International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8, Issue-9S, July 2019

VANET and FANET under the Impact of the Security Attack

Vinay Bhatia, Eti Walia, Parveen Singla

Abstract*: The flying ad hoc network (FANET) is a distributed type of network in which nodes have the ability to join or leave the network at any time as and when needed. FANET is the kind of ad-hoc network just like the Mobile ad-hoc network (MANET) and the Vehicular ad-hoc network (VANET). In our previous work a monitor mode technique is proposed for the detection of malicious nodes in Flying ad-hoc network (FANET). In this research work, a secure architecture for FANET and VANET is designed for the detection and isolation of malicious nodes in the network. The ad- hoc network is unstable when malicious nodes are present in the network which create fake identities, so that security of the network is to be reduced. A multiple copies of fake identities create by Sybil attack which is harmful for the network. In this research work, the performance of the proposed technique for the detection and isolation of malicious node of FANET is compared with VANET. It is analyzed that FANET performs well in terms of all parameters like throughput, packet loss and routing overhead as compare to VANET.

Keywords* : Mobile ad-hoc network (MANET), Vehicular ad-hoc Network(VANET), Flying ad-hoc network (FANET), Sybil attack, Malicious nodes, Unmanned aerial Vehicle Network(UAV).

I. INTRODUCTION

An emerging technology which is applied within military, public and civil applications is the Unmanned Aerial Mobiles (UAVs). The UAVs are also known popularly as drones. Flying ad-hoc network (FANET) are remotely piloted aircrafts. These networks have been applied in numerous applications due to their important characteristics which include high mobility and low cost. In order to minimize the losses of pilots these networks have been deployed largely in hostile territories such as military. The small sized UAVs can be easily accessed to public as they have very less cost and device miniaturization[1]. There are numerous applications emerging within the civilian and commercial fields which include the monitoring of weather, detection of forest fire, traffic control and various other services. There are numerous challenges being faced within the wireless communications performed within UAVs along with various advantages. In order to support safety-based functions like collision and crash avoidance, the Control non-payload and communication links (CNPC) that have higher latency and security requirements can be added along with normal communication links within these networks. For FANET communication thus there is a need of more efficient management and security method [2].

Revised Manuscript Received on June 25, 2019.
Vinay Bhatia, ECED, Chandigarh Engineering College, Landran, India.
Eti Walia, ECED, Chandigarh Engineering College, Landran, India
Parveen Singla, ECED, Chandigarh Engineering College, Landran, India

Highly dynamic network topologies that are sparsely and intermittently connected are provided in unmanned aircraft system (UAS) networks along with high mobility environment. In order to ensure reliable network connectivity, effective multi-UAV coordination is utilized. By considering the possibility of sparse and intermittent network connectivity, various communication protocols are also designed. On the basis of size, weight and power (SWAP) constraints of FANETs, another major challenge is raised in the network. This will result in limiting the communication, computation and endurance capabilities within these networks. Energy-aware FANET deployment and operation methods are required in order to handle such problems. These methods will help in providing intelligent energy usage and replenishment scenarios within the network. There will be unique security issues provided by UAVs [3]. A secure control of UAV flights is difficult when there is huge variation of flight environments, missions, and mobile sizes. Within the system design operational policies and procedures of FANETs, there is a need of security in the ground control station, data link design and the Mobile [4]. There is higher closeness of the MANET and VANET nodes to the ground level and amongst the sender and receiver there is no line-of-sight present. Due to the geographic structure, there are lots of variations seen in the radio signals. There is remote variation of the nodes that are far from the ground in FANETs and within UAVs, there usually seen a line-of- sight in such cases. In order to increase the lifetime of these networks, there is a need to develop energy efficient communication protocols [5]. Within the MANETs, since there are battery-powered computing devices available, there is a need to design energy efficient communication protocols carefully. However, there is an energy source provided in UAV systems for providing power to the FANET communication hardware. Thus, unlike MANETs, there is no power resource issue within the FANET communication hardware. Similar to the laptops and smart phones, the nodes of MANETs are small battery powered computers. There is however, inadequate computational power present within these nodes due to their size and energy constraints. Whereas, there is higher computational power within devices present in VANETs and FANETs. So as to obtain the coordinates of a mobile communication terminal, the GPS is utilized generally within MANETs. In most of the cases, in order to regulate the location of nodes, GPS is enough. There is a need of highly accurate localization data along with smaller time intervals within the FANETs. At one second interval, the position information is provided by GPS and for particular FANET protocols, this might not be appropriate [6]. Based on the issues & challenges extracted from literature survey as discussed in previous section there is still a lot of work need to be done in area of FANETs that includes security issues and management

of energy efficiently in the networks to detect the malicious attacks . A secured FANET architecture can be proposed in future for smart disaster management. It is also analyzed that a smart architecture can be develop with the co-existence of VANETs and MANETs. Along with the various challenges that arise within MANET and FANET also faces some separate challenges due to the higher node mobility, topology changes as well as the mobility models generated. From all the other ad hoc networks, there are various differences within the routing that occurs in FANETs due to higher node mobility in these networks. Thus, there is very frequently change in the topology of these networks [7]. Thus, an efficient routing algorithm which can handle high mobility nodes long with the updating of routing tables along with the changes arising in topology of these networks is required here which is a major challenge. Another major issue being faced in these networks is providing communication amongst the UAVs and UAV to ground by ensuring confidentiality, availability as well as integrity of the information required. Any malicious node in the network can disturb the whole network. Various types of attacks like Sybil attack, the black hole, wormhole, cyber-attack takes place in the network under which a legitimate node behaves like a malicious node.

II. THE NEED OF SECURITY IN AD-HOC NETWORKS

Although the ad hoc networks are widely used nowadays, still these networks have some vulnerability associated to them. Therefore, there arises a need of security so as to defend the network. An intruder utilizes this vulnerability to know about the processes utilized in the network and then attack the concerned network. So there are some vulnerability present in ad hoc networks.

A. Mobility

This forms one of the vulnerability as each node present in ad hoc network is movable. Thus it can join or leave a network at any time without informing any node. This gives a chance to the attacker to easily enter in the network.

B. Open Wireless Medium

Since medium of data transfer in these network is air, this medium can be compromised. This is because an attacker too has the access to this medium and creates a challenge to its security.

C. Dynamic Network Topology

Since nodes are highly movable in nature, so the topology keeps on changing dynamically each time the communication takes place. Therefore packets of information from source to destination may take a different path for communication. Here an attacker can introduce itself in any path.

D. Resource Constraint

Every node in mobile ad hoc network has limited resources like battery, computational power bandwidth etc. An intruder can unnecessarily waste these limited resources.

Fig. 1. Various Ad-hoc network

III. COMPARISON OF FANET WITH MANET AND VANET

FANET can be viewed as a special form of MANET and VANET. So, there are some differences between FANET and other existing ad hoc networks like MANET and VANET.

A. *Node mobility*

Mobility degree of FANET nodes is much higher than the mobility degree of MANET and VANET nodes[8]. While typical MANETs are mobile nodes such as mobile phones , laptops etc. VANET nodes are vehicles such as cars, bikes and FANET nodes are drones, quadcopters [9].

B. *Node density*

Node density is defined as the number of nodes in a per unit area. FANET nodes are normally spread in the sky, and the distance between UAVs can be several kilometres . As a result of this, FANET node density is much lower than in the MANET and VANET[10].

C. *Radio propagation model:*

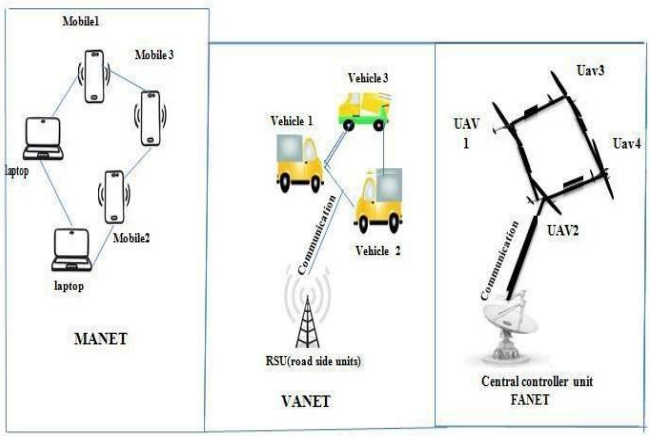
Flying ad-hoc network (FANET) affect the radio propagation characteristics. MANET and VANET nodes are very close to the ground and in many cases, there is no line of-sight between the sender and the receiver. Radio signals are mostly affected by the geographic structure. Again, FANET nodes those are away from the ground can be driven remotely and in maximum case, there is a line-of sight between UAVs [11].

D. *Energy consumption and network lifetime:*

The lifetime of the network is dependent on its energy consumption. Thus an efficient energy consumption protocol is a requirement for any ad- hoc network. The battery-powered devices in MANETs system developers have to pay extra attention to the energy proficient communication protocols. However, FANET communication hardware is powered by the energy source of the UAV. This means FANET communication hardware has no power resource problem as like in MANET[12].

E. *Localization:*

A MANET is typically characterized with a Global Positioning System (GPS) which is used to determine the position of the node in the a network. Here a GPS is enough to regulate the location of the nodes. However, in a VANET, there exists a navigation-grade GPS receiver, with an accuracy of about 10–15 m, which can be acceptable for route guidance. Due to high velocity and dissimilar mobility models of multi- UAV systems, FANET needs highly accurate localization data with smaller time intervals [3] GPS provides



position information at one second interval.

F. *Topology change:*

Flying objects are generally more mobile due to which topology of FANETs is more dynamic and changes very frequently as compared to its counterparts the MANET or VANNET.

IV. ROUTING PROTOCOLS IN FANET AND VANET

The routing protocols are the set of rules which are applied to establish path from source to destination. FANET is a sub-form of MANET and VANET network in which the nodes are the UAV. Due to decentralized nature of the network, routing is the major issue in network. So the routing protocols are classified into six main categories.

- *Static Routing protocols*: These protocols having fixed routing tables (no need to refresh these tables) viz. Data centric routing (DCR) , Load carry and deliver routing (LCDR) [13].

- *Reactive routing protocols:* Reactive routing protocols can be referred as on demand routing protocols. If there is no connection between the nodes, there is no need to calculate route between them. viz. are Ad-hoc on demand vector routing (AODV), Dynamic source routing (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. viz. Optimized link state routing (OLSR), Destination sequenced distance vector (DSDV).

- *Position geographic based routing protocol:* These protocols needs information about the physical position of nodes in the network. Generally each node calculates its own location through the use of GPS. viz. Global positioning system routing (GPSR), Location aided routing (LAR)[14].

- *Hybrid routing protocols:* it is the combination of both proactive and reactive protocols. By maintaining some form of routing tables these protocols reduce traffic overhead and reducing route discovery delays of reactive system [15]. viz. Zone routing protocol (ZRP), Temporally ordered routing algorithm (TORA).

V. RESEARCH METHODOLOGY

So, in this work first of all we will study what is flying ad- hoc network, need of security in the network, routing protocols and comparison of FANET with MANET and VANET. A comparative analysis will be done between the VANET and FANET for the detection and isolation of malicious nodes in the network. It has been analyzed that FANET performs well rather than VANET.

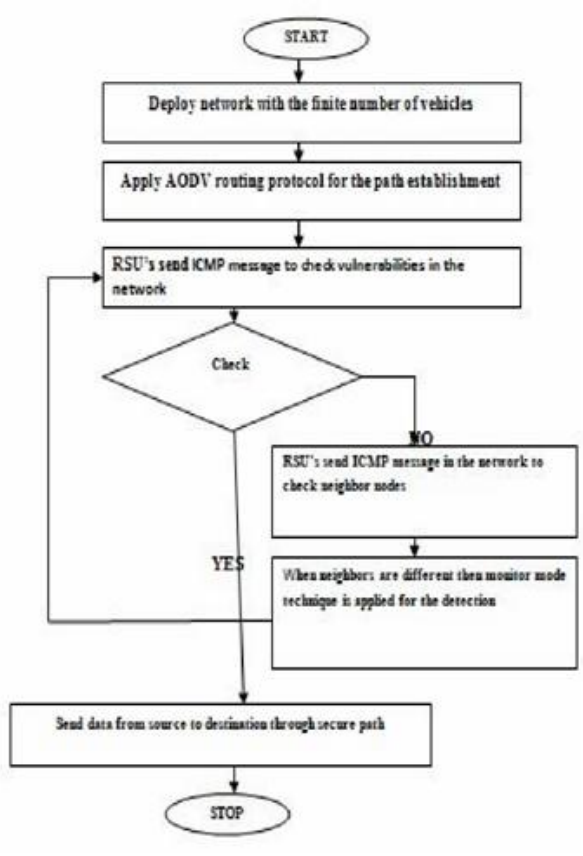


Fig. 2. Proposed Architecture of VANET

The malicious nodes enter the network because of the decentralize and dynamic nature of the networks. These malicious nodes trigger various active and passive types of attacks in these networks. The identification of a legitimate node is spoofed by an active type of attack known as Sybil attack. The throughput of network is minimized since the required data does not reach to the legitimate node. The Sybil attack is triggered within the network because of the presence of malicious nodes which are identified and eliminated in this research with the help of proposed technique. On the basis of monitor model techniques, the signal strength is introduced in the proposed technique. The Internet control message protocol (ICMP) messages are flooded within the network by the road side units within the proposed technique. The complete information is collected by the road side units and then the data is shared by them[16]. It is assumed that node might result in causing intrusion within the networks which has multiple signal strength values. The control packets and sent within the network by the road side units in order to confirm which node is malicious. The vehicles which initiate monitor mode and will begin to observe the adjacent nodes after they receive the control packets. The malicious node is identified here and multiple path routing is applied through which the malicious nodes present in the network are eliminated.

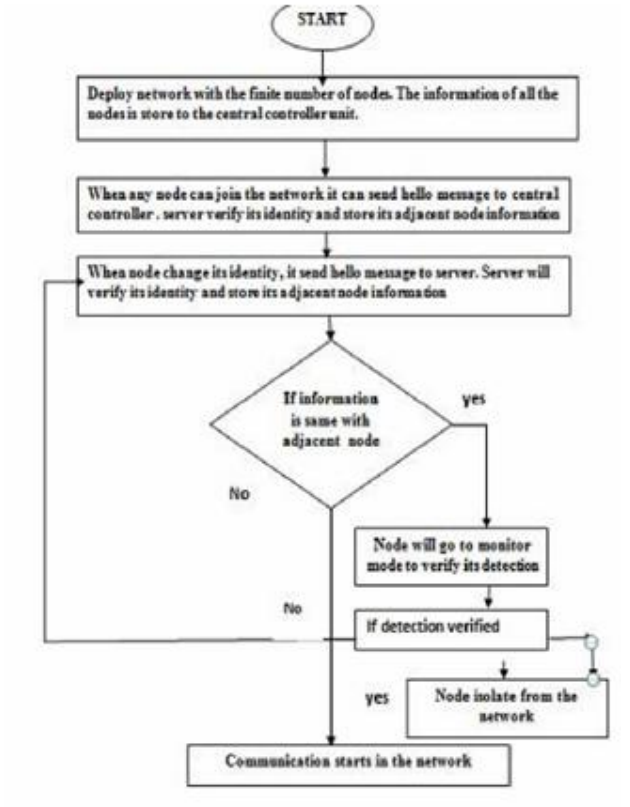


Fig. 3. Propose architecture for FANET

VI. SIMULATION ANALYSIS METHOD AND RESULTS

The proposed FANET approach is implemented in NS2 and the results are evaluated by making comparison against proposed and VANET approach with respect to several parameters.

TABLE I: SIMULATION PARAMETERS

Platform	Ubuntu
NS Version	Ns-allinone-2.35
Protocol	AODV
Simulation time	8s
No of nodes	40,50 and 60
Simulation area size	800*800m
Mobility model	Random Mobility
Traffic	CBR type
Packet size	512kb
Node speed	30m/s
Number of exchange packets	1000

A. Monitor Process:

As shown in figure, the RSU (Road side units) floods ICMP messages in the network[18].

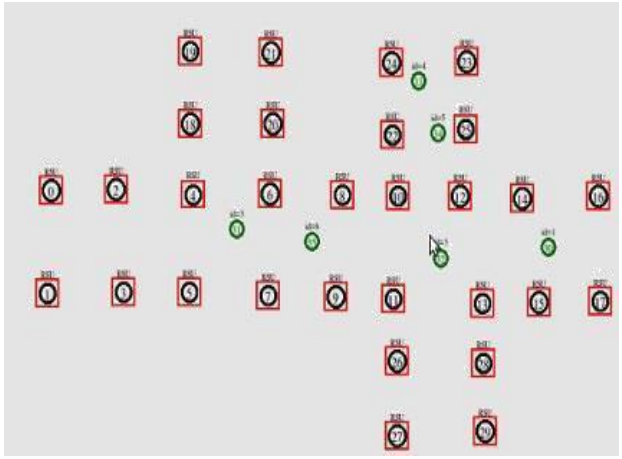


Fig. 4. Monitoring process of malicious nodes in VANET

As shown in the figure , When the central controller unit came to know that some malicious nodes exists in the network, the central controller send hello messages in the network[17]. The UAV nodes in the network receive hello messages and start monitoring its adjacent nodes. From the monitoring mode technique, the malicious nodes are detected in the network.

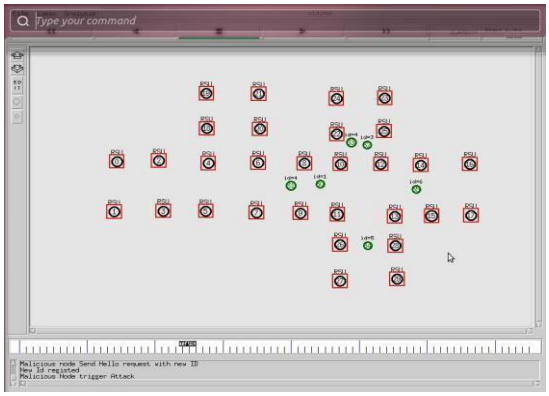


Fig. 5. Monitoring process of malicious nodes in FANET

B. Detection and isolation of Malicious node:

As shown in figure 6, when the road side unit came to know that some malicious nodes enter in the network, it flood ICMP message in the network, to its adjacent nodes

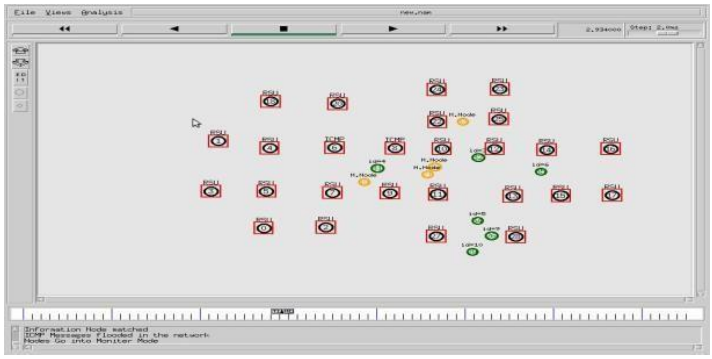


Fig. 6. Detection and isolation of malicious nodes in VANET

As shown in figure 7, when the central controller unit came to know that some

malicious nodes enter in the network, it flood ICMP message in the network, to its adjacent nodes.

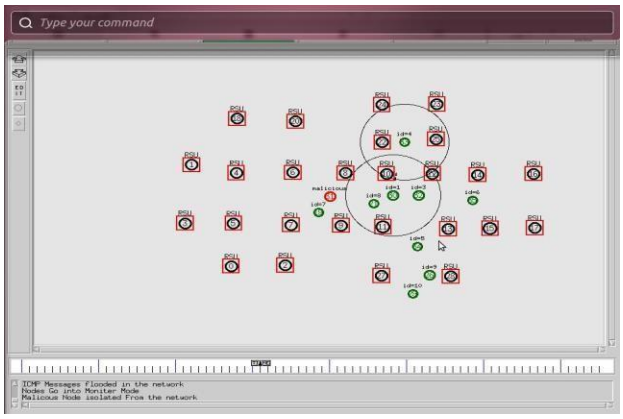
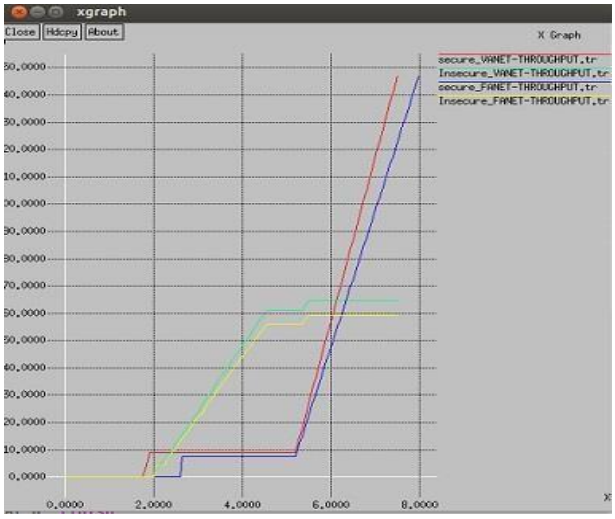


Fig. 7. Detection and isolation of malicious nodes in FANET

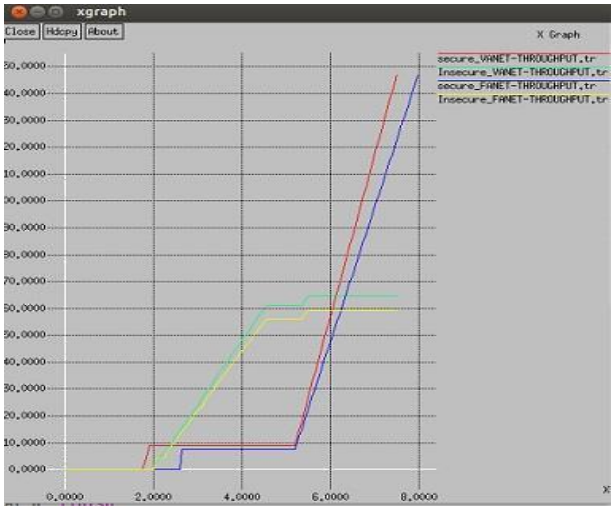
PERFORMANCE ANALYSIS:

A. Throughput:

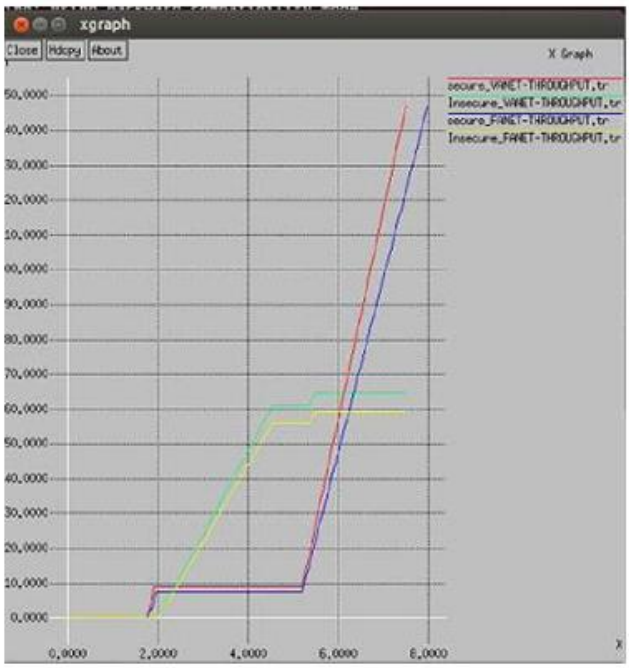
It is defined as the number of packets received in the network in given amount of time [19].



a. Throughput comparison at node 40



b. Throughput comparison at node 50



c. Throughput comparison at node 60

Fig. 8. Shows throughput simulation (a, b, c)

Table II. Throughput comparison between secure and insecure VANET

Throughput		Existing Technique in VANET	Proposed Technique in VANET
Simulation time	Number of nodes	Number of packets received	Number of packets received
8s	40	65	140
8s	50	68	149
8s	60	70	149

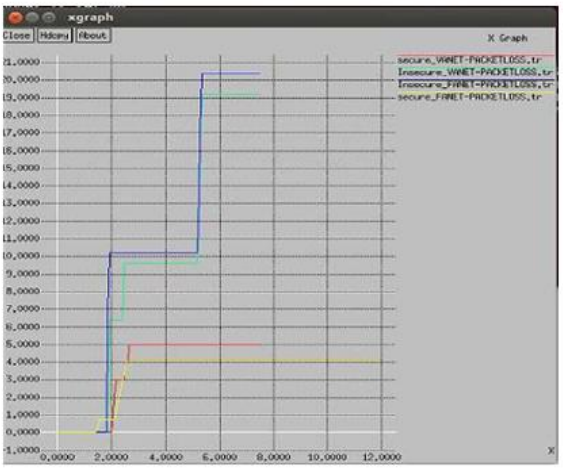
Table III. Throughput comparison between a secure and an insecure FANET

Throughput		Existing Technique in FANET	Proposed Technique in FANET
Simulation time	Number of nodes	Number of packets received	Number of packets received
8s	40	60	140
8s	50	58	145
8s	60	60	150

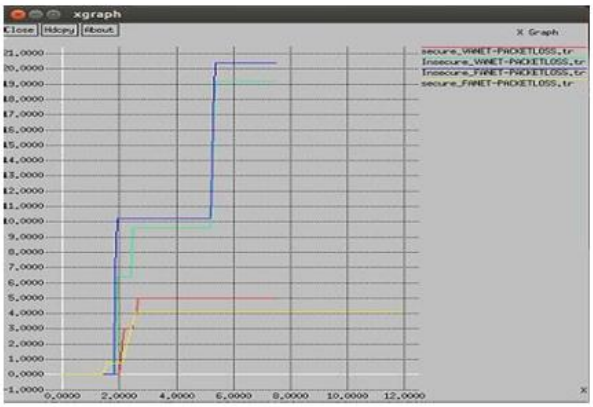
As shown in figure, the throughput of secure architecture of VANET is analysed with the secure architecture of FANET at node 40, 50 and 60. It has been analysed that secure architecture of FANET has maximum throughput and perform well as compared to secure architecture of VANET.

B. Packet loss:

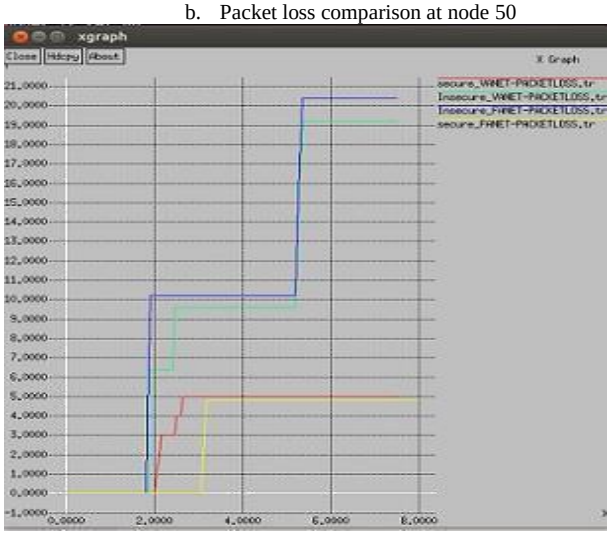
This loss is the result of non-delivery of packets to the required destination node after they have been sent succesusfully by the source. [20].



a. Packet loss comparison at node 40



b. Packet loss comparison at node 50



c. Packet loss comparison at node 60

Fig. 9. shows packet loss simulation(a, b, c)

Table V. Packet loss comparison between secure and insecure VANET

Packet loss		Existing Technique in VANET	Proposed Technique in VANET
Simulation time	Number of nodes	Number of packets received	Number of packets received
8s	40	100	50
8s	50	105	50
8s	60	190	50

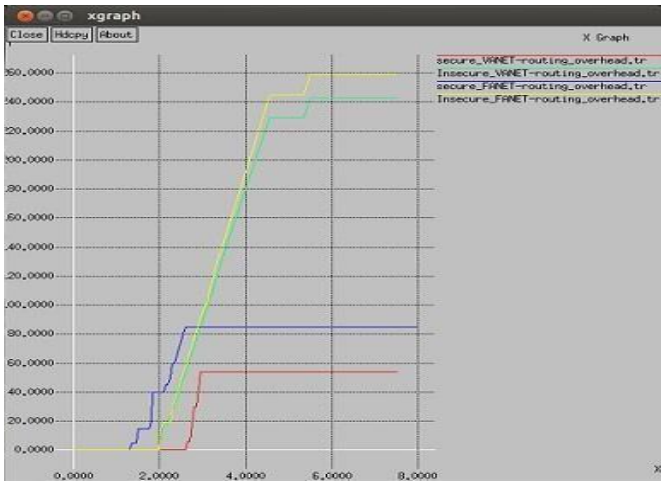
Table VI. Packet loss comparison between secure and insecure FANET

Packet loss		Existing Technique in FANET	Proposed Technique in FANET
Simulation time	Number of nodes	Number of packets received	Number of packets received
8s	40	800	40
8s	50	800	40
8s	60	200	40

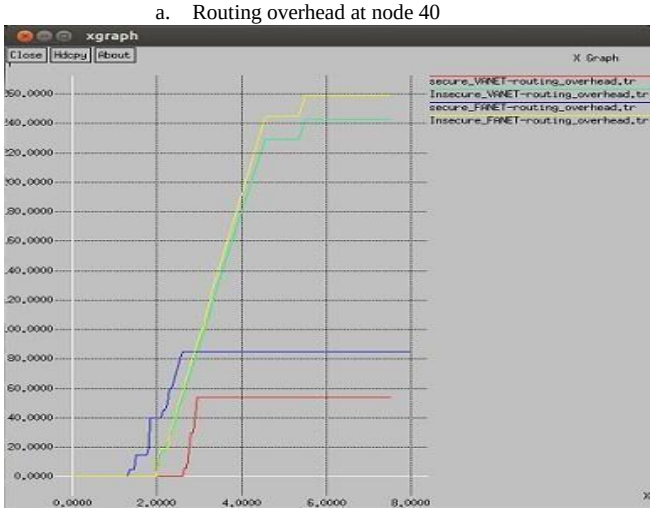
As shown in figure, the packet loss of secure architecture of VANET is analysed with the secure architecture of FANET at node 40, 50 and 60. It has been analysed that secure architecture of FANET has least number of packet loss and perform well as compared to secure architecture of VANET .

C. Routing Overhead:

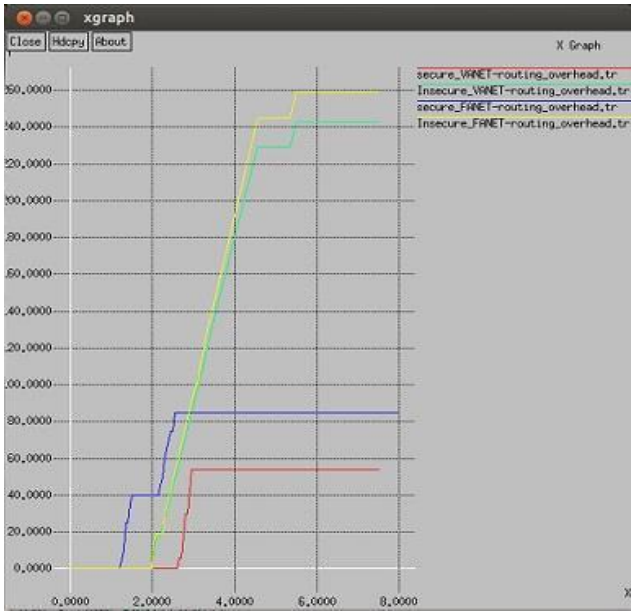
Routing overhead is defined as the number of extra packets that are collected during the transmission process in the network[22].



a. Routing overhead at node 40



b. Routing overhead at node 50



c. Routing overhead at node 60

Fig. 10. Shows routing overhead simulation (a, b, c)

Table VII. Routing overhead comparison between secure and insecure VANET

Routing overhead		Existing Technique in VANET	Proposed Technique in VANET
Simulation time	Number of nodes	Packet causing routing overhead	Packet causing routing overhead
8s	40	260	80
8s	50	240	80
8s	60	250	90

Table VIII. Routing overhead comparison between secure and insecure FANET

Routing overhead		Existing Technique in FANET	Proposed Technique in FANET
Simulation time	Number of nodes	Packet causing routing overhead	Packet causing routing overhead
8s	40	240	50
8s	50	240	50
8s	60	345	50

In this figure, the routing overhead of secure architecture of VANET is analysed with the secure architecture of FANET at node 40, 50 and 60. It has been analysed that secure architecture of FANET has least routing overhead and performs well as compared to secure architecture of VANET .

VII. CONCLUSION

The FANET is decentralized type of network in which UAV nodes can join or leave the network when they require. Due to decentralized nature of network, routing, quality of service and security is the three major issues of FANET. In this research work, it has been concluded that UAV network is the ad-hoc type of network due to which malicious nodes enter the network and trigger various type of active and passive attacks. . In the base paper, the technique is proposed which detect and isolate malicious nodes from the network which are responsible to trigger Sybil attack. In this research work, secure architecture is proposed for the detection and isolation of malicious node in both FANET and VANET. The performance of FANET and VANET is analyze on the basis of certain parameters like throughput, routing overhead and packet loss. The simulation of proposed model is performed in NS2 and it is analyzed that secure architecture of Flying ad-hoc network (FANET) performs well in terms of throughput, packet loss and routing overhead as compared to Vehicular ad-hoc network. It has been analyzed that FANET performs well than VANET.

Future prospective of this work includes that routing overhead parameter can be improved with the help of some optimization techniques.

REFERENCES

1. Gatteschi, F. Lamberti, G. Paravati, A. Sanna, C. Demartini, A. Lisanti, and G. Venezia, ―New frontiers of delivery services using drones: A prototype system exploiting a quadcopter for autonomous drug shipments,‖ in 39th IEEE Annual Computer Software and Applications Conference (COMPSAC), vol. 2, July 2015, pp. 920–927.
2. K. Mansfield, T. Eveleigh, T. H. Holler, and S. Sakami,Unmanned aerial vehicle smart device ground control station cyber security threat model,‖ in IEEE International Conference on Technologies for Homeland Security (HST), Nov 2013, pp. 722–728.
3. N. M. Roddy, R. d. O. Schmidt, and A. Pars, Exploring security vulnerabilities of unmanned aerial vehicles,‖ in IEEE/IFIP Network Operations and Management Symposium (NOMS), April 2016, pp. 993–994.
4. W. Sad, A. L. Glass, N. B. Mandayam, and H. V. Poor, Toward a consumer-centric grid: A behavioural perspective,‖ Proceedings of the IEEE, vol. 104, no. 4, pp. 865–882, April 2016.
5. G. E. Rahil, A. Sanjeev, W. Sad, 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. 248–255.
6. Hichem Sedjelmaci, Sidi Mohammed Senouci, and Nirwan Ansari, A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks‖, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, vol. 88, pp. 1-13, 2017.
7. Kwanwoong Yoon, Daejeon Park, Yujin Yim, Kyounghee Kim, Szu Kai Yang, Myles Robinson, Security Authentication System using Encrypted Channel on UAV Network‖, 2017 First IEEE International Conference on Robotic Computing, vol. 78, pp. 1003-110, 2017.
8. E. Yanmaz, R. Kuschnig, and C. Bettstetter, Channel measurements over 802.11a-based UAV-to-ground links,‖ GLOBECOM Wi-UAV Work. shop, pp. 1280–1284, 2011.
9. Jin Li and Youngnam Han, Optimal Resource Allocation for Packet Delay Minimization in Multi-layer UAV Networks‖, 2016, IEEE
10. Krishan Yadav, Amit naan, Sunil Makkar, Routing Protocols in FANET: Survey, National Conference on Innovative Trends in Computer Science and engineering(ITCSE-2015).
11. Eti Walia, Vinay Bhatia, Gurdeep Kaur, Detection of malicious nodes in flyong ad-hoc networks‖, SSRJ-IJECE), International journal of electronics and communication engineering, Sep 2018.
12. Vinay Bhatia andGurdeep 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.
13. Vinay Bhatia, Dushyant Gupta Throughput and Delay Analysis of wireless LAN Security Protocol implementing NS2‖,Internatioal Journal of Applied Engineering Research (IJAER) may 2015.

AUTHORS PROFILE

Prof.(Dr.) Vinay Bhatia is a B.Tech, M.Tech, Ph.D in

Electronics and Communication Engineering. Currently he is serving as Professor and Head, Department of Electronics and Communication Engineering at CGC Landran. He has authored about 90 research papers in various national/international conferences/journals. Currently he is working on routing and security issues pertaining to wireless networks. His main research interests include mobile and ad-hoc wireless networks, wireless mesh networks and wireless securities.

Dr. Parveen Singla, did B.Tech in Electronics and Communication Engg. from Hindu college of Engineering, Sonepat affiliated to Maharishi Dayanand University, Rohtak in 2003 and M.Tech in Electronics and Communication Engg from N.C College of engineering, Panipat affiliated to Kurukshetra University, Kurukshetra in 2008. He did PhD in ECE from IKGPTU in 2016. His total teaching & research experience is 15 years. Now he is working as Associate Professor in Electronics & Communication department in Chandigarh engineering college. He has more than 20 publications in various reputed journal/conferences. His research area includes wireless communication and soft computing.