Detection Of Malicious Nodes in Flying Ad-HOC Networks (FANET)

Eti Walia[#1], Vinay Bhatia[*2], Gurdeep Kaur[#3]
[#] *E.C.E Department Baddi University Of Emerging Science and Technology, India*

Abstract

The usage of Unmanned Aerial Vehicles (UAV) is increasing each day. The UAV network is the decentralized and self - configuring network in which nodes can join or leave the network any time. Security is the biggest challenge in flying ad-hoc networks (FANETs). In Sybil attack, FANET is unstable by malicious nodes which create fake identities. In this paper, a mutual authentication technique is proposed to detect Sybil attack in network. . A multiple copies of fake identities create by Sybil attack which is harmful for the network. Malicious nodes flood the wrong information in the network that degrades the network performance. In this paper, simulation results show the mutual authentication scheme is used to trigger the Sybil attack in network.

Keywords - *VANET, FANET, malicious node, Sybil attack, UAV to UAV communication*

I. INTRODUCTION

FANETs (Flying Ad-hoc Networks) is a group of Unmanned Air Vehicle (UAVs) communicating with each other with no need to access point, but at least one of UAV must be connected to a ground base or satellite. UAV can be small aircraft, drone and balloon. These are remotely controlled and pre-programmed networks. The applications of UAV networks are they are used in emergency situations such as flooding military and civil application (search and rescue operations, data mining, and forest fire detection. Security is the biggest challenge in FANET. There are several number of attacks occurs in the FANET. These attacks occurs due to malicious nodes enter in the network. However, dealing with these malicious nodes in FANET is the biggest challenging task in the network.

Security in the network is defined as the preservation of private information, authentication (confirm the true identity of person) [1]. Sybil attacks might be ruinous to a variation of FANET applications. Sybil attacks cause serious safety threats. For example, in the application of deceleration warning systems, if a UAV reduces its speed, it will broadcast a warning to the other UAV.

The remainder of the paper is organized as follows. Section II defines the various challenges and routing protocols in FANET. Sybil attacks in FANET are described in Section III. Section IV explains the proposed work. Simulation results are given in Section V. At last, Section VI approaches the conclusion of the paper.

II. FANET ROUTING PROTOCOLS AND CHALLENGES

A. FANET Routing Protocols

FANET is a subclass of MANET and VANET network. So, the MANET routing protocols are initially to chosen and tested for FANET. Due to various types of issues in UAV such as sudden change in link quality, most of these types of protocols are not directly available for FANET. FANET protocols can be classified into six main categories.

- *Static Routing protocols*: These protocols having fixed routing tables (no need to refresh these tables).Such protocols are data centric routing protocols and Load Carry and Deliver routing protocols.

- *Reactive routing protocols:* Reactive routing protocols can be refereed as on demand routing protocols. If there is no connection between the nodes, there is no need to calculate route between them. Such types of protocols are AODV, DSR.

- *Proactive routing protocols:* These protocols have periodically refreshed routing tables. The main advantage of these protocols is it store the latest information of routes. Such protocols are OLSR, DSDV.

- *Position geographic based routing protocol:* These protocols use position and area coverage. Position based routing information about the physical position of the nodes in the network. Such protocols are GPSR, LAR.

- *Hybrid routing protocols:* it is the combination of both proactive and reactive protocols. By maintain some form of routing tables these protocols reduce traffic overhead and reducing route discovery delays of reactive system [2]. Such protocols are ZRP, TORA.

B. FANET challenges:

- *Routing:* Routing in FANETs is different from other ad-hoc networks family. One of the biggest challenges is to develop an efficient routing algorithm that not only able to work with high mobility nodes but should be quick to update its routing table frequently as the topology changes [3].
- *Security:* Ensuring confidentiality, availability and Integrity of information during the communication between UAV to UAV communication and UAV to ground node communication security is one of the major issues faced by FANET [4].
- *QOS (Quality of Service):* In FANETs UAVs transmit data includes audio, video, images, text, GPS locations etc. To transfer such data it should have a good quality of service with less delays and error rates. [5].
- *Reliable data delivery:* FANET applications transfer very important information in different applications, which required to be delivered in time bound manner.so the reliability of the network is to be very high[6].

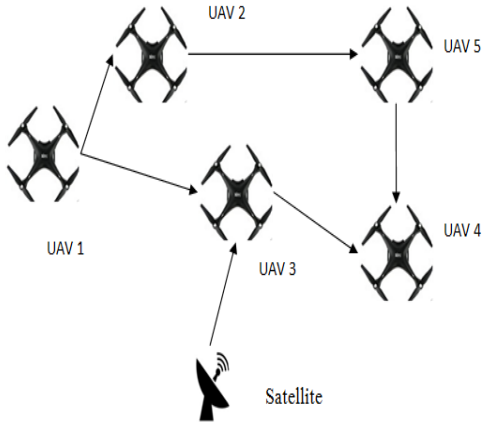


Fig 1: UAV network

III. SYBIL ATTACKS IN UAV NETWORK

In the beginnings of 2000s there was a hijacking incident of Predator UAV video stream due to which there was increase in interest of cyber security within UAV networks. In this attack, the cheap equipment's were utilized within the video steam by the militants in this network. It is very important to destroy any kinds of Sybil attacks occurring within the network which can be done with the help of huge funding and skills. There is a clear interest shown by various cyber and security departments in order to protect the systems from any Sybil attacks. Thus, there is a need to provide a deep study related to Sybil attack threats and vulnerabilities which can help in identifying and separating the attacks [7].

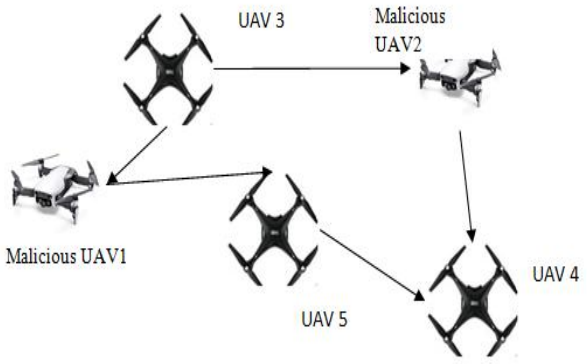


Fig 2: Sybil attack in UAV

There are five different categories of these attacks such as hardware attack, wireless attack, sensor spoofing, denial of service attack, distributed denial of service attack.

A. Hardware attack:

There is a direct access of the UAV autopilot components by the attacker. Due to this, the attacker directly attacks the hardware components. Any kind of data that is stored on-board by the autopilot is directly attacked here. It is possible that the attacker might install extra components which can cause the corruption of data flow of these networks.

B. Wireless attack:

If the wireless communication channels are utilized by the attacker for gathering or changing any data stored on-board, it is known to be a wireless attack [8]. An attacker can gain complete control over the UAV systems during the presence of this kind of attack in case where the knowledge of communication protocol is known to the user [8]. An attack also might occur here in which the data present on board can be buffered or any event can be initiated within the networks. The attacker can carry out the attacks from far places which is a very concerning issue.

C. Denial of Service Attacks:

DOS attacks are a type of attack which are caused by the network insiders and outsiders and provide the network which is not available to the real users. This is done by flooding the control channel with high amount of naturally generated messages and thus stopping the connection. [9]

D. Sensor Spoofing:

On the basis of the environment surrounding the network, the sensor spoofing attacks are directed towards the on-board sensors. With the help of GPS channels, the false data can be sent through GPS channels by the attacker [8].

E. Distributed Denial of Service Attack:

DDOS is more harmful than DOS attack because it is in distributed manner. Different types of locations

are used by the attacker to launch the attack. DDOS is possible at UAV2 to UAV and UAV2 to VANET. Its main objective is to slow down the network and jam the network [9].

BASICS STEPS TO SOLVE SECURITY ISSUES:

A. *Threats and Vulnerability Identification*:

In order to provide a verification of the flow in and out of the UAV network, a study is carried out initially on the complete network and its components [10]. Further, in various hypothesized ways of corrupting the data within the autopilot data flow path, the knowledge of the user of current autopilot system is utilized. The previous studies related to these network security issues are also studied here in order to provide an analysis about which kinds of methods have been utilized [11].

B. *Post-Attack Behaviour Analysis*:

A high fidelity aircraft model is utilized which helps in providing an extensive numerical analysis. This helps in studying the post-attack behaviour of UAV in case of particular types of Sybil attacks. In order to determine which kinds of attacks were most effective, various studies were also performed through which the different scenario were understood and utilized as per need.

IV. PROPOSED WORK

An approach is used to localize the fake identities by analysing the consistent similarity in neighbourhood information [12]. In this work, the new scheme had been proposed which will be based on to detection of malicious nodes from the network which are responsible to trigger Sybil attack in the network.

A. *Assumptions*:

The throughput of the network can be reduced because network resources get wasted [13]. The delay can be raised because packets are routed to wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

1) The speed of the UAV nodes are fixed on the defined roads
2) The central controller are responsible to maintain the information about all UAV nodes.
3) The UAV nodes have to present its neighbour node information to central controller units.
4) The central controller unit can maintain the neighbour node information about all the nodes.

B. *Illustration*

This work is based on to detect the malicious nodes from the network which are responsible to trigger Sybil attack in the network. The cyber is the distributed denial of service attack in which malicious node choose the legitimate node which will trigger attack on the victim node [14]. In the Sybil attack the malicious node will send the control packets to the legitimate nodes and legitimate nodes will send the route data packets to the victim node to trigger attack. In the work, technique will be proposed which will detect malicious nodes from the network and to detect malicious nodes following are the steps which are followed:-

1. In the first step, the network is deployed with the finite number of nodes. The fixed bandwidth is allocated to each node in the network.S

2. The Control units start analysing the bandwidth consumption of each node and node which is using the bandwidth above allocated value will be the malicious node.

3. In the third step, the control units check the type of packets which node is sending which is using the bandwidth above the allocated value. When the node is sending the data packets to the victim node, it may be the malicious node.

4. Any node that will be detected as the malicious node which is responsible to trigger DDOS attack. The nodes which are sending the rouge data packets, if that node will receive control packets from other node then node can be detected as the malicious node which is responsible to trigger DDOS attack.

C. *Detection algorithm steps:*

Steps of Detection Algorithm:
Step 1: Registration Process Start.
Step 2: Deploy the network with finite number of nodes.
Step 3: Central unit controller send the ICMP messages to each node.
Step 4: Each node send reply.
4.1 Each node send its neighbour node information to central controller unit.
4.2 controller unit exchanges received information.
Step 5: Repeat step 4 until all nodes cover.
Step 6: Check node neighbours.
6.1 If (node with same id, but different neighbours).
6.2 Mark the node as intruder node.
Step 7: Apply monitor mode technique on the intruder node.
Step 8: If the intruder node changes its identification then node is malicious.
Else Continue communication.

V. SIMULATION AND RESULTS

Simulation is performed using NS2 (Network Simulator-2) version 2.35. Some nodes are act as central controller unit and other are act as UAV nodes. For the detection of malicious nodes, two nodes are act as malicious nodes. AODV protocol is to be used

for communication with 512 bytes packet size. The whole arrangement is to be summarized in table I.

TABLE I
Simulation Parameters

Parameters	Values
Simulator	NS-2.34
Area	1000*1000
Number of nodes	35
Node speed	30m/sec
Malicious speed	2
Threshold value	60m/sec
Packet size	512kb
Packet type	TCP
Protocol	AODV

A. Monitor Process

as shown in figure, the central controller units flood ICMP messages in the network, it

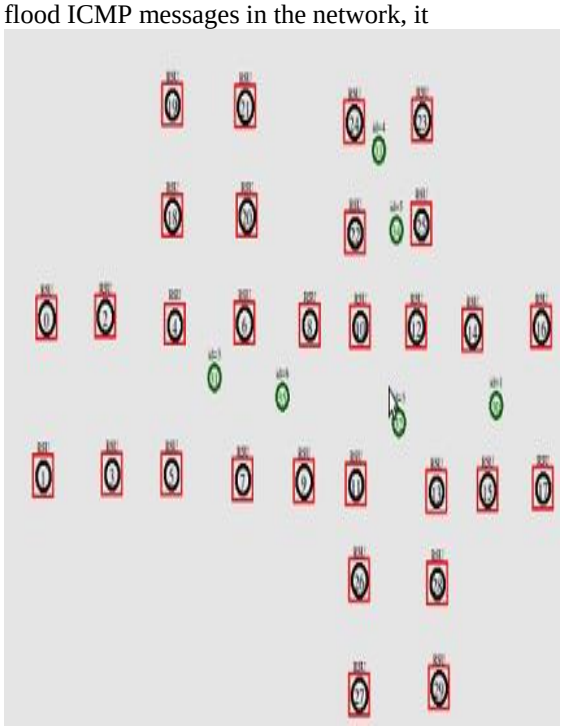


Fig 3: Monitoring process of malicious nodes

B. Detection of Malicious node

As shown in figure, when the central controller unit came to know that some Malicious nodes enter in the network, it flood ICMP message in the network, its adjacent nodes.

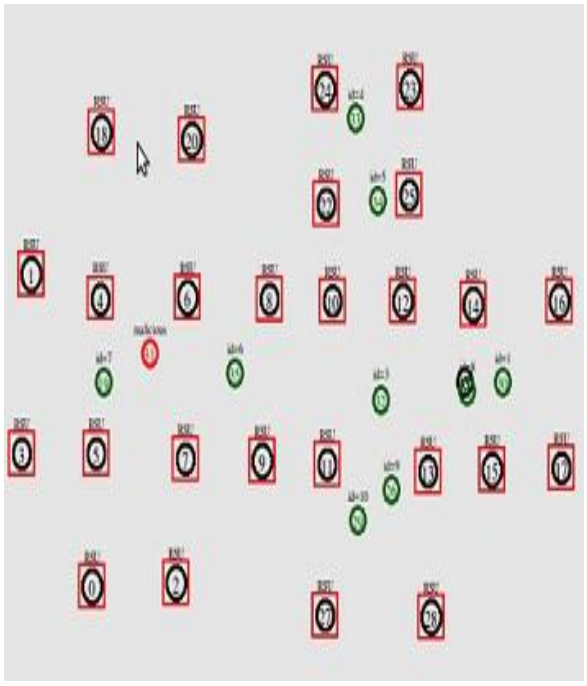
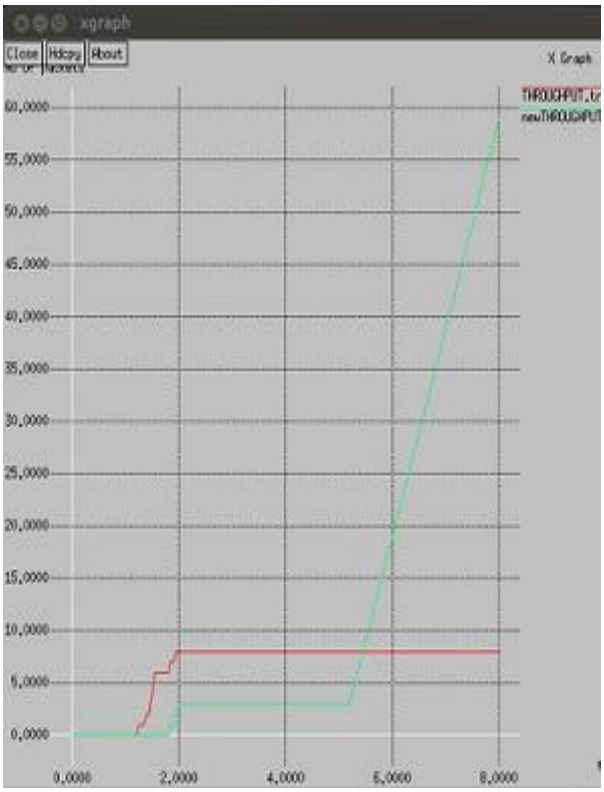


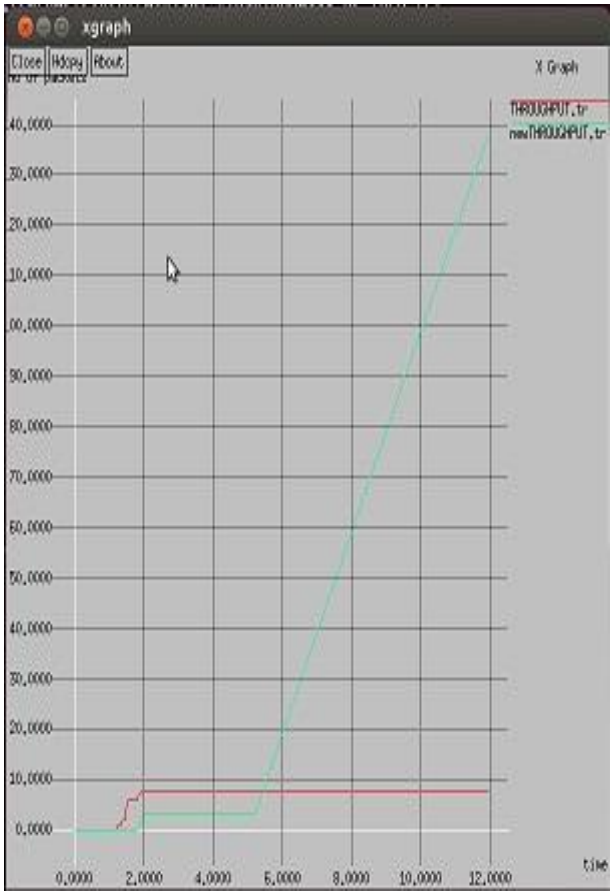
Fig 4: Detection of malicious node

C. Performance analysis:

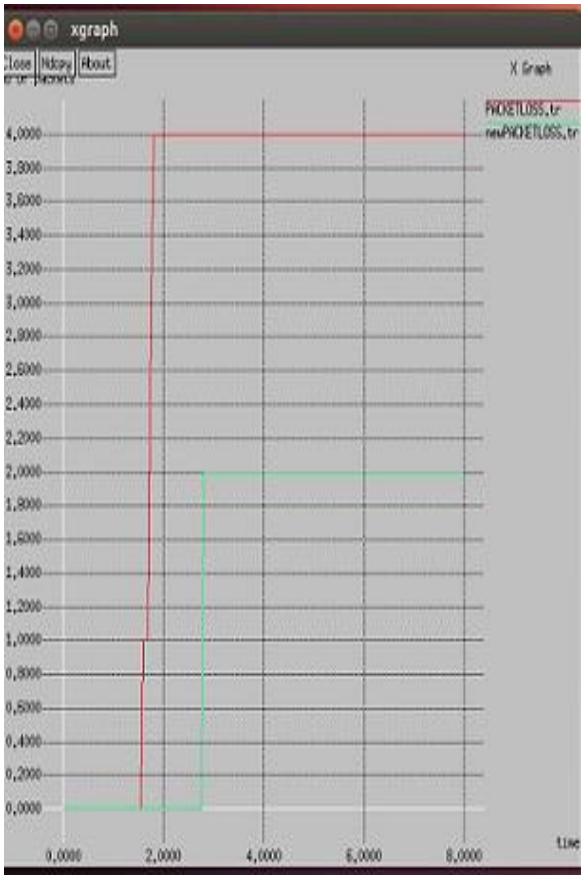
***Throughput*:** Throughput is defined as number of data packet receive per unit time [15].
Throughput= P/T



a. Simulation time for 8 sec



b. Simulation time for 12 sec



a. Simulation time for 8 sec

Fig 5: Throughput comparison between old and proposed technique (a, b)

TABLE II

Throughput

Existing technique	
Simulation time	No of packets
8s	80
12s	80
Proposed technique	
8S	90
12S	390

In this case, , comparison of existing technique is done with proposed technique. It has been analysed that proposed technique has maximum throughput over the existing technique.

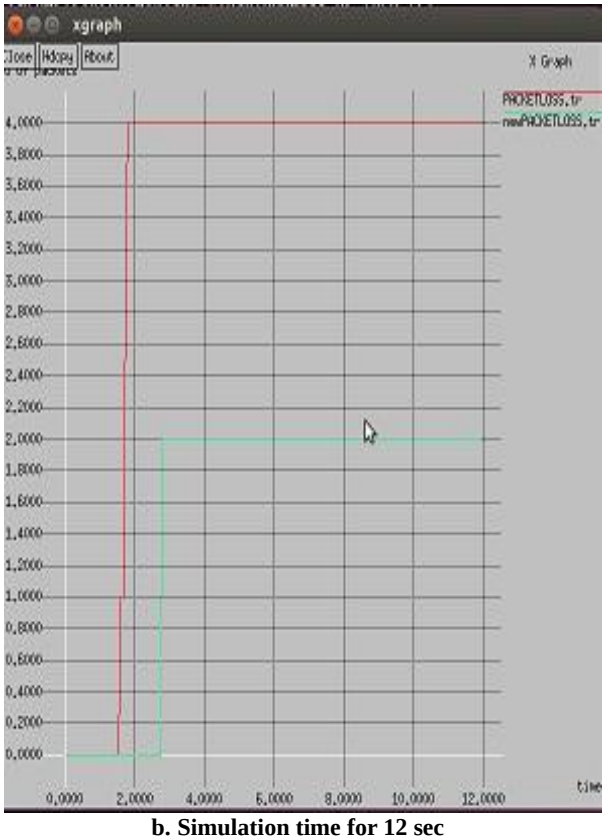
D. Packet loss ratio

Packet loss ratio is the ratio of the number of packets that are originated at source and receive at destination.

$$P.L.R = (SP-RP)/SP * 100$$

Where SP is number of Sending Packets

RP is number of Receiving Packet



b. Simulation time for 12 sec

Fig 6: Packet loss comparison between old and proposed technique (a, b)

TABLE II

Packet loss

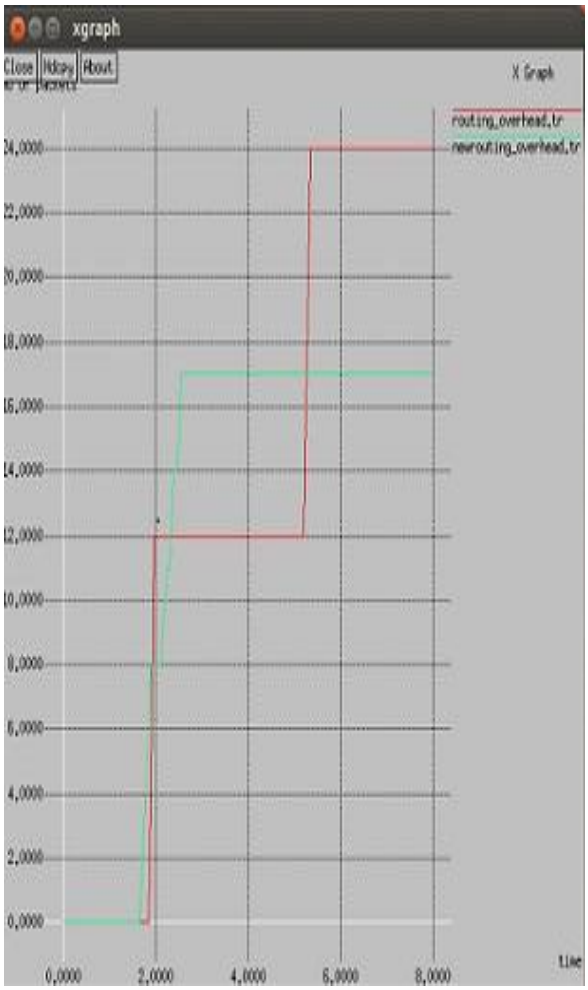
Existing technique	
Simulation time	No of packets
8s	40
12s	30
Proposed technique	
8S	20
12S	19

In this table, comparison of existing technique is done with proposed technique. Below is the table which shows how much packet lost in the used protocol and proposed technique. It has been analysed that proposed technique has least number of packet loss over the existing technique.

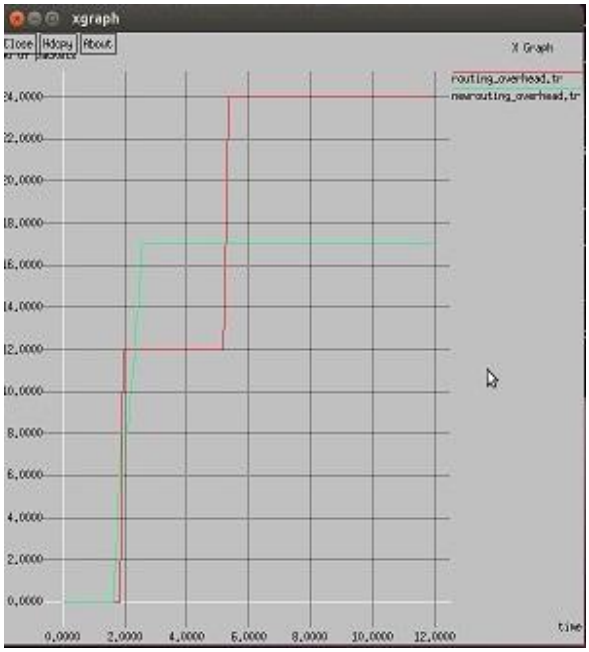
E. Routing Overhead

Routing overhead is defined as the number of data packets used for communication.

Routing overhead= routing packet send/total packets send



a. Simulation time for 8 sec



b. Simulation time for 12 sec

Fig 6: Routing Overhead comparison between old and proposed technique (a, b)

TABLE II

Packet loss

Existing technique	
Simulation time	No of packets
8s	40
12s	39
Proposed technique	
8S	20
12S	19

In this table comparison of existing technique is done with proposed technique. It has been analyzed that proposed technique has least routing overhead over the existing technique.

VI. CONCLUSION

In this research work, it has been concluded that UAV network is the ad-hoc type of network due to which malicious nodes enter in the network and trigger various type of active and passive attacks. The Sybil attack is the distributed denial of service attack which can flood the victim node with raw packets. The classification technique can classify the nodes into malicious, suspect and in legitimate class. For the detection of malicious nodes in the network mutual authentication technique will be proposed in this research. As results indicates that the proposed method generate maximum throughput as compare to other methods. Also the propose technique has least routing overhead and packet loss.

REFERENCES

[1] Man deep Kaur Saggy and Ramjet Kaur, " Isolation of Sybil Attack in VANET using Neighbouring Information", April 2015,pp.994206.

[2] Yanmaz, Costanzia, Bettstetter and W. Elmenreich "A discrete stochastic process for coverage analysis of autonomous UAV networks", "GLOBECOM Workshops GC Wkshps", 2010 IEEE, pp. 1777-1782.

[3] Sahingoz, "Networking models in flying Ad-hoc networks (FANETs)", "Journal of Intelligent & Robotic Systems", 74(1-2), 513-527 2014.

[4] Singh, A. K. "Applying OLSR routing in FANETs", " In Advanced Communication Control and Computing Technologies", (ICACCT), 2014 .

[5] N.M Rodday, R.D Schmidth "Exploring securities vulnerabilities of unmanned aerial vehicles", " in IEE/IFIP Network Operations and management symposium", (NOMS), April 2016, pp.993-994.

[6] D.Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks in Mobile Computing", (T. Imielinskiand H. Korth, eds.), Kluwere Academic Publishers.

[7] W.Saad, A. L. Glass, N. B. Mandayam, and H. V. Poor, "Toward a consumer-centric grid: A behavioural perspective proceedings ",IEEE, vol. 104, no. 4, pp. 865–882, April 2016.

[8] Vinay Bhatia, D.G Gupta and H.P Sinha, "Impact of security algorithms on various performance matrices of Wireless LAN", "international conference of wireless networks, LONDON, U.K, July – 2013).

[9] A.Ranet, S.sharma, "VANET security attacks and its possible solutions", "Journal of information and operation management, vol.3-no.1,pp 301-304" , 2012.

[10] Yap, W. SLiu, J. K., Tan, S. Yon the security of a lightweight authentication and encryption scheme for mobile ad hoc network. 2015.

[11] A.Sanjab and W.Saad, "Data injection attacks a smart grid" Vol.7, no. 4, pp.2038-2049, July 2016.

[12] G.E.Rahi, A. Sanjab, W. Saad, N. B. Mandayam, and H. V. Poor, "Prospect theory for enhanced smart grid resilience using distributed energy storage," in 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Sept 2016, pp. 248.

[13] W.Zafar and B. M. Khan, " "Networking models in flying ad-hoc networks(FANETs) Concepts and challenges", Journal of intelligent and Robotic Systems, vol. 74, no. 1, pp. 512-527, 2014.

[14] D.Johnson, D. A. Maltz, and J. Broch, "The dynamic source routing protocol for mobile ad hoc networks (Internet-Draft)",Mar. 1998.

[15] Vinay Bhatia and Gurdeep Kaur, " Evaluation and Improvement in AODV for Path Establishment using Bio Inspired Techniques" , "IEEE International conference of power, control and signal and institutional(ICPCSI)'' 2017.