Design Secure Interconnected Network using ACO Optimisation with Routing Protocol

Jagdeep Kaur[1], Amandeep Kaur[2], Dr. G. N. Verma[3]
[1]Research Scholar, [2]Assistance Professor, [3]Principle
Shri Shukmani Institute of Engineering & Technology
Dera Bassi, Punjab (India)

Abstract **-** For providing broadband internet access for the community, WMNs have become a practical solution because of the explosion of internet. WMN s are the communication networks, which made up of mesh node, mesh router, gateway and mesh client. They are composed as a mesh topology. Mesh router used to transmit data to and from the mesh gateways. A WMN is a self-organized and self-configured network. With the help of nodes, it can automatically establish and maintain network connectivity. The main focus on this research work as to identify the wormhole attacker node in the network with the help of the AODV routing protocol and prevention using Ant Colony Optimization algorithm. In this thesis work, a routing protocol is discussed to communicate the information according to the set of rules and shortest distance measure based in three terms i.e., Request, Reply and Route Error. In routing protocol to detect the attacker node in the WMNs and implement the ACO approach to prevention or mitigate the attackers effect in the wireless mesh network. The existing Position based routing protocols are compared using new approach or the conception of the secure technique that is implemented in ACO with Mesh wireless network based on encryption technique. In realistic UAV-WMN scenarios, Compare location achieves comparable presentation results as the well-established; Routing-Optimization mutual with the IEEE 802.11s security apparatuses. We have used the MATLAB 2016a simulation tool with SCRIPT Language. We calculated the performance parameters, i.e. energy, packet delivery rate, probability distribution vs. time and delay vs. Frame error rate [ms].

Keywords **–** Wireless Mesh Network, Routing Protocol, AODV, ACO algorithm and MATLAB.

I. INTRODUCTION

Multi-hop wireless message system has traditional improved attention due the growing demur for low cost or high presentation ever-present stemming. In the late 1970s,the first production of Mobile Adhoc systems was proposed,or in the early 1990s, MANETs had become a key answer for military applications or emergency operations. MANET is messages less or non-hierarchical multi-hop wireless systems consisting exclusively of mobile knobs.

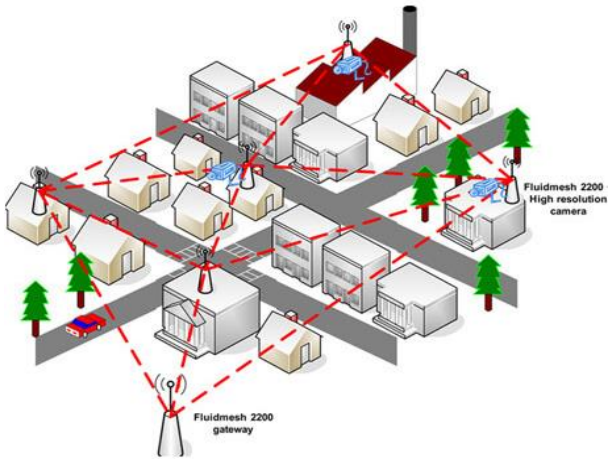

Figure 1: Archtiecture in Wirless Mesh Network

That is, in a MANET ,the mobile knobs set up or preserve a system on demo or without any maintain from an existing transportation. In this way, all the knobs have identical responsibilities counting the routing or forwarding of data. In a wireless mesh system created [1] down the assembly of wireless admittance facts connected at every system consumer's locale. Each system user is also a worker, forwarding [2] data for following knob. The stemming arrangement is rationalized or simplified for every knob essential only transfer as [3] far as the next knob. Wireless mesh stemming could allow people living in distant zones or minor industries working with pastoral districts to join the systems collected for reasonable Internet networks.

Mesh System mesh system is a system topology in which every knob relays data for the system. All mesh knobs co-operate in the portion of data in [4] the system. Mesh systems can communicate post using either a saturating method or a routing technique [5] . With routing, the message is broadcast along a path by hopping from knob to knob until it reaches its endpoint. To ensure all its paths' accessibility, the system must allow for permanent associates or must re-configure itself approximately [6] broken paths, using self-healing procedures such as Straight Path Bridging.Self-healing permits a routing-based system to operate when knobs break-down or when a connection becomes unreliable.

The connectivity based WMNs can be classified as sorts of the different system components, which are either Point to Multi-Point (MPM), Multi-Point (PTM), Point To Point (PTP), or Multi-Point to systems. The complete scientific categorization of this grouping appears in Fig.2. It is believed that PTP forms of the WMN are highly trusted worthy and offer very easier implementation of the wireless network. It basically consists of two communicating nodes (or radio) along with antenna with high gain in order to accomplish highquality links. Such links are used for applications that demand maximized communication performance with higher speed data transmission. Unfortunately, PTP forms lack scalability and also suffers from lower adaptability. PTM form of network applies star topology to support both single and dual direction transmission. It normally uses the omnidirectional antenna for facilitating uplink transmission, and it uses the antenna with high gain for supporting downlink transmission [7].

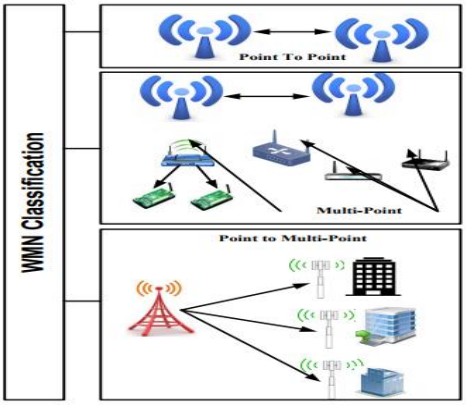

Figure 2: Classification in WMNs

Uses of PTM network are highly suitable for clients requiring high-speed data transmission without much focus on channel capacity. It is also used in backhaul operation. Although PTM networks are scalable to the moderate extent, it lacks reliability as well as adaptability. MTM network is meant for overcoming the flaws of PTM network i.e. to offer the higher degree of adaptability, reliability, and scalability. It is also suitable for large-scale network deployment. In MTM, the communicating devices are inter-connected with various forms of network nodes e.g. switches and routers. The increase in node number also has a positive effect on energy conservation. The utilization of these three forms of the WMN depends on the types of the application and networking demands of the clients [8].

II. RELATED WORK

Kruti.N.Kapadia et al., 2015 [9] presented that the wireless multi-hop network architecture called Wireless Mesh Network (WMN) has recently attracted much attention. They proposed congestion aware multipath routing protocol called EAOMDV-LB for multiracial multiple interface wireless mesh networks (WMN).. The effective load balancing technique maintains data transmission on optimal path by diverting traffic all the way through congested area. WMN recently gained a lot of popularity due to their rapid deployment, instant communication capabilities and support for many types of application. Applications, network congestion is the main reason for lower throughput and longer delay. WMN's are not designed to adapt congestion and optimal link quality.

Awadallah M. Ahmed 2015 et al., [10] presented that the Wireless Mesh Network (WMN) has gained important roles in current communication technologies. It has been used in several applications, which the majorities of them are critical applications such as surveillance and rescue systems. Hence, the WMN attracts a bunch of attention from many researchers. WMN consists of mainly mesh clients (MC) s and mesh routers (MR) s, some of the latter are functionalized by additional functions to serve as internet gateways (IG) s. Therefore, finding the optimal resolution is difficult or it takes polynomial time. Thus, finding near optimal solution is essential to improve the net operation. Novel approach to solve this problem using Genetic Algorithm (GA) to achieve a near optimal solution, considering the number of IGs and the number. Finally, they evaluated the proposed algorithm using many generated instances using different parameters (population size, tournament size, crossover type, mutation type), the experimental results had shown that the high convergence rate using different parameters.

Prithviraj Pati et al., 2016 [11] Managing and upgrading these protocols is a difficult and error-prone task since the configuration must be enforced individually at each router. SDN promises to enables creating a customizable and programmable network data plane. Described that the intelligent network architecture comprising a three-stage routing approach WMNs in uses cases, Smart Grids that provides an efficient and affordable coverage as well as scalable high bandwidth capacity. Experimental results evaluating our approach for various Qi's metrics like latency and bandwidth utilization show that our solution is suitable for the requirements of mission-critical WMNs.

Naveen T.H et al., 2017 [12] Wireless Mesh Network (WMN) is one of the significant forms of the wireless mesh network that assists in creating highly interconnected communication node. Since a decade, there have been various studies towards enhancing the performance of WMN which is successful to a large extent. The technology of pervasive and dynamic networks WMN suffer from several routing issues, Quality-of-Service (QoS) issue, channel allocation, sustainability of routes which makes the theory contradicting when considering for real-world challenges in wireless networks. Briefs about fundamental information of WMN followed by a discussion of existing research trends and existing research techniques Discusses the open research issues after reviewing the existing research techniques.

Ninni Singh et al., 2015 [13] defined that the wireless mesh

network technique because configuration and adaptive characteristics, supports a huge scale network especially in an organization and academics. As with any network, communication among nodes plays an important role, when two nodes in a network communicate with each other via the internet, secure authentication is an imperative challenge. They suggested to deliver a secure authentication between nodes in WMN all these outlines contain some disadvantages. Secure Authentication in Wireless Mesh Network (SAWMN) approach is proposed which overcomes these drawbacks and provides an efficient authentication to the mesh clients. Further, SAWMN results have been shown simulated on AVISPA SPAN to ascertain the authenticity of the proposed approach.

Rakesh Matam et al., [14] discussed the multicast is key correspondence system in remote work arrange (WMN). Applications in WMN including multicast TV, sound and video conferencing, and multiplayer social gaming use multicast transmission. Then again, security in multicast transmissions is essential, without which the system administrations are fundamentally disturbed. Existing secure directing conventions that address diverse dynamic assaults are as yet powerless because of unpretentious nature of imperfections in convention plan. Existing secure directing conventions expect that ill-disposed hubs can't share an out-of-band correspondence channel which discounts the likelihood of wormhole assault. They propose SEMRAW (Secure Multicast Routing Algorithm for Wireless work arrange) that is safe against all known dynamic dangers including wormhole assault. SEMRAW utilizes advanced marks to keep a vindictive hub from increasing ill-conceived access to the message substance. Security of SEMRAW is assessed utilizing the re-enactment worldview approach.

Table 1: Literature Review in Wireless Mesh Network

Author Name	Technique	Parameters
Kruti.N.Kapadia	Airtime congestion aware (ACA) metrics and Load Balancing using Computation Queue Utilization	Throughput End to end delay
Awadallah M. Ahmed	Genetic Algorithm	Calculate the Convergence Rate Fitness value
Prithviraj Patil	AODV or OLSR	Latency Bandwidth Utilization
Naveen T.H	Channel Alloation and Quality od Services	-
Ninni Singh	Secure Authentication in Wireless Mesh Network	Protocol falsification and bounded verification of SAWMN
Rakesh Matam	SEcure Multicast Routing Algorithm for Wireless mesh network	Malicious and Attacker node

III. EXISTING ISSUES IN WMNs

Lots of papers study and found some problems and research gaps in a Mesh Network like network planning and security issues [2]. In Network Planning are be multiple capabilities the situations of routers or entryways and there is no problem amongst routers [3]. Routers are not transferable and have several radio transceivers, which tolerate them to connect instantaneously with supplementary than one neighbor at the similar interval using diverse channels. Transmission power or variety of routers can be particularly from an understated set of probable ranges [6]. The Node request of masses is collected per node; these multitudes are in the broadcast variety of the node. The future perfect can be used un-connectedly to resolution users' exposure: both routers are substituted by a host with a demand [4]. The hacker can operate the information and attract all the payloads and misappropriations the UAV's due to which there are lots of risks of dropping packets [5] by the hacker or stranger. The hacker can loss the route and generate the fake /duplicate route and makes the prospect of each packet to travel on that fake/duplicate route [4]. A hacker can produce the multiple fake Traffic copies of the Unmanned Aerial vehicle to increase the packet above which reductions the accuracy of the network and decreases the system lifetime which affects the route discovery delay in the network [6]. A high need of security in routing protocols for the well-organized routing due to which there will be less unplanned of packet drops and high delivery of packets with less delay from basis for the purpose [15].

IV. METHODOLOGY

Phase I. First, we create the wireless mesh network, which connects one UAV node to another UAV node. To communicate the information in connecting form, this is linked together.

Phase II. Next, we search the source and destination node in this network. We plot the Main Head node name is Key Distributed Centre.

Phase III. In 'Main Head' normal id's and unique id's as created in the wireless mesh networks to travel on position to another position in the mesh networks.

Phase IV. The unique id generate, the purpose is Main Head communicates a secure message and send the trusted node, which is defined by the KDC administration.

Phase V. KDC administrator provides authentication by means of the registration process. Limit decided at the 20 - 50 Unmanned Aerial Vehicles. If any other user who crosses the limit, then message will be displayed by KDC (not authorized Unmanned Aerial Vehicles).

Phase VI. We implement the routing protocol (AODV) to provide the security and manage packet according to the rules in the mesh networks. AODV protocol performs well with mobile knobs it incurs high above with an increase in network size. AODV is an on –Demand routing protocol. The route is calculated on demand, via route discovery process. That is why it is called a reactive protocol. AODV maintains a routing table where it preserves one entry per

endpoint AODV provides loop gratis routes while repair link breakages, but it doesn't require global periodic routing advertisements.

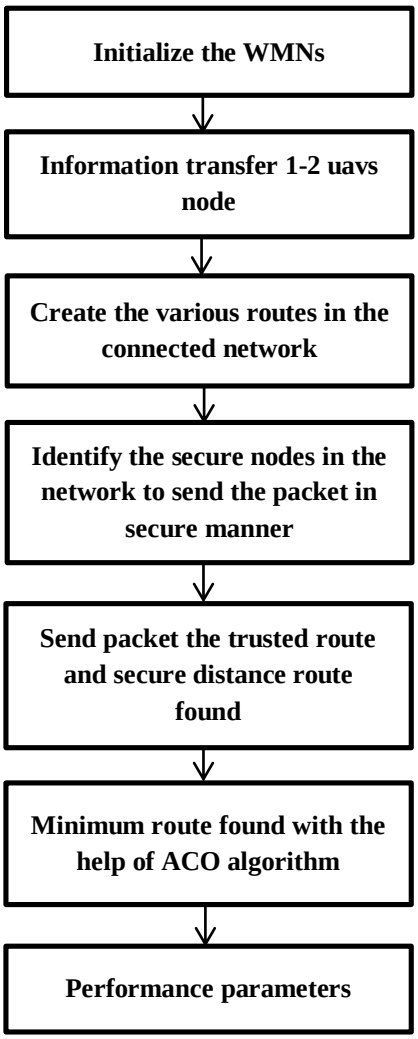

Figure 3: Flow chart in proposed work

Phase VII. We calculate the performance parameters based on the PASER (Power Aware Secure, Efficient Routing Protocol) with Encryption Techniques (Distance Probability, Throughput, packet delivery rate and frame error rate based on delay (0%, 10% and 20%).

Phase VIII. We implement the proposed approach named as an Ant colony optimization algorithm. This is resolving the network issues and transmits the data securely and calculates the performance parameters, i.e throughput, delay and delivery rate etc.

Phase IX. Comparison between the existing and proposed approach and proved that proposed work is better than previous one.

V. RESULT EXPLANATIONS

In this section we explained the result with proposed method and existing methods. The mesh network design system, enter the number of unmanned air vehicles and mesh network length and width 1000*1000. the MESH system with connected UAVs for the broadcast of packets from start node to the sink in which source or destination is plotted in red or green color or all other knobs with their ids. The routing delay to transfer the packets from the basis to the destination having FER which is edge error rate in ACO. These are showing the delay in between the transfer of the packets when the FER with ACO is 0%, FER with ACO is 10 % or FER with ACO is 20%. Little delay results in the high Packet Delivery rates. The packet delivery rate for the successful transmission of packets from source to the destination through trusted vehicles which shows that 96% throughput with ACO are transmitted using secure transmission. Energy for the successful transmission of packets from source to the destination through trusted vehicles which shows that 1.2(joules) energy with ACO are transmitted using secure transmission. With ACO algorithm to optimize the energy based on Ant colony optimization approach in the wireless mesh network.

Table 2: Proposed Performance Parameters

Performance Parameters	Values
Delay 0%	64.63ms
Delay 10%	6.4ms
Delay 20%	12.93ms
Energy	1.2 Joules
Packet Delivery rate	98%

Table 3: Comparison between Packet Delivery Rate (Proposed and Existing Work)

Time [ms]	PDR - AODV	PDR-ACO	PDR-PASER
100	30	50	23
200	46	65	35
300	57	73	50
400	68	84	64
500	73	97.5	70

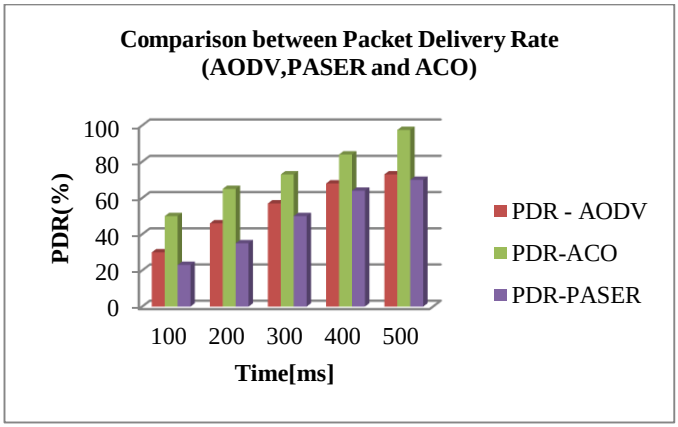

Figure 4: Comparison between packet Delivery (proposed and existing work)

The figure 4. represents that the comparison based on PASER,AODV and ACO in the PDR (%). We improve the packet delivery with ACO and PASER and AODV. We implement the proposed approach to enhance the performance of the information transmission.

Table 4: Comparison between Delay – 0% (Proposed and Existing work)

Time [ms]	Delay-Paser 0%	Delay-AODV 0%	Delay-ACO 0%
100	34	32	26
200	48	46	32
300	70	68	56
400	119	113	106
500	107	103	96

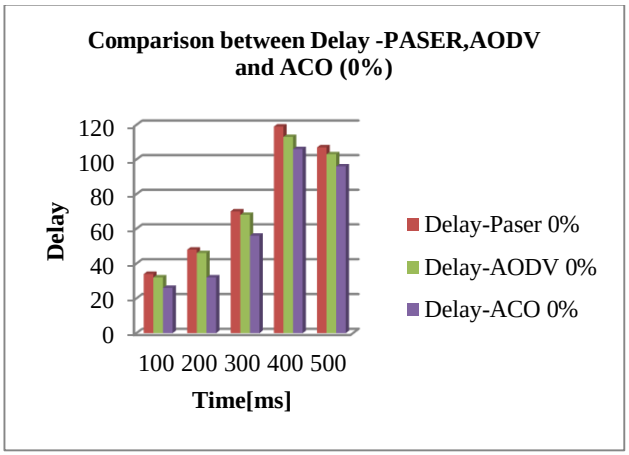

Figure 5: Comparison Between Delay (0%) with PASER,AODV and ACO

The above figure shows that the delay in 0% AODV, PASER and ACO algorithm. We reduce the delay in the wireless mesh network 0% level.

Table 5: Comparison between Delay – 10% (Proposed and Existing work)

Time [ms]	Delay-Paser 10%	Delay-AODV 10%	Delay-ACO 10%
100	3.4	3.0	2.6
200	4.8	4.6	3.0
300	7.0	6.8	5.2
400	11.9	11.0	10.6
500	10.7	9.0	8.9

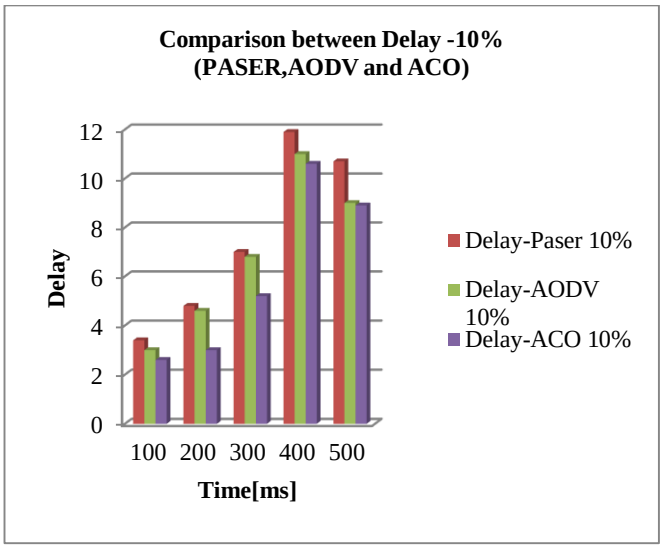

Figure 6: Comparison between Delay (10%) with PASER,AODV and ACO

The above figure shows that the delay in 10% AODV, PASER and ACO algorithm. We reduce the delay in the wireless mesh network 10% level.

Table 6: Comparison between Delay – 20% (Proposed and Existing work)

Time [ms]	Delay-Paser 20%	Delay-AODV 20%	Delay-ACO 20%
100	6.1	5.8	2.6
200	7.2	6.9	3.0
300	8.6	7.8	5.2
400	9.0	8.7	6.6
500	10.3	9.3	8.9

The below figure 7 shown that the delay in 20% AODV, PASER and ACO algorithm. We reduce the delay in the wireless mesh network 20% level.

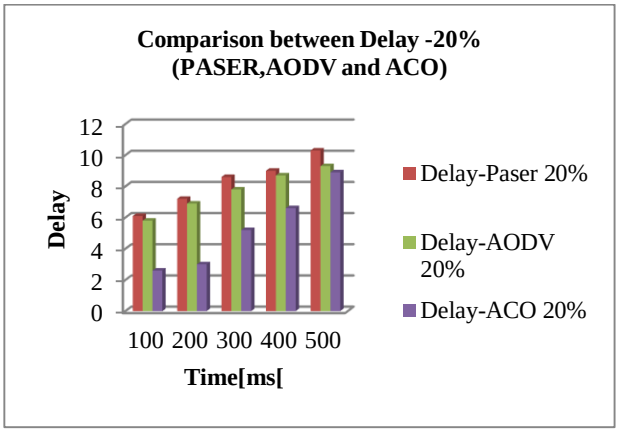

Figure 7. Comparison between Delay (20%) with PASER,AODV and ACO

VI. CONCLUSION AND FUTURE SCOPE

In this conclusion, analyses the AODV-ACO secure approach in UAV-WMN. It is shown that AODV-ACO 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 AODV- ACO 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, none-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms. Last, the benefits of AODV-ACO 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 air AODV-ACO -WMN has compare presentation evaluation like packet delivery rate, end to end delay or throughput.

In future scope, will implement the use of 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. It will implement in military areas, business and industrial areas.

VII. REFERENCES

[1]. De Judicibus, Dario, et al. "Method or system for secured transactions over a wireless networ k." U.S. Patent No. 8,352,360. 8 Jan. 2013.

[2]. Liu, Yunhao, et al. "Does wireless sensor networ k scale? A measurement study on GreenOrbs." *Parallel or Distributed Systems, IEEE Transactions on* 24.10 (2013): 1983-1993.

[3]. Branch, Joel W., et al. "In-networ k outlier detection in wireless sensor networks." *Knowledge or information systems* 34.1 (2013): 23-54.

[4]. Lewis, Ted G. *Critical infrastructure protection in homelor security: defending a networ ked nation*. John Wiley & Sons, 2014.

[5]. El-Hoiydi, Amre. "Implementation options for the distribution system in the 802.11 Wireless LAN Infrastructure Networ k." *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*. Vol. 1. IEEE, 2000.

[6]. Sato, Mitsuhisa, et al. "Ninf: A networ k based information library for globalworld-wide computing infrastructure." *High-Performance Computing or Networ king*. Springer Berlin Heidelberg, 1997.

[7]. JI, De-yu, FengTian, or Chuan-yun WANG. "Design of intelligent warehousing system based on WSN or RFID [J]." *Journal of Shenyang Aerospace University* 2 (2011): 59-62.

[8]. Dimitrievski, Ace, Vera Pejovska, or DancoDavcev. "Security Issues or Methods in WSN." *Department of computer science, Faculty of Electrical Engineering or Information Technology, Skopje, Republic of Macedonia*(2011).

[9]. Kapadia, Kruti N., and Dayanand D. Ambawade. "Congestion aware load balancing for multiradio Wireless Mesh Network." In *Communication, Information & Computing Technology (ICCICT), 2015 International Conference on*, pp. 1-6. IEEE, 2015.

[10]. Ahmed, Awadallah M., and Aisha Hassan A. Hashim. "A Genetic Approach for Gateway Placement in Wireless Mesh Networks." *International Journal of Computer Science and Network Security (IJCSNS)* 15, no. 7 (2015): 11.

[11]. Patil, Prithviraj, Akram Hakiri, Yogesh Barve, and Aniruddha Gokhale. "Enabling Software-Defined Networking for Wireless Mesh Networks in Smart Environments." In *Network Computing and Applications (NCA), 2016 IEEE 15th International Symposium on*, pp. 153-157. IEEE, 2016.

[12]. Naveen, T. H., and G. Vasanth. "Qualitative Study of Existing Research Techniques on Wireless Mesh Network." *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS* 8, no. 3 (2017): 49-57.

[13]. Singh, Ninni, and Hemraj Saini. "Formal Verification of Secure Authentication in Wireless Mesh Network (SAWMN)." In *Proceedings of the Second International Conference on Computer and Communication Technologies*, pp. 375-388. Springer India, 2016.

[14]. Matam, Rakesh, and Somanath Tripathy. "Secure Multicast Routing Algorithm for Wireless Mesh Networks." *Journal of Computer Networks and Communications* 2016 (2016).

[15]. Wu, Xiaoxin, or Ninghui Li. "Achieving privacy in mesh networks."Proceedings of the fourth ACM workshop on Security of ad hoc or sensor networks. ACM, 2006.