MAC address and enquired lifetime for the ID or IP address unicasts a Registration Request (RR) to OAIH. The OAIH contributes the information for such node to their address list and unicasts a RR to the node suggesting whether the registration process was successful. On success, the RR suggests the sanctioned lifetime for the IP address. Now the former OAIH will become Backup Address Information Holder (BAIH) and transmit the address list with their state information to the novel registered node that is now novel OAIH. After getting OAIH it has to transmit their unique identifier of the network so that each and every node updates itself about novel OAIH and that network ID they belongs to. The former BAIH will arrive to experience with such broadcast that it is no longer been BAIH.

Path Selection Routing (PSR) Protocol

Then, we proposed Path Selection Routing (PSR) protocol which is a novel protocol that selects an alternate path while the current path is busy or it became failure since it has the dropped packets as maximum number and our PSR protocol selects the paths frequent and efficient manner for packet transmission with no delay. Here, the packets are transmitted to the determined destination without any time delay which also increases the overall network performance that can provide and affirm efficient transmission with scalable and robust and the life-time of the network is increased by reducing the traffic and is required for reliable and scalable communication without any interruption within the routing paths through the way the PDR is increased. In PSR protocol, there is no need to keep any routing information on routing table to update the link status since the sustainment and storage of this routing table necessitates much more bandwidth that also degrades the performance of the network.

Algorithm For Fake ID Detection (FIDD) Protocol

1. Collections of neighbors nodes λN_{ix}
2. Initialize source ΔS_{ix} and destination ΔD_{iy}
3. Attach agent ΔA_{ix}
4. Network processing starts packet flow
5. Packets transmission and ID creation
6. Phase 1
7. To detect the fake ID
8. Total number of packets = 1000 (ΔP_{ix} and ΔP_{id})
9. Total number of transmission Path = 10
10. Create packet ID ΔP_{id}

11. For ($\Delta P_{ix} = 0$; $\Delta P_{id} \leq N$; ΔP_{ix} ++)
12. If $\Delta P_{ix} = 0$
13. No Fake ID packets are delivered to destination
14. Else
15. $\Delta P_{ix} = 1$
16. Duplicate packet was injected fake id create
17. Phase 2
18. Node initialization ΔN_{ix}
19. For ($\Delta P_{ix} = 0$; $\Delta P_{ix} \leq N$; ΔP_{ix} ++)
20. To refer the packet ID
21. Phase 3
22. Register the OLH (Data's are store) this process

Algorithm For Path Selection Routing (PSR)

1. Path failure choose alternate path
2. Total number of transmission path = 5 (denoted ΔP_{ix})
3. Queue process was followed (FIFO)
4. For ($\Delta P_{ix} = 0$; $\Delta P_{ix} \leq 10$; ΔP_{ix} ++)
5. If ($\Delta P_{ix} = 1$)
6. ΔP_{ix} = Choose path A (Busy)
7. Else
8. ΔP_{ix} = Choose path B
9. if ($\Delta P_{ix} = 2$)
10. ΔP_{ix} = Choose path C (Busy)
11. Else
12. ΔP_{ix} = Choose path D
13. if ($\Delta P_{ix} = 3$)
14. ΔP_{ix} = Choose path E (Busy)
15. Else
16. ΔP_{ix} = Choose path F
17. if ($\Delta P_{ix} = 4$)
18. ΔP_{ix} = Choose path G (Busy)
19. Else
20. ΔP_{ix} = Choose path H
21. if ($\Delta P_{ix} = 5$)
22. ΔP_{ix} = Choose path I (Busy)
23. Else
24. ΔP_{ix} = Choose path J
25. End if
26. $D_{iy} <= S_{ix} + A_{ix}$ // Receive the packets send the acknowledgement to source
27. End process

Description

In this study, we proposed two protocols namely Fake ID Detection (FIDD) and Path Selection Routing protocol (PSR) in which the FIDD protocol is used to detect the fake id i.e., the duplicate packets and PSR protocol is used to select the alternate path when the current path became busy or failure.

Generally, the network is said to be a collection of mobile nodes in which each mobile nodes contains their own packet ID which is not same as that of another one i.e., the packet ID (which means packet address) is a unique one for each and every packets. Some times during packet transmission fake IDs are created by the network itself due to some other problems of the network and such fake ID containing packets comprises of duplicate packets which is not similar with the original message. When the destination receives those packets it may collapse to detect which packet is original and then it intimates the source by sending an acknowledgement message. For that reason the packets are sensed or fake IDs are detected before packet transmission takes place and this process takes place at the receiver side. This fake ID detection protocol comprises of two three phases such as fake ID detection, Node initialization and Node Registration. Each path of the network contains queue buffer through which the packets are transmitted hop-by-hop manner or one by one. At first phase, the packets which are needed to be transmitted are sensed by the network in order to detect fake IDs and at the second phase nodes are initialized for transmission. In phase three, the initialized packets are registered in the network. Thus, the fake IDs are detected at the sender side.

Then, we are going to discuss about the Path Selection Routing (PSR) protocol which is used to choose alternate path when the current transmission path is busy (packet transmission takes place) or it became failure. Here, we use 1200 packets and 10 paths for transmission. If any of the paths are busy or it contains high packet dropping ratio due to some other factors like channel noise, it quickly chooses another one as an alternate path in order to continue the transmission without any interruption. Thus, the efficiency and life-time of the network can be increased. Finally, the overall performance of the network can be increased.

Comparison of Existing and Proposed Protocols

In above Table 1, we compare the parameters of Existing DAD and Proposed FIDD Protocols. In Existing DAD, we can send only 1000 packets but in Proposed FIDD we can transmit 1200 packets through an individual path. The DAD protocol uses total number of paths as 50 but our proposed FIDD protocol utilizes total number of paths as 20. Path selection in DAD protocol is random but in FIDD protocol is chooses the alternate path by using another protocol called PSR protocol in order to make the network efficient. The DAD protocol requires 10dB bandwidth but FIDD protocol has 15dB bandwidth. Transmission power of DAD and FIDD protocol is 8.0 W and 5.0 W respectively. The data rate of DAD protocol is 16.5e and FIDD protocol is 18.5e.

In above Table 2, we compare the parameters of existing WADD and Proposed PSR Protocols. In existing WADD, we can send only 1200 packets but in Proposed PSR we can transmit 1500 packets through an individual path. The WADD protocol and proposed FIDD protocol use the omnidirectional antenna for 360 degree Coverage. Path selection in WADD protocol is random but in PSR protocol is chooses the alternate path by using another protocol called PSR protocol in order to make the network efficient. The WADD protocol requires total number of paths count as 10 PSR protocols Choose the path total number path is 25. Transmission power of WADD and PSR protocol is 5.0 W and 12.0 W respectively. The data rate of WADD protocol is 10.5e and PSR protocol is 28.5e.

Experimental Results

In Fig. 1, we particularly compare packet delivery ratio and scalability. The network that employs the FIDD protocol has high PDR and scalability.

In Fig. 2, we particularly compare Number of nodes and Latency. The network that uses the FIDD protocol has more number of nodes and high latency.

In Fig. 3 we particularly compare scalability and time delay. The network that uses the FIDD protocol has high scalability and reduced time delay.

In Fig. 4 and here we particularly compare delay and avg. time delay. The network that uses the FIDD protocol has reduced delay and average time delay.

In Fig. 5, we and here we particularly compare communication overhead and throughput. The network that uses the FIDD protocol has reduced communication overhead and high throughput.

Table 1. Network parameters and protocols discussion

Parameter	DAD protocol	FIDD protocol
Total number of nodes	50	20
Total packets	1000	1200
Path selection	Random	Choose alternate path using PSR protocol
Bandwidth	10dB	15dB
Transmission power	8.0 W	5.0 W
Data rate	16.5e	18.5e

Table 2. Network parameters and protocols discussion

Parameter	WADD protocol	PSR protocol
Total number of nodes/packets	30/1000	20/1500
Antenna type	Omni directional	Omni directional
Path selection	random	choose alternate path using PSR protocol
Total paths	15	25
Transmission power	5.0 W	12.0 W
Data rate	10.5e	28.5e

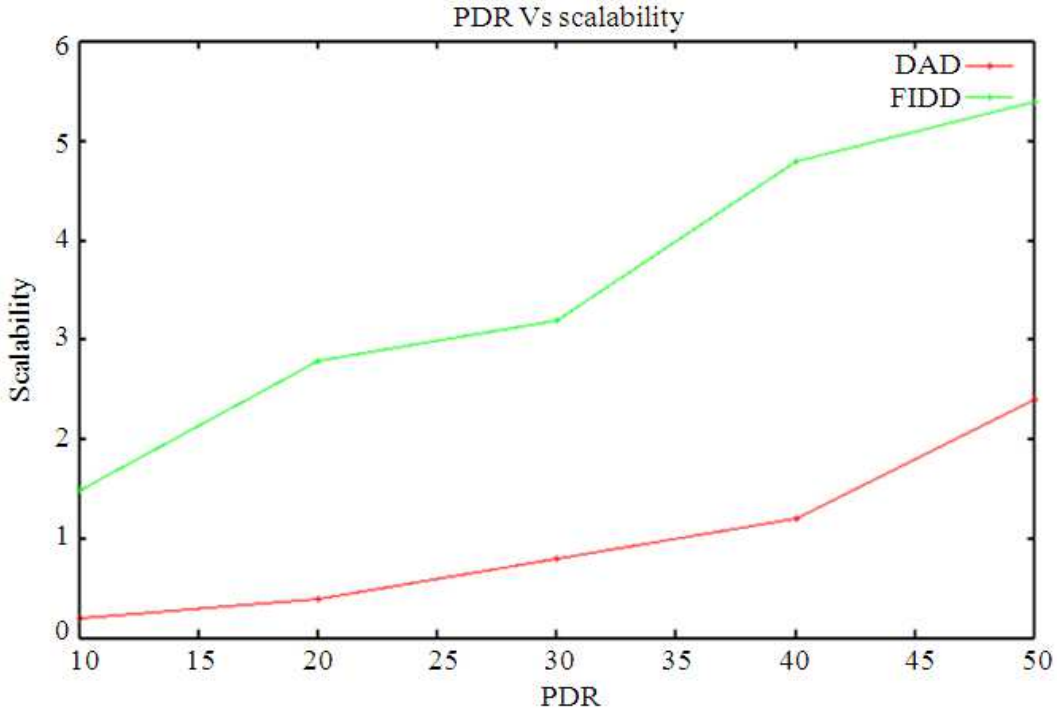

Fig. 1. Compare the performance of networks that uses DAD and FIDD protocol

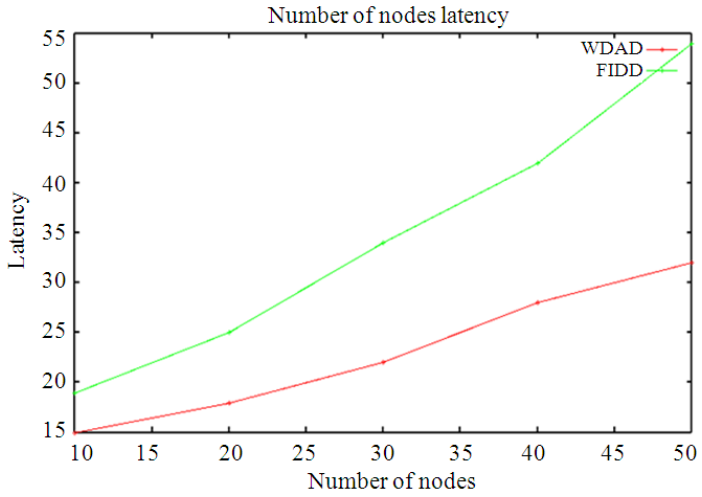

Fig. 2. Compare the performance of networks that employs DAD and FIDD protocol

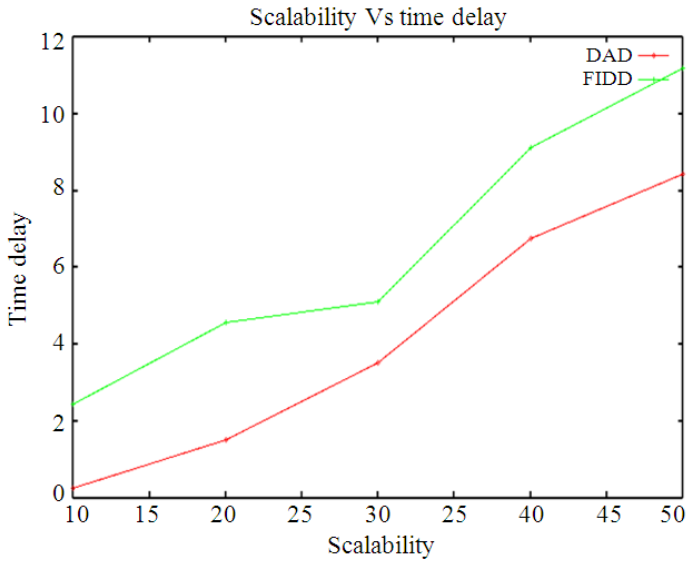

Fig. 3. Compare the performance of networks that uses DAD and FIDD protocol

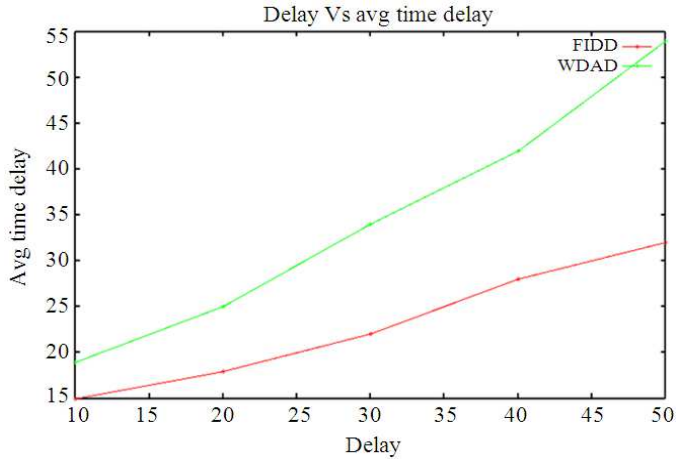

Fig. 4. Compare the performance of networks that uses DAD and FIDD protocol

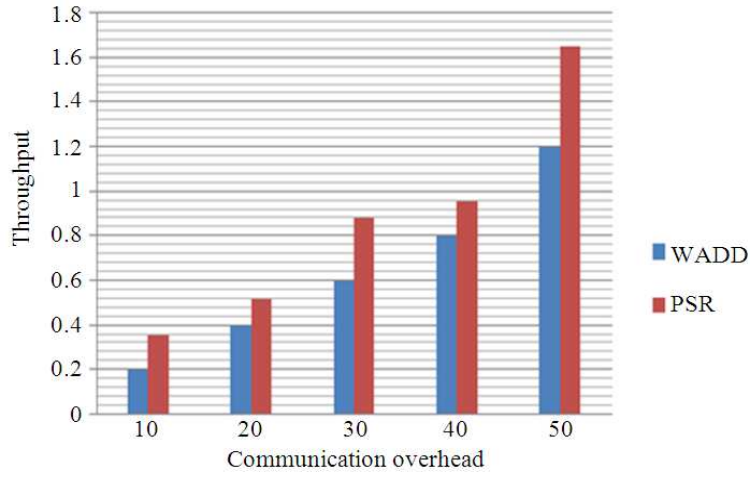

Fig. 5. Compare the performance of networks that uses WDAD and FIDD protocol

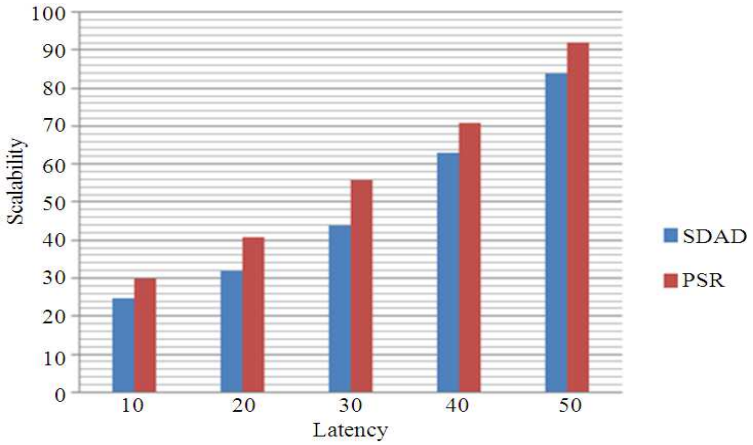

Fig. 6. The performance of networks that uses WDAD and FIDD protocol

In Fig. 6, we compare and here we particularly compare latency and scalability. The network that uses the FIDD protocol has high scalability and high latency.

Conclusion

Thus, we proposed Fake ID Detection (FIDD) protocol and Path Selection Routing (PSR) protocol in which the FIDD protocol is used to detect the fake id i.e., the duplicate packets and PSR protocol is used to select the alternate path when the current path became busy or failure. Here, we have dealt the effect of assignment of unique ID or IP address to mobile nodes in mobile ad hoc networks in the absence of whatever fixed configuration or centralized hosts. Such intention has been accomplished by a reactive scheme in handling fake addresses, besides through reserve options in the function of network resources, such as information quantity that are stored in the mobile nodes. The proposed protocol allots unique addresses and which can be merged with a several routing approaches. Moreover, the Address Information Holder assists in the discovery of duplicate addresses and deals address dispute behind the partition of the network and combines. The PSR protocol frequently chooses alternate path when the current path is busy or failure. Thus, the packet transmission process continuously occurs in the network. Hence, the efficiency and life-time of the ad hoc network can be increased. Finally, increased overall network performance is obtained. In future, we extend our research to provide security for the network by proposing new authentication protocol.

Funding Information

The authors have no support or funding to report.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Basagni, S., M. Conti, S. Giordano and I. Stojmenovic, 2004. Mobile Ad Hoc Networking. 1st Edn., John Wiley and Sons, Hoboken, ISBN-10: 0471656887, pp: 416.

Camp, T., J. Boleng and V. Davies, 2002. A survey of mobility models for ad hoc network research. Wireless Commun. Mob. Comput., 2: 483-502. DOI: 10.1002/wcm.72

Chlamtac, I., M. Conti and J.J.N. Liu, 2003. Mobile ad hoc networking: Imperatives and challenges. Ad Hoc Netw., 1: 13-64. DOI: 10.1016/S1570-8705(03)00013-1

Ganeshkumar, P. and K. Thyagarajah, 2010. Balancing throughput and fairness for concurrent flows based on per flow scheduling in ad hoc networks. Int. J. Comput. Applic., 32: 408-415. DOI: 10.2316/Journal.202.2010.4.202-28

Gopalakrishnan, S. and P. Ganeshkumar, 2014. Intrusion detection in mobile ad hoc network using secure routing for attacker identification protocol. Am. J. Applied Sci., 11: 1391-1397. DOI: 10.3844/ajassp.2014.1391.1397

Kim, N., S. Ahn and Y. Lee, 2007. AROD: An address autoconfiguration with address reservation and optimistic duplicated address detection for mobile ad hoc networks. Comput. Commun., 30: 1913-1925. DOI: 10.1016/j.comcom.2007.03.002

Mohsin, M. and R. Prakash, 2002. IP address assignment in a mobile ad hoc network. Proceedings of the IEEE MILCOM, Oct. 7-10, IEEE Xplore Press, Anaheim, CA, pp: 856-861. DOI: 10.1109/MILCOM.2002.1179586

Perkins, C. and E. Royer, 1999. Ad hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans, LA, pp: 90-100. DOI: 10.1109/MCSA.1999.749281

Perkins, C., J. Malinen, R. Wakikawa, E. Belding-Royer and Y. Sun, 2001. IP address Auto configuration for ad hoc networks.

Ros, F., P. Ruiz and C.E. Perkins, 2010. Extensible MANET Auto-Configuration Protocol (EMAP). Internet Draft.

Sun, Y. and E.M. Belding-Royer, 2003. Dynamic address configuration in mobile ad hoc networks. Department of Computer Science, University at Santa Barbara.

Thoppian, M.R. and R. Prakash, 2006. A distributed protocol for dynamic address assignment in mobile ad hoc networks. IEEE Trans. Mob. Comput., 5: 4-19. DOI: 10.1109/TMC.2006.2

Vaidya, N.H., 2002. Weak duplicate address detection in mobile ad hoc networks. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Jun. 09-11, Lausanne, Switzerland, pp: 206-216. DOI: 10.1145/513800.513826

Villalba, L.J.G., J.G. Matesanz, A.L.S. Orozco and J.D.M. Díaz 2011. Auto-configuration protocols in mobile ad hoc networks. Sensors, 11: 3652-3666. DOI: 10.3390/s110403652

Zahoor ul Huq, S., K.E.S. Murthy, B.S. Narayana and D. Kavitha, 2010. Study of detection of IP address conflicts in MANETS. Global J. Comput. Sci. Technol., 10: 23-26.

Velayutham, R. and D. Manimegalai, 2014. CCMP AES cipher for wlan (ieee 802.11i): A Comparison with DES and RSA. J. Comput. Sci., 11: 283-290. DOI: 10.3844/jcssp.2015.283.290