A Novel Technique to Detect and Isolate Selective Packet Forward Attack in MANET using Acknowledge based Scheme

Tarun Goyal
Research Scholar, M-Tech
Punjabi University Patiala

Meenakshi Bansal
Asst. Prof
Punjabi University,
Patiala

ABSTRACT
MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be composed either by mobile nodes or by both fine-tuned and mobile nodes. In MANET routing protocols for both static and dynamic topology are utilized. There are several security issues in MANET. Due to this various types of attack can be triggered easily in MANET. Selective packet drop attack is very easy to perform but indulge to isolate it. Network parameters are affected due to this attack and they degrade the performance of the network. In this paper, a novel technique is proposed to detect and isolate selective packet drop attack based upon IDS acknowledge based scheme after applying Diffie-Hellman technique. This novel technique isolated and detected attack in the network and improves its throughput and decrease packet loss.

Keywords
MANET, Selective Packet Drop Attack.

1. INTRODUCTION
Networking is used to replicate, swapping and share information like data communication. Allocation resources can be software type or hardware types e.g. routers. There is centralized master system that handles and supports these types of system. Networks can be classified as Wired and Wireless Networks. As the name only suggest one is organized with wired and another Wireless medium. Both can be differentiate by their characteristics of transmission medium, resources, hardware and software constraints. Different communication protocols being use to maintain network traffic, network size and selection topology. Wireless Networks term is refers to a kind of networking that does not require cables to connect with devices during communication. Radio waves are used for transmission at physical level. It is widely known as Wi-Fi or WLAN. According to wireless operation modes categories in 2 types:

1. Infrastructure
2. Ad-Hoc or Infrastructure less

In infrastructure predicated network, communication is takes place only between the wireless nodes and the access points. The communication is not established between the wireless nodes.

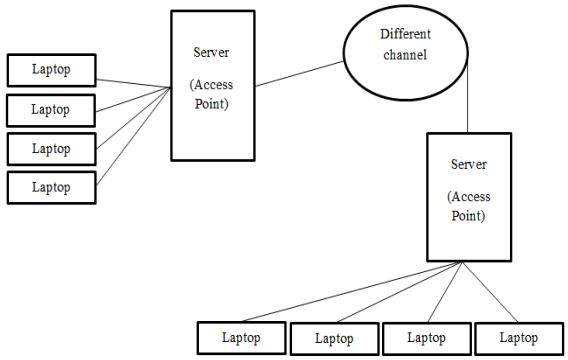

Fig 1: Infrastructure mode

Infrastructure less network is collection of many devices equipped with wireless communications and networking capabilities. Ad-hoc network is decentralized with no pre-subsisting infrastructure such as routers in wired networks or access points in wireless networks on which it is depended

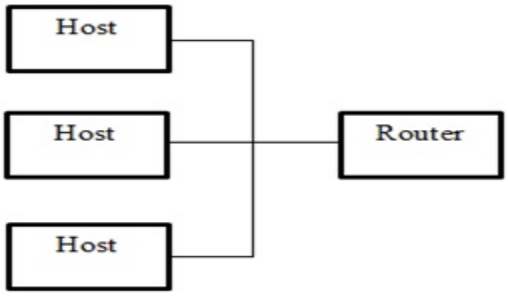

Fig 2: Block diagram of mobile node acting both as hosts and as router

It is further divided into three types i.e. MANET, Wireless Sensor Networks [6] and Wireless Mesh Network.

1.1 MANET
MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be composed either by mobile nodes or by both fine-tuned and mobile nodes. In MANET routing protocols for both static and dynamic topology are utilized [1].

To transfer the data between source and destination it follows a routing technique. A mobile host may not be communicate with the destination node directly in a single hop network design, in this view it should occur the multi hop scenario, where the packets can be sent through several nodes which acts as the intermediate between source and destination.

Location of the concrete node can be traced by the task of location vigilant routing protocols.

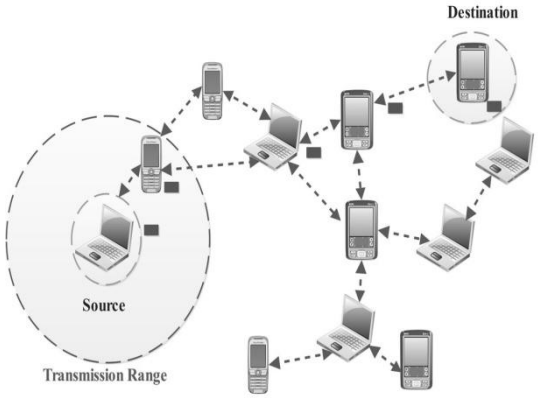

Fig 3: MANET

1.1.1 Attacks in MANET

There are a variety of attacks possible in MANET.

1. Active Attack
2. Passive Attack

1. Passive attacks: A passive attack obtains data switched in the network without disturbing the communications operation. The passive attacks are difficult to detection [2, 3].This attack target confidentiality attribute of the system. It includes accessing network traffic between browser and server accessing restricted information on a website. Examples of Passive Attacks are eavesdropping, snooping.

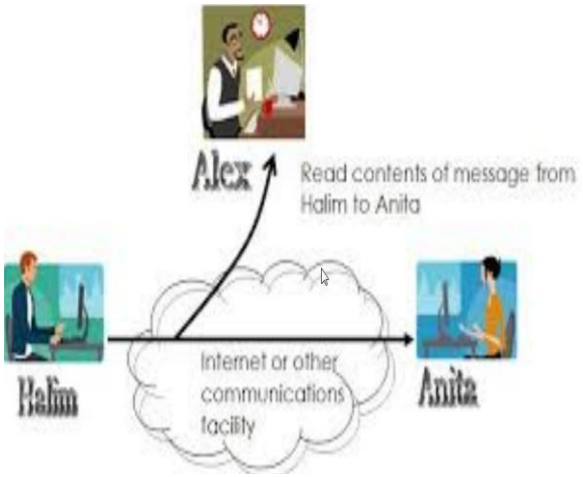

Fig4: Passive Attack

2. Active Attack: An active attack in which any data or info is interleaved into the network so that information and procedure may harm [2, 3]. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing**.**

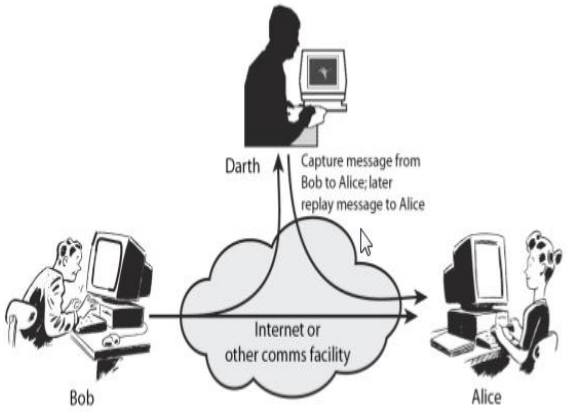

Fig 5: Active Attack

3. LITERATURE REVIEW

In this Paper [1], they present an overview of Ad hoc network that uses mobile nodes to enable communication outside wireless transmission range. We briefly describe the ad-hoc routing protocols, the attackers, attacks by the attackers and some suggestions and solution for secure routing protocols that follow the table driven and on- demand approaches. With the advances of wireless communication technology, low-cost and powerful wireless transceivers are widely used in mobile applications. Mobile networks have attracted significant interests in recent years because of their improved flexibility and reduced costs. A comparison between proposed solutions can provide the basis for future research with some analysis and suggestions. In this paper [2] they discussed about various routing protocols for Mobile value. To simulate this result they use Common Open Research Emulator (CORE).Ad-Hoc Network against security issues. MANET is vulnerable to various security attacks due to its dynamically changing topology, self configurable nature and lack of centralized control. Malicious node can significantly degrade the performance and reliability of Ad-hoc Network routing protocols. From the survey it has been made quite clear that basic MANET protocols are vulnerable to various routing attacks. While Secure AODV (SAODV) routing protocol performs quite well to improve performance in the presence of security attacks in MANET .In this paper [5] they discussed about the Mobile ad-hoc network is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to brutal challenges, the special features of MANET bring this technology great opportunistic together. In this [4] paper, they proposed new methodology how to detect and prevent selective packet drop attack. In this paper they discuss 4 previous methods to protect against 1.reputation based 2. Acknowledgement based 3. IDS based 4. Trust based. The new proposed schema called challenge and response schema. It contains 2 phase I) Key distribution phase II) Challenge and response phase. The message is encrypted using the public key and routed in two-hop neighbor, take ratio of local one compare it with neighbor node. The malicious node can be detected by setting threshold value to cache and at the end this value to the neighbor value. To simulate this result they use Common Open Research Emulator (CORE)..In this paper [5], they introduced that ad-hoc networks are frequently targeted by participating malicious nodes to sabotage the network. A common mechanism to protect these networks is through the

use of encryption and hashing mechanisms. However, the implementation of these mechanisms generally imposes certain unessential requirements, which are considered as restrictive for unplanned environments. In this paper, they discussed the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks connected to ad-hoc networks. With the help of the Network simulator they were able to prove that the proposed scheme increases the routing security and encourages the nodes to cooperate in the ad-hoc structure. This scheme is equipped with technique to identify and isolate the malicious nodes from the active data forwarding and routing. In this paper [6] they discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet delivery ratio and through put. The malicious node is detected based on the acknowledgement and energy level of the node. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate with various mobility and receiver sensitivity of the node. In this paper [7] they proposed efficient authentication mechanisms for low-power devices. In the proposed scheme the mobile station only need to pass one packet for mutual authentication .They used the elliptic-curve-crypto system based trust delegation Mechanism to generated group pass code for mobile station authentication. With the use of this authentication mechanism many active and passive attacks will be prevented including the denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one packet .This purposed mechanism is required less computations and less message exchange as compared to other authentication schemes.

4. SELECTIVE PACKET DROP ATTACK

Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched on the forward phase. So it is very complex and difficult to segregate. This attack is easy to trigger but very hard to detect it [4, 5]. Defected node also drops packet in their different ways. The main reason for drop packets is to save their resources only not to damage any other nodes. The main problem of selective forwarding attacks cannot distinguish malicious nodes or need time synchronization. Selective forwarding attacks can root stern threats on many applications. Attacker can kick off the selective forwarding attack and crash a segment of packets for which it require to store set while forward the rest.

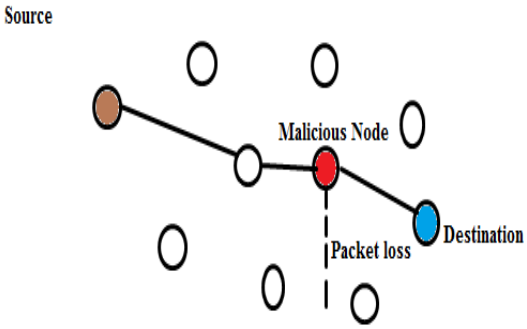

Fig 6: Selective Packet Drop

Selective Packet drop is barely feasible after the debacle of jamming attack. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehavior. Post-reception dropping is fewer bendy than selective jamming because the challenger is limited to dropping only the packets routed through it. Selective policy known as the Jellyfish attack which is a compromised node that is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero. This attack can be achieve even by remind random delays to TCP packets, without dropping them, while left over protocol compliant [6].

5. PROPOSED METHODOLOGY

A passive outsider eavesdrops on all communication and aims to compromise privacy. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the past, many techniques have been proposed to isolate Selective attacks from the network. When this attack is triggered in the network, end to end delay increase as steady rate and throughput of the network reduced. In this work, a new methodology is proposed to detect and isolate Selective Packet Drop attack in AODV Protocol.

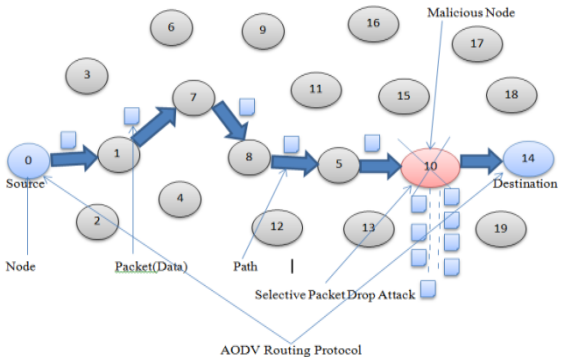

Fig 7: Packet Loss Due to Attack

There are nodes in the network one act as source and other act as destination. Suppose source sends packet from source to destination. It sends 10 packets. There is a malicious node at the centre which drops the packet and only forward few packets. This problem arise the packet loss problem. To

overcome this problem a novel technique will be proposed that is Diffie-Hellman.

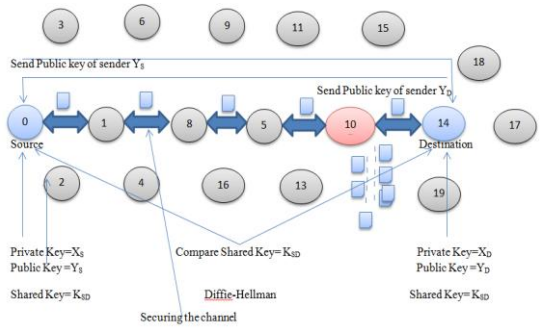

Fig 8: Diffie Hellman Technique

In fig 8**:** Diffie Hellman Technique is applied on Source and Destination. In this both Source and destination share their public keys and then applying their formula and generate some value using their private key. After that this value is shared between again source and destination. Then both source and destination decode this value using their private key. If both has same value then communication starts. If both keys do not match then Source sends ICMP messages and call monitor mode.

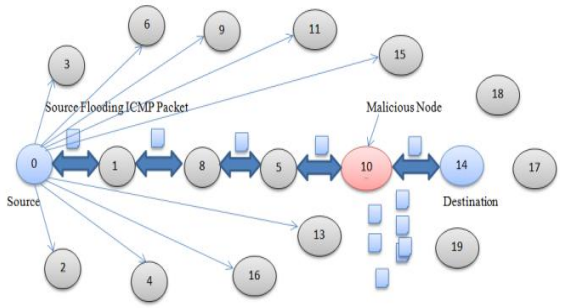

Fig 9: Send ICMP packets

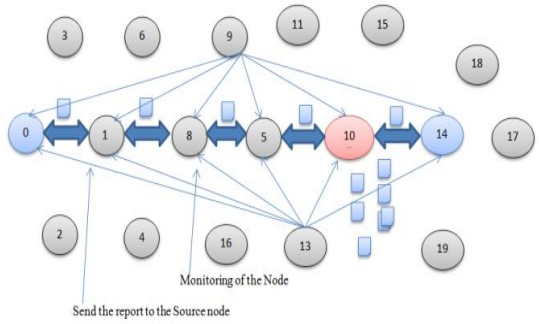

Fig 10: Detection of Malicious Node

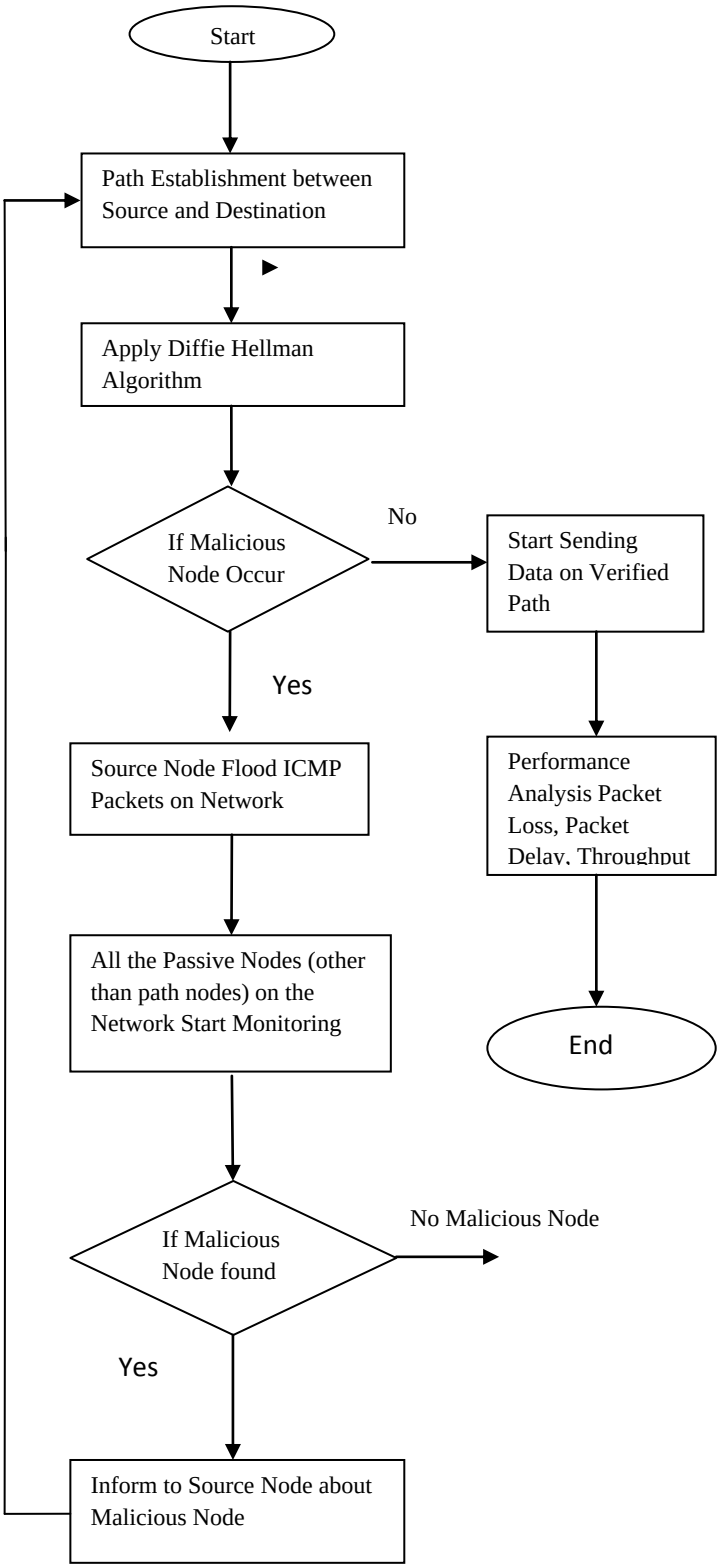

Fig 11 Flowchart of the methodology

6. EXPERIMENTAL RESULTS

The whole scenario has been implemented on NS2 simulator.

Fig 12: Delay Graph

In the figure, it is shown that graph of network delay. The network delay is more in the previous scenarios. The network delay is reduced in the new scenario

Table 1. Delay Comparison

Time (Seconds)	Old Technique Delay (Seconds)	New Technique Delay (Seconds)
4.0000	37	0
6.0000	92	0
8.0000	92	40
10.0000	92	60
12.0000	92	60

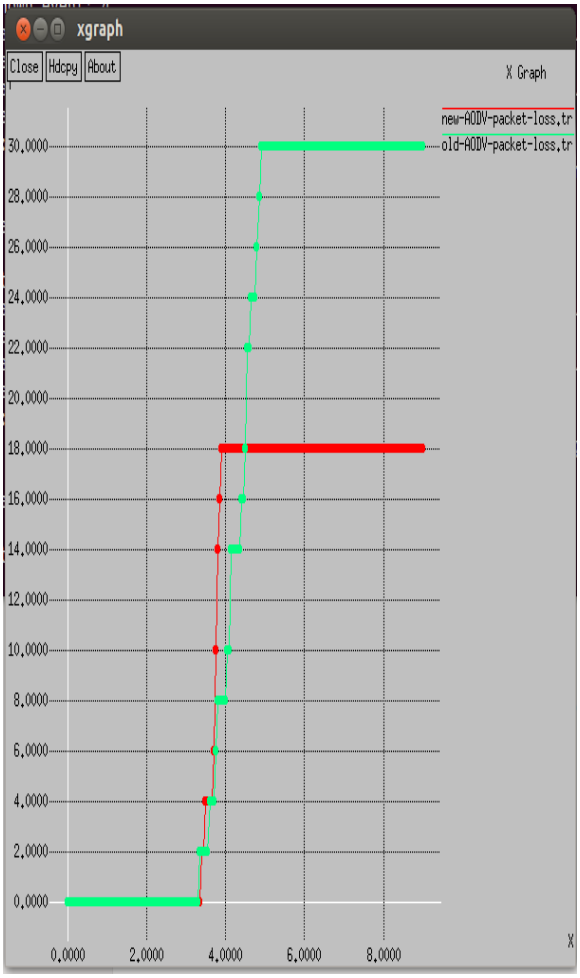

Fig 13: Packet loss Graph

In the figure, it is shown that graph of packet loss. The packet loss is more in the previous scenarios. The packet loss is reduced in the new scenario.

Table 2. Packet Loss Comparison

Time(seconds)	**Old Technique**	**New Technique**
2.0000	0	0
4.0000	10	18
6.0000	30	18
8.0000	30	18

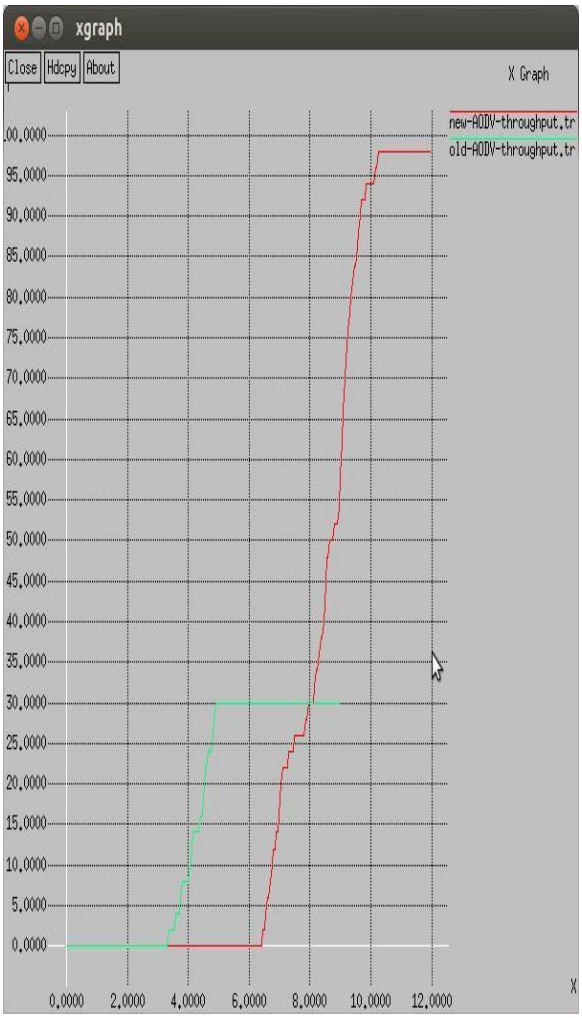

Fig 14: Throughput Graph

In the figure, it is shown that graph of Throughput. The network throughput is more in the new scenario. In the old scenario it will reduced due to selective packet drop attack in the network which is triggered by the malicious node.

Table 3. Throughput Comparison

Time(seconds)	Old Technique	New Technique
4.0000	10	0
6.0000	30	0
8.0000	30	30
10.0000	30	95

7. CONCLUSION AND FUTURE SCOPE

Mobile ad-hoc network have been vast area of research work from past few years because it is widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker. In this paper discussed about MANET, its attack which trigger on it and various techniques to isolate and prevent selective packet drop attack which degrade the system performance by decreasing throughput, increasing latency and end-to-end delay. There is acknowledgement and IDS based schema which prevent this attack in AODV protocol. In this feature work a new algorithm is proposed which is based on monitor node technique to which improves network efficiency. Although there was increased through put, reduced delay of packets and packet loss during the Selective Packet Forward Attack. It can be said that even if the proposed technique is better as compared to the existing technique yet there is further scope of improvement in the designed methodology and further investigation of the proposed methodology is required for better results.

8. REFRERNCE

[1] Garg V., Shukla M.K., Choudhury T., Gupta C., "Advance Survey of Mobile Ad-Hoc Network," IJCST Vol. 2, Issue 4, Oct. - Dec. 2011

[2] Patel C.V., Joshi A.H., Shah B.D., Patel C., "Security Attacks On MANET Routing Protocols" ,*International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue 10, Oct 2013*

[3] Goyal P., Parmar V., Rishi R.," MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011.

[4] Chuachan T., Puangpronpitag S., " A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANETs", 2013 IEEE

[5] Bhalaji N., Shanmugan A., "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", JOURNAL OF SOFTWARE, Vol.4, No.6, AUGUST 2009

[6] Sharmila S., Umamaheswari G.," Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012

[7] Tang C., Oilver D., "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE TRASACTIONS ON WIRELESS COMMUNICATION, VOL. 7, NO. 4, APRIL 2008.