Balance-AODV Routing Protocol using Neural Network Prevention in Wireless Mesh Network

Amanpreet kaur[1], Er.Jyoti Rani[2]
[1]*M.Tech (Scholar),* [2]*Assistant professor*
Department of Electronics & Communication Engineering, SUS College of Engineering & Technology, Tangori, Mohali, India

Abstract **–** Network is among the self-systematize, self-configured and multi-hop wireless network that render wireless services to variant applications. These applications involve broadband home networking, community, transport system, security surveillance systems, health and medical system etc. used in personal, local campus and metropolitan areas. Due to dispersed nature of WMNs, it is vulnerable to various attacks. viz internal or external. Sybil attack is among the recurrent types of attack in the wireless mesh networks. Due to extensive employment of broadband internet access, WMNs are more susceptible to Sybil (multiple copies) attack. In this paper, we propound different types of attacks in a network used that alleviate the upshot of sybil attack in the network. Balance on demand distance vector routing protocol and Feed forward Neural Network technique to establish algorithm which considers packet delivery, throughput and delay. The existing position aware secure enhance routing protocol are compared using new approach or the conception of the secure technique that is implemented in FFNN and B-AODV with Mesh wireless network based on routing technique. Our proposal prevents worm attack than the IEEE 802.11s/i security mechanisms or the well-known, secure FFNN without making restrictive assumptions. In realistic UAV-WMN scenarios, Compare PASER achieves comparable presentation results as the well-established; Routing-classified combined with the IEEE 802.11s security mechanisms. We calculate the performance parameters result achieved like the Packet Delivery rate is 97%, throughput is 90% or less end to end Delay and reduce the energy consumption.

Keywords **–** *Wireless Mesh Network, Sybil attacks ,PASER and FFNN (Feed Forward Neural Network).*

I. INTRODUCTION

A network predominately comprises of wired and wireless technologies through which it communicate. Wired networks incorporate optical fibre ,coaxial cable or copper wires to form a twisted pair among users. In terms of a computer network, a network is defined as series of points or nodes, interconnected by communication paths for transmitting, receiving and exchanging data, voice and video traffic. Exchange of information materializes with the aid of switches and routers (Network devices) via various versions of protocols and algorithms. These endpoints may embrace cellular radio broadcast radio, microwave or satellite.

Networks are categorized by extent of their domains. Local area networks (LAN- interconnects endpoints in a single domain). Wide area networks (WAN-interconnects multiple LANs), and metropolitan area networks (MAN-interconnect computer resources in a geographic area). Storage area networks (SAN-interconnect storage devices and resources). Network categorization based on span of topologies includes Wireless sensor networks (WSNs), which is a large scale network of small embedded devices, escorted by sensing, computational and communication capabilities. However in WSNs, the sensor nodes have constraints in terms of processing power, communication bandwidth and storage a space which required very efficient resource utilization [1].

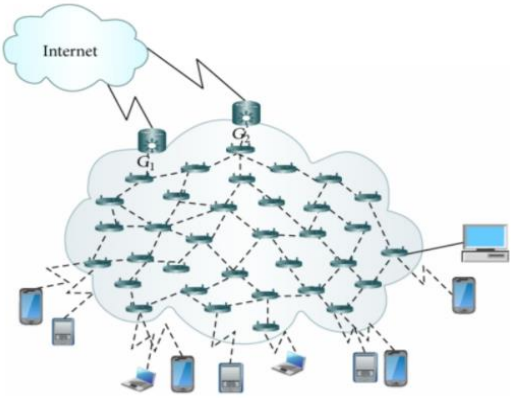

Fig 1. Mesh Network

Mobile Ad-hoc networks (MANET) are a wireless ad-hoc network which is self-configuring and accommodate network of mobile users connected via wireless links. It is one of the types of wireless network without having cumbersome infrastructure. Network topologies alter frequently as mobile nodes are free to move randomly, leading to network partition, route change and loss of information. Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network (MANET) that provides communication between vehicles and vehicles-road-side base stations with an aim of yielding efficient and safe transportation. Unmanned aerial vehicles combined with a WLAN mesh network forms the airborne mesh network. A secure routing protocol approach for the deployment of UAV-WMN aims to provide:

- *Efficient Secure Routing:* A combination of symmetric and asymmetric cryptosystems.

To take the specifies of the target network into consideration like closed network with main nodes.

- *Set of Routing's Band Key Management:* To resolve the inter-dependency cycle between key management and secure routing.

Balanced- AODV is one of the reactive routing protocol means that only on demand it creates path to destination node. Pure AODV uses traditional routing tables and destination sequence number is used for identification of latest route to a destination and formation of routing loops. Although BAODV protocol performs well with mobile knobs it incurs high above with an increase in network size. BAODV is an on –Demand routing protocol. Route is calculated on demand, via route discovery process.

II. USES AND CHALLENGES IN WMNs

Assignable to the recent amelioration in research, WMNs, are desired numerous applications. These applications are as numerated below:

1. *Home networking:* Broadband home networking is a network of home appliances (personal computer, television, video recorder, video camera, washing machine, refrigerator etc.) apprehended by WLAN technology. WMNs administer broadband connectivity between the home networking devices with the aid of single Internet connection through the gateway router.
2. *Disaster Management and Rescue Operations:* WMNs are useful at places where spontaneous network connectivity is solicited, such as disaster management and emergency operations. During disasters like fire, flood, and earthquake, all the existing communication infrastructures might collapse.

Consequently during the rescue operation, mesh routers can be installed at rescue team's vehicle and at different locations which form the high-bandwidth mesh backbone network.. Different communication interfaces at the mesh routers confer access to different mobile devices of network. This abets public users to communicate with others when they are in critical circumstances. These networks can be established in insignificant time, which makes the rescue operation more effective.

There are prevalent challenges in wireless mesh network that are as follows:

1. *Directional Antennas:* Principally in WMNs, directional antennas are exploited which scale down the interferences between the simultaneous transmissions and also cut down the transmission power for long distance communications. Notwithstanding, directional antennas can significantly complicate the design of upper layers [4].
2. *Mobility:* WMNs are barely capable of supporting supplemental user mobility therefore it is mandatory for physical layer to support fast fading conditions associated with mobile users.
3. *Authentication:* Data is transferred amid the authenticated users in the network. Unauthorised users deferred services in the network[5].

III. RELATED WORK

Ahmed E. A. A. and et. al. [6] worked on unmanned aircraft systems. In this process there are many unmanned aircraft system and ground base stations are configured. These are responsible to create a UAS network and communication of data packets from one to another node. Ahmed investigated some problem during setup and operating this type of terminology. These problem cause high operating cost and maximize the time consumption of network communication.

Author also investigates the adaptive modulation effects on the network and their communication with this architecture using a small design of a game based on formulated potential for checking the performance and energy consumption of current scenario [7].

Various security issues in the wireless networks along with their some routing challenges were also considered. They also assume some attacks in the wireless networks. Attacks can degrade the performance of the network [9].

They stole information with many anonymous routes in the network. Different attacks are having their own way to perform degradation on the network. Some of them are working with some kind of clone node and other are working with by pushing a heavy load on the network. These types of attacks are known as DDos attacks. Dos attacks applied through a heavy load of request pushing on the server which will just to degrade the processing speed of the network. Various techniques are also there for prevent these type of attacks. Most common technique is encryption of data packets when data travel from intermediate node in the network or authentication scheme for the network node etc.

AggelikiSgora, and et. al. [8] survey about mesh networks in wireless communication. The mesh network technology can save much more cost for communication as compare to other networks. It's a high speed network which can be combination of various other topologies. Due to their very flexible behavior it can be easy to adjustable in all the conditions and can provide much more satisfaction for their users. In future the mesh networks can be used as high speed communications in wireless mediums [10]. Author analyzes the fundamental security challenges in the wireless networks. It can degrade the performance of the network with less security. Attack can affect various parameters of the network as throughput, packet drop, and delay in communication.

IV. ATTACKS

In this section discussed the various types of attacks in network security.

a) Sybil Attack

In peer-to-peer network, computer bank on assumptions of identity, where each computer represents a single identity. Sybil attack is a type where a node in a network claims multiple identities. This attack emerges when an insecure computer is hijacked to plea multiple identities. Here the node fakes multiple identities and claims itself to be a distinct nodes on the network though it is just a single malicious node. The sybil attack hampers the routing protocols by creating false links between a honest and a malicious node. The attack can have detrimental effects on resource allocation, misbehaviour detection, disrupting communication by stealing information and voting techniques in the wireless networks. It is essential to recognize a Sybil attack and transcript its hazards. Since Sybil attack is a harmful attack in distributed peer-to-peer systems therefore almost all such systems are based on a common assumption that each participating entity controls exactly one identity[11].

Sybil attack was first exposed in distributed computing applications where the redundancy in the system was exploited by creating multiple identities and controlling the considerable system resources. In the networking scenario, a number of services like packet forwarding, routing and collaborative security mechanisms could be disrupted by the adversary using sybil attack.

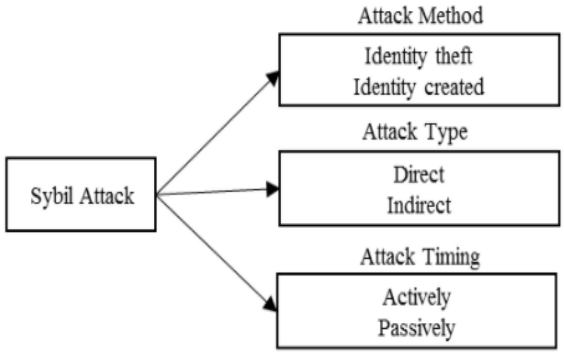

Fig 2: Sybil attack

The above figure shows Sybil attack. Here the wireless mesh networks are equally prone to network partitioning attacks and routing loop attack. In network partitioning attack, the malicious nodes collude together to disrupt the routing tables in such a way that the network is divided into non-connected partitions resulting in denial of service for certain network portion. Routing loop attacks affect the packet forwarding capability of the network. When the packets are forwarded to these fake nodes, the malicious node, that created the identities, processes these packets. Thus creating multiple identities, this attack degrades the performance of wireless mesh networks.

b) WormHole Attack

A wormhole is an attack on the routing protocol of a Mobile Ad-hoc Network. Wormhole attack is also known as tunneling attack. A mining attack is where two or more nodes may cooperate to encapsulate and [12] conversation messages between them along current data routes. In a wormhole attack, an attacker obtains packets at one point in the network, "shafts" them to another point in the network, and then repetitions them into the network from that point.

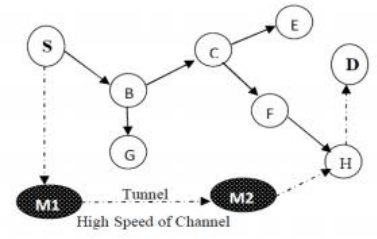

Fig 3: Worm Hole Attack

In overall, wormhole attacks consists two spiteful nodes burrowing traffic from one end of the network to the other For tunneled reserves longer than the regular wireless broadcast range of a single

hop, it is simple for the assailant to make the excavated packet arrive with better metric than a normal multichip route, for example through use a only long-range directional wireless link or finished a direct wired link to a colluding attacker.

V. RESULT AND DISCUSSIONS

Before we can proceed with performance evaluation, we must choose the different metrics that would help us in making comparisons. There could be different metrics to determine the performance like throughput, delay, packet delivery and energy consumption. The choice of metric would depend upon the purpose the network has been set up for. The metrics could be related to the different layers of the network stack.

The table 1 below shows different metrics of evaluation, and categories they are appropriate for

Category	Metric	Units
Delivery	Packet Delivery	%ge
Accuracy	Throughput	%ge
Buffer Issue	Energy Consumption	Joules (j)
Time	Delay	ms

Table 2. Proposed Performance Parameters

Performance Parameters	Values
Delay 0%	64.63ms
Delay 10%	6.4ms
Delay 20%	12.93ms
Throughput	98%
Packet Delivery rate	98.4%
Energy Consumption	2.4Joules

Following are some of the performance measurement metrics:

(i) **Throughput:** The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second.

(ii) **Packet Delivery :**Packet delivery ratio is the ratio of packets successfully received to the total sent.

(iii) **Energy Consumption:** The energy consumption is the sum of used energy of all the nodes in the network, where the used energy of a node is the sum of the energy used for communication, including transmitting (Pt), receiving (Pr), and idling (Pi). Assuming each transmission consumes an energy unit, the total energy consumption is equivalent to the total number of packets sent on the network.

(iv) **Delay :** It refers to the time taken for a packet to be transmitted across a network from source to destination.

Table 3. Comparison between Packet delivery Rate (Proposed and Existing work)

Time [ms]	Packet delivery rate FFNN	Packet Delivery Rate PASER
100	84	54
200	89	58
300	93	60
400	95	69
500	98	70

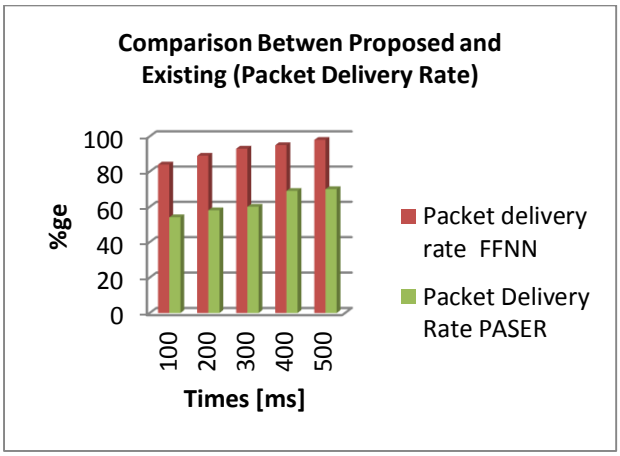

Fig. 4. Comparison (Packet Delivery rate) with FFNN

The figure represents that the comparison based on PASER and FFNN in the PDR (%). We improve the packet delivery with FFNN and PASER. We implement the proposed approach to enhance the performance of the information transmission.

VI. CONCLUSION AND FUTURE SCOPE

Security is an exceptionally crucial concern in wireless mesh networks. Sybil attack is one of the major attack-occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages and/or other commands. The analyse the B-AODV with FFNN secure approach in UAV-WMN. It is shown that B-AODV with FFNN mitigates in the investigated situations, more attacks than the well-known, secure routing protocol and the standardized security mechanisms of IEEE 802.11s/i. The efficiency of B-AODV with FFNN is explored in a theoretical and simulation-based analysis of its route discovery process, and its scalability with respect to network size and traffic load is reasoned. Using the network simulator MATLAB, realistic mobility patterns of UAVs, and an experimentally derived channel model of UAV-WMN, it is demonstrated that in UAV-WMN-assisted network provisioning and area exploration scenarios PASER have a comparable performance with that of the well-established, non-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms. Last, the benefits of B-AODV with FFNN were recently presented in different events, such as the Vodafone innovation days 2014. Using the network simulator MATLAB 2016a, realistic mobility patterns of unmanned air vehicles or experimentally derived data transfer model of unmanned aerial network B-AODV with FFNN. WMN has compare presentation evaluation like packet delivery rate, end to end delay or throughput and energy consumption.

In future scope, it will implement the use of hybridization in routing protocol in a wider range of application scenarios. It

shall use the hybrid approach for improving the performance parameters like network load, packet delivery, throughput or delay.

VII. REFERENCES

[1]. Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari (sept 2011) "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey" international journal of computer science, ISSN: 1694-0814, Vol no: 8, Issue:5, page no.:259-268.

[2]. Divya Chadha, Reena (March 2015) , "Vehicular Ad hoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering, Issn: 2320-9801, Vol no: 3, Issue:3, page no.; 2339-2346.

[3]. Abdul Nasser A. Moh **,** Borhanuddin Mohd. (Nov 2015) " Optimum QoS Resource Allocation Algorithm for Video Traffic over Wireless Mesh Networks based on IEEE 802.11s" , IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, isbn: 978-1-5090-0020-3, page no: 102-106.

[4]. Jubil Jose, Rigi C.R, (Feb , 2014) "Wireless mesh networks: issues and challenges", International journal of computer Science and mobile computing, issn: 2320-088X, Vol. 3, issue .2, page no-831-833.

[5]. Ms. Ankita Umale, 2, Ms. Priyanka Fulare , (2014), "Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", International Journal Of Engineering And Science, ISSN: 2319 – 1805, Vol:3, issue :3, page no.- 7-12.

[6]. Abdulla, Ahmed EAA, ZubairMdFadlullah, Hiroki Nishiyama, Nei Kato, Fumie Ono, and RyuMiura. (2015) "Toward fair maximization of energy efficiency in multiple uas-aided networks: a game-theoretic methodology." IEEE Transactions on Wireless Communications 14, Vol :1, page no.- 305-316.

[7]. Yih-Chun, Hu, and Adrian Perrig.(2004) "A survey of secure wireless ad hoc routing." IEEE Security & Privacy 2, Vol: 3, page no.-28-39.

[8]. Yih-Chun, Hu, and Adrian Perrig.(2004) "A survey of secure wireless ad hoc routing." IEEE Security & Privacy 2, no. 3 :28-39.

[9]. Sgora, Aggeliki, Dimitrios D. Vergados, and P. Chatzimisios.(2013) "A survey on security and privacy issues in wireless mesh networks." Security and Communication Networks.

[10]. Sbeiti, Mohamad, NiklasGoddemeier, Daniel Behnke, and Christian Wietfeld. "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks.(2016)" IEEE Transactions on Wireless Communications 15, no. 3 : 1950-1964.

[11]. 11.Douceur, John R. "The sybil attack." In *International Workshop on Peer-to-Peer Systems*, pp. 251-260. Springer, Berlin, Heidelberg, 2002.

[12]. Banerjee, Subhashis, and Koushik Majumder. "WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE."International Journal of Computer Networks & Communications 6.1 (2014): 45.