Optimization Encryption Based Approach for Wireless Mesh Network

Ramanjeet Kaur[1,] Shweta Ohri[2]
[1]*Student (M.tech),* [2]*Head of Department*
Doaba Institute of Engineering and Technology, Kharar

Abstract - The wireless mesh networks functions, characteristics, network management and finally different protocols with security issues and applications. Wireless Mesh Networks (WMNs) are replacing wireless Infrastructure networks in many areas because of their lower cost and higher flexibility. Wireless mesh network has resolved the limitation of ad hoc networks which is ultimately improves the performance of Ad hoc networks. Security is a very important issue which can be resolve through proper management of network. The improvement of 802.11i security has greatly improved the network performance and increase the encryption and integrity security capabilities. Attacks which can come on different layers are being discussed in this survey. Security of wireless mesh network is still under consideration. Here, we present the encryption technique for Secure, or Efficient mesh Routing approach. In this thesis discusses dissimilar des encryption or genetic algorithm optimization technique to established algorithm which considers packet delivery. The existing PASER routing protocols are compared using new approach or the conception of the secure technique that is implemented in improved genetic algorithm and RSA algorithm Mesh wireless network based on encryption technique. Our proposal prevents from Wormhole attack than the IEEE 802.11s/I security mechanism or the well-known, secure IGA, without making respective assumptions. We calculate performance parameters result achieved like Packet Delivery rate, throughput and less end to end Delay.

Keywords - *Wireless mesh networks infrastructure, characteristics, network management, security issues in WMNs and applications of WMNs.*

I. INTRODUCTION

Mesh networking treats each base station as a node that exchanges information continuously about network conditions with all adjacent nodes across the entire set. This allows nodes that aren't sending and receiving data to each other to still know all about each other. This knowledge might reside in a cloud-based backend or in firmware on each router Mesh networks don't retransmit all the data passing through among a set of base stations. The systems on the market dynamically adjust radio attributes and channels to create the least possible interference and the greatest possible coverage area, which results in a high level of throughput—far higher than anything that's possible with WDS (Wireless Distribution System) and similar broadcast-style systems. A wireless mesh network (WMN) is a communication network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network.[1]

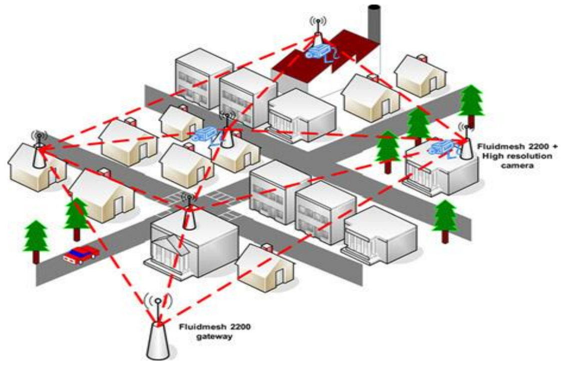

Fig.1: Wireless mesh network

Wireless mesh networks are the third topology after point to point and point to multipoint in order to build a wireless network infrastructure. Each device in a wireless mesh network is typically called a mesh node and is connected with multiple other mesh nodes at the same time. Wireless mesh networks are also multi hop networks because each mesh node can reach another node going through multiple hops and leveraging other nodes as repeaters. The major advantage of a wireless mesh networks is the intrinsic redundancy and, consequently, reliability because a mesh network is able to reroute traffic through multiple paths to cope with link failures, interference, power failures or network device failures and explained in below: [2]

- Traditional networks rely on a small number of wired access points or wireless hotspots to connect users. In a wireless mesh network, the network connection is spread out among dozens or even hundreds of wireless mesh nodes that "talk" to each other to share the network connection across a large area.[3]
- It is also called mesh topology or a mesh network, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a true mesh topology every node has a connection to every other node in the network. There are two types of mesh topologies: full mesh and partial mesh.
- Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the

rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes.

- Mesh system can relay post using either a flooding technique or a routing technique.
- With routing, the message is forwarding along a path by hopping from knob to knob until reaches its destination.
- Self-healing permits routing based system to operate when knobs break downer when a connection becomes unreliable.
- In mesh system, all nodes are coupled to each other is a fully connected system.[4]

Applications of WMNs

- **Developing Countries:** Wireless mesh networks are useful in countries without a widespread wired infrastructure, such as telephone service or even electricity.
- **Isolated Locations, Rugged Terrain:** Even in developed countries, there are rugged locations too far off the grid for traditional high-speed Internet service providers..
- **Education:** Many colleges, universities and high schools are converting their entire campuses to wireless mesh networks. This solution eliminates the need to bury cables in old buildings and across campuses.
- **Healthcare:** Wireless mesh nodes can sneak around corners and send signals short distances through thick glass to ensure access in every operating room, lab and office. The ability to connect to the network is crucial as more doctors and caregivers maintain and update patient information -- test results, medical history, even insurance information -- on portable electronic devices carried from room to room.
- **Hospitality:** High-speed Internet connectivity at hotels and resorts has become the rule, not the exception. Wireless mesh networks are quick and easy to set up indoors and outdoors without having to remodel existing structures or disrupt business.
- **Warehouses:** There is simply no effective way to keep track of stock and shipping logistics without the types of Ethernet-enabled handheld scanners used in modern warehouses.
- **Future Applications:** The U.S. military, which helped develop wireless mesh technology, foresees a day when thousands of microchip-size mesh nodes can be dropped onto a battlefield to set up instant scouting and surveillance networks.
- Information can be routed to both ground troops and headquarter personnel.[5]

II. LITERATURE SURVEY

WMN can be defined as a dynamic, self-organized, self-configured, decentralized wireless multi-hop-network, consisting of MRs and MCs (Zeng & Lou, 2008; Kone & Das, 2008; Shubat & Eissed, 2013). The purpose of this review is to investigate WMN security issues and challenges based on: confidentiality, integrity,[6] reliability and authentication. Shubat et al, (2013) explain that two types of nodes MR and CR have specific functions essential to the operation of the WMN. This in turn requires wide usage of Internet Protocol (IP) addresses, hence the significance or routing protocols (Shubat et al, 2013).[7] explain that two types of nodes MR and CR have specific functions essential to the operation of the WMN. This in turn requires wide usage of Internet Protocol (IP) addresses, hence the significance or routing protocols (Shubat et al, 2013). WMN relies heavily on boundary-less and unprotected RF to traverse data to network members. WMN is being characterized by its cheap easy and fast deploy capabilities for last-mile solution for ubiquitous internet access (Zhu, Fang, & Wang, 2010; Yi, Wu, Zou & Liu, 2010).[8,9] Traditional wired and wireless systems such as IEEE 802.11 Wireless Fidelity (WiFi) which is the same as Wireless Local Area Network (WLAN), IEEE 802.15 Wireless Personal Area Network (WPAN), IEEE 802.16 World Wide Interoperability for Microwave Access (WiMAX) , and IEEE. 802.3 Ethernet / Local Area Network (LAN) (Lewis, 2008), although differ from WMNs, they are still part of its architecture e.g. they are required to formulate the backbone connections between internetworks and multi clients, hence the multi-cast multi-hop mesh. The remainder of this review is organized as follow: session one defines and describes the WMNs[10,11] while session two provides a summary of the IEEE 802.11 standards and RF applications. [12]

III. ISSUES AND RESOLVING TECHNIQUES

- Lots of papers have studied and found some problems and research gaps in Mesh Network like network planning and security issues. In
- Network Planning are multiple capabilities situations of routers or gateways and there is no problem between routers.[13]
- Routers are not moveable and have multiple radio transceivers, which allow them to communicate with more than one neighbor at the same time using different channels. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes.
- Wireless mesh networks can self-form and self-heal. Transmission power or range of routers can be selected from understated set of possible ranges. The Node request of hosts is collected per node; these hosts are in the transmission range of the node. The future model can be used separately to resolution users' exposure: each router is substituted by a host with a demand. [14]
- The Hacker can operate the information and attract all the payloads and misappropriations the UAVs due to which there are lots of risks of dropping packets by the hacker, makes the prospect of each packet to travel on that fake/duplicate route. Hacker can produce the multiple fake Traffic copies of the Unnamed Air Vehicle

to increase the packet above which reductions the throughput of the network and decreases the network lifetime which increases the delay in the network.

Encryption RSA techniques: [15]
RSA implemented two important ideas:
(i) Public-key encryption. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.[16]
(ii) Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be varied by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. The security of the RSA algorithm has so far been validated, since no known attempts to break it have yet been successful, mostly due to the difficulty of factoring large numbers n = pq, where p and q are large prime numbers.[17,18]

IV. SIMULATION RESULTS

First we will deal with the planning of the network which deals with the calculation of network range and spreading of nodes in the network. Then there is a registration process with the key distribution center for UAVs. Then we will deal with the transmission of the packets using RSA algorithm in the encrypted form and see the authentication of the routes. Then we will perform the attack in the network through which we can see the performance of the network in the presence of the attack. If the packets drop increases then we will find that the optimization of the network is required and then we will developed the network and then we will evaluate the performance of the network in terms of throughput, end delay, packet delivery rate, energy consumption of the network.

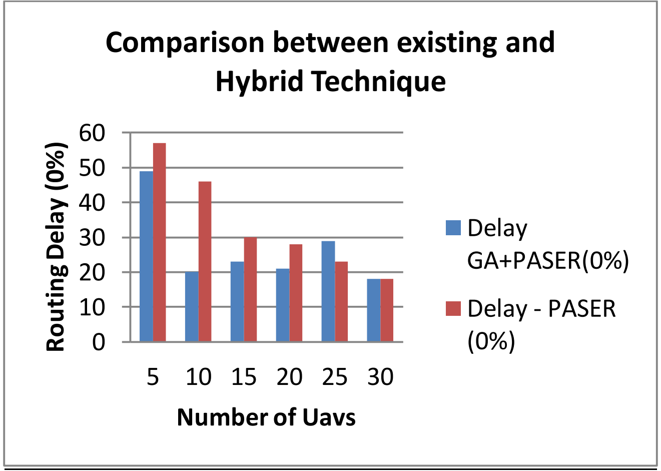

Fig.2: Comparison between existing and Proposed work (Hybrid) with 0%

The above figure shows the routing delay to transfer the packets from source to the destination having FER which is frame error rate in comparison with PASER or EGA. These are showing the delay in between the transfer of the packets when the FER with PASER or EGA is 0%, FER and Less the Delay as compare with PASER.

The below 3. figure shows the routing delay to handover the packets from foundation to the destination having FER which is frame error rate in comparison with PASER or EGA.

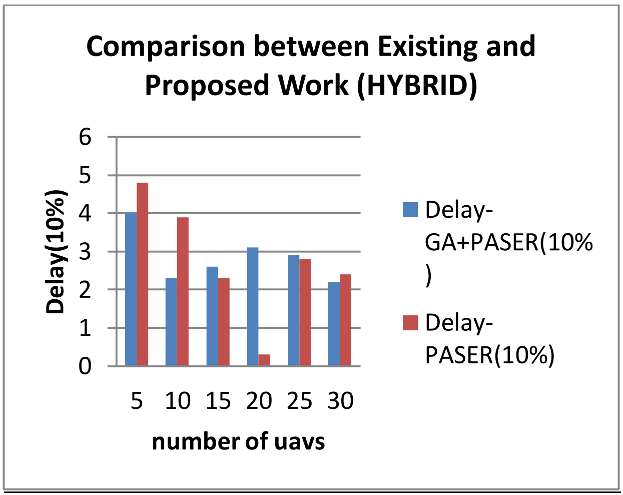

Fig.3. Comparison between existing and Proposed work (Hybrid) with 10%

These are showing the delay in between the transfer of the packets when the FER with PASER or EGA is10%,FER and Less the Delay as compare with Hybrid.

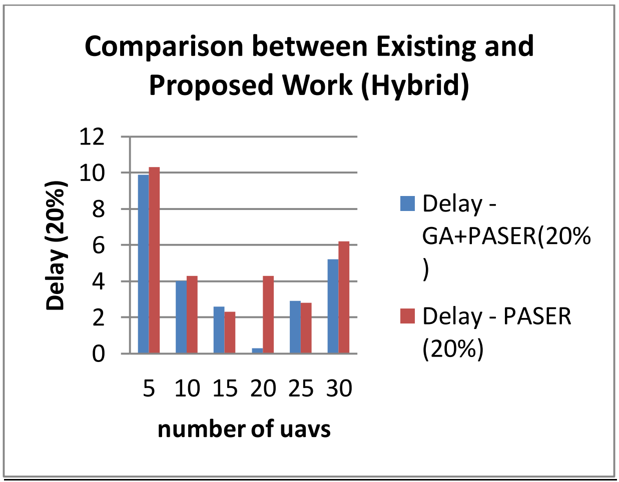

Fig.4. Comparison between existing and Proposed work (Hybrid) with 30%

The above figure shows the routing delay to transfer the packets having FER which is frame error rate in comparison with PASER or EGA. These are showing the delay in between the transfer of the packets when the FER with PASER or EGA is 20%, FER. Less the Delay as compare with PASER or EGA.

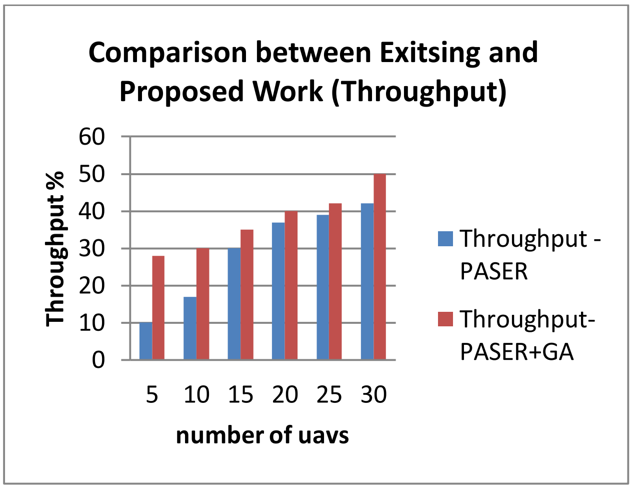

Fig.5. Comparison between existing and Proposed work (Hybrid) with Throughput

The above figure shows throughput for the successful transmission of packets which shows that 40% throughput (PASER) or 50% throughput (EGA) are transmitted using secure transmission.

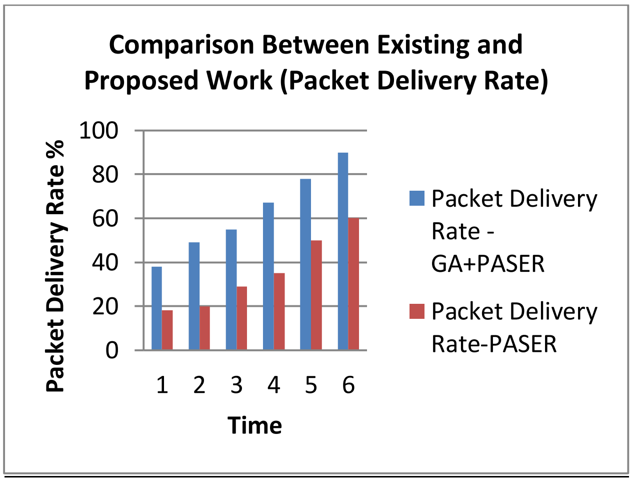

Fig.6. Comparison between existing and Proposed work (Hybrid) with PDR

The above figure shows packet delivery rate for the successful transmission of packets from source to the destination through trusted vehicles which shows that 90% throughput with EGA or PASER with 70% are transmitted using secure transmission.

V. CONCLUSION AND FUTURE SCOPE

In this conclusion, through a series of experiments and measurements this research work analyses the RSA or IGA Optimization secure rules approach in unnamed air-vehicle-Mesh wireless network. RSA-IGA mitigates in the study scenarios, more hijackers than the well-known, secure information transfer or the standardized security device. The efficiency of RSA-IGA is explored in a simulation based analysis of its path discovery procedure, or its scalability w.r.t network size or traffic load is reasoned. Using the network simulator MATLAB, realistic mobility patterns of unnamed air vehicles or experimentally derived data transfer model of unnamed air RSA-WMN has compare performance parameters like packet delivery rate, end to end delay. In future scope, will implement the use of DES-AODV protocol in a wider range of application scenarios. We shall use the hybrid approach for improve the performance parameters like network load, packet delivery, throughput or delay. This may change in the future, however, as new wireless technologies supporting quality of service (QoS) are also being developed.

VI. REFERENCES

[1]. Siddiqui, M.S. Amin, S.O. Choong Seon Hong. “An Efficient Mechanism for Network Management in Wireless Mesh Network.” ICACT 10th International Conference, Feb. 2008.

[2]. Ian F. Akyildiz, Xudong Wang, Weilin Wang, “Wireless mesh networks: A Survey” 1st January 2005.

[3]. Anastasios, D. Khalil, K. “IEEE 802.11sWireless Mesh Networks” Dept. of Communication Systems, Lund University, Sweden.

[4]. Omar Villavicencio-Calderon. “wireless mesh networks: performance analysis and enhancements.” university of puerto rico mayag uez campus, 2008.

[5]. Hamid, Zara; Khan, Shoab A., "An Augmented Security Protocol for WirelessMAN Mesh Networks," Communications and Information Technologies, 2006. ISCIT '06. International Symposium on , vol., no., pp.861-865, Oct. 18 2006-Sept. 20 2006

[6]. Netgear everybody connecting ‘’The ABGs of Wireless LAN’’ Technology Overview. February 2003.

[7]. Puttipong Mahasukhon, Michael Hempel, Song Ci, Hamid Sharif ‘’Comparison of Throughput Performance for the IEEE 802.11a and 802.11g Networks’’.

[8]. www.cs.berkeley.edu/~daw/crypto.html. Access date:- 1st May, 2009.

[9]. Bruce Schneier, John Wiley & Sons; “Applied Cryptography: Protocols, Algorithms, and Source Code in C,” ISBN: 0-471-12845-7.

[10]. A.Gerkis ‘’A Survey of Wireless Mesh Networking Security Technology and Threats’’. September 2006.

[11]. Ian F. Akyildiz, Xudong Wang, ‘’Security in Wireless Mesh Networks’’.December 19, 2006

[12]. Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen ‘’IEEE 802.11 wireless LAN Security Overview’’. May 2006.

[13]. E. Jovanov, "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation", *J. NeuroEng. Rehab.*, vol. 2, no. 6, Mar. 2005.

[14]. D. Halperin, "Security and Privacy for Implantable Medical Devices", *IEEE Pervasive Comp.*, vol. 7, no. 1, pp. 30-39, Jan. 2008.

[15]. K. Lorincz, "Sensor Networks for Emergency Response: Challenges and Opportunities", *IEEE Pervasive Comp.*, vol. 3, no. 4, pp. 16-23, Oct.-Dec. 2004.

[16]. Srikrishna, devabhaktuni, or Amalavoyal Chari. “Selection of routing paths based upon path quality of a wireless mesh network. “U.S. Patent No. 6,965,575. 15 Nov. 2005.

[17]. Sbieti, Mohamad, et al. “PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks. “IEEE Transaction, 2015.

[18]. Y. Zhang and Y. Fang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh NETWORKS, “IEEE Journal on Selected Area in communications, vol.24, No. 10, 2006.