ISSN:0975-9646

Security Enhancement Technique for Defending Wormhole Attacks in Wireless Mesh Networks

Virendra Dani [1] Vijay Birchha [2]
PG Scholar [1], Professors, Head [2], Department of Computer Science & Engineering,
Swami Vivekanand College of Engineering
(SVCE), Indore, India

***Abstract*-Wireless mesh network is one the most potential application network for outdoor communication. In this presented work the security issues are investigated in WMN and a solution for security issue is designed more specifically for wormhole attack detection and prevention. The issues rise when the nodes are mobile and poor routing techniques allow a user to change or modify the information during data transmission because, during network communication the data is transmitted through the intermediate routers where any node can leave or join the network any time. Thus a malevolent node also can join the network and harm the privacy and security. This given scheme is desired to prepare for the secure communication route discovery which is able to provide the solution for defending routing based attacks in the network one of the attack is wormhole. Thus a novel key is desired to set up for the secure communication route sighting which is able to provide the solution for wormhole link attack in WMNs. The implementation of the proposed secure routing technique is in NS2 simulator.**

***Keywords*- Wireless Mesh Network, Simulator, AODV, Route Discovery, Routing, Attacks.**

I. INTRODUCTION

Wireless Mesh Network:

WMNs (Wireless mesh networks) have appeared as a promising knowledge to offer low cost, high bandwidth, wireless entrance services in a range of application scenarios [1]. A wireless mesh network (WMN) is a recent enhancement in the technologies which relieves us from the expensive deployment costs. It is a self-configuration; multi hoped packet switched network, infrastructure less network of mobile devices. These networks offer closer interface with humans as compared to the other types of Ad hoc Networks.

A wireless web can deliver the similar ne tcapability, consistency and safety that were once retained for wired networks – but with the elasticity of wireless. With today's state-of-the-art solution, municipalities, community security agency, port establishment, and industrial association can rely on mesh networks to afford vital connectivity to their workers and constituents.

Two kinds of wireless mesh network can be recognized-

Infrastructure WMNS: Mesh routers form a network offering connectivity to the clients. The network is mean to be self-configuring and self-healing [2].

Clients WMN: In this none of the dedicated routers or infrastructure exists, so that the clients have to be self-configuring and act as a router for the traffic [2].

Fig. 1 Infrastructure/backbone WMNs [2]

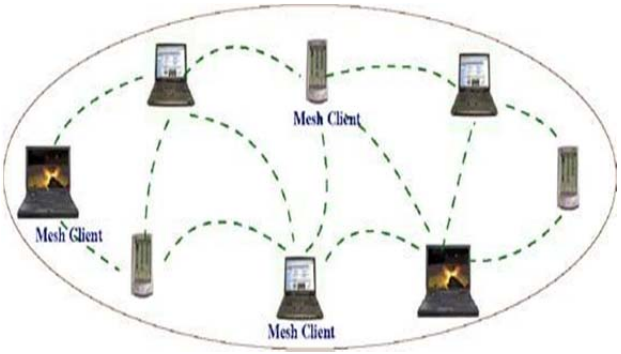

Fig. 2 Client WMNs [2]

APPLICATIONS

In Research and enhancement of WMNs is a immense area of applications which obviously exhibit the expert advertise while at the same time these applications cannot be support directly by supplementary wireless networks such as mobile networks, ad hoc networks, wireless sensor networks, typical IEEE 802.11, etc[3].

Community and Neighborhood Networking: In a neighborhood, the common architecture for net-work admittance is based on cable or DSL linked to the Internet, and the last-hop is wireless by connecting a wireless router to a cable or DSL modem.

Transportation Systems: Instead of limiting IEEE 802.11 or 802.16 accesses to stations and stops, mesh networking technology can extend access into buses, ferries, and trains. Thus, convenient passenger information services, remote monitoring of in-vehicle security video and driver communications can be supported.

Compatibility and Inter-operability: It is a desired feature for WMNs to support network access for both conventional and mesh clients. Thus, WMNs need to be backward compatible with conventional client nodes; or else, the stimulus of deploying WMNs will be significantly compromised.

Enterprise Networking: This can be a small net-work within office or a medium-size network for all offices in an entire building, or a large scale network among offices in multiple buildings.

Capacity of WMNs: The capacity of WMNs is affected by many factors such as network architecture, network topology, traffic pattern, network node density, number of channels used for each node, transmission power level, and node mobility.

Metropolitan Area Networks: WMNs in metro-Politian area have several advantages. The physical-layer transmission rate of a node in WMNs is much greater than that in any cellular net-works

Defense Supervision Systems: As security is turning out to be a very high concern, security surveillance systems become an essential for enterprise buildings, shopping malls, grocery stores, etc.

Broadband Home Networking: At present broad-band home networking is realized throughout IEEE 802.11 WLANs.

II. LITURATURE SURVEY

Numerous Researchers have worked on multiple detection and prevention of wormhole attacks in wireless mesh network, based on the detection mechanism, the existing techniques of detecting and preventing wormhole attacks can be illustrate in this section.

Clock Synchronization

Hu et al. proposed the concept of packet leashes to detect wormholes in wireless networks. It uses two types of packet leashes one is geographical leashes and another one is temporal leashes, but this method requires GPS and tightly synchronized clocks. In geographical leashes, each node knows its precise location and all nodes have loosely synchronized clocks to determine the neighbor relation. Before sending a packet, node appends its current position and transmission time to it. On getting packet, receiving node computes the distance with respect to the sender and the time required by the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole link or not. In Temporal leashes, every node maintains a tightly synchronized clock but does not depend on GPS information [4].

Statistical Analysis Method

Song et al. realize a method on wormhole attack detection called Statistical Analysis of Multi-path Routing (SAMR). In this scenario a link created by a wormhole is extremely attractive in terms of routing and will be selected and requested with unusually high occurrence as it only uses routing data previously available to a node. These aspects have the ability to easily integrate to this method into Intrusion Detection System (IDS) only to routing protocols that are both on-demand and multi-path [5]

Hardware Based Method

Hu and Evans proposed a cooperative protocol in which directional information is shared among nodes to prevent wormhole attack. This method does not require clock synchronization and location information but it requires supplementary hardware i.e. directional antenna [6].

Hop Based Method

The Hop Count (delay per hop indication i.e. (DELPHI) method can identify hidden and exposed wormhole attack. Together hop count and delay per hop indication are monitored for wormhole detection. The essential hypothesis is that, the reshuffle of packet under typical condition for propagating one hop is very high in wormhole attack as the legitimate path between the nodes is longer than advertised path [7].

Graphical Theory Method

In case of Localization based approach, a "graph-theoretical" approach to wormhole attack prevention in Wireless Network. According to it, limited-aware guard nodes (LAGNs) which are in the known location and origination which can be acquired through GPS receivers are used. LAGNs used "local broadcast key" that are valid between instant one hop neighbors [8].

Trust Based Method

Method used a trust based model for the recognition of wormhole in sensor network. In trust based systems, each source node uses its trust information to estimate the most consistent path to an exacting destination by get around intermediary malevolent nodes. A wormhole system have the slightest trust level if that wormhole drops all the packets and if all the packets sent attain the destination then the neighboring node of a source node will have the uppermost trust level[9].

Software Based Method

In this, a software based method for preventing wormhole attack in wireless mesh network, planned method relies on digital signature and avert structure of wormholes throughout route detection procedure and it is intended for an on command hop-by-hop routing procedure. Here not requires additional or specialized hardware [10].

III. ROLE OF ROUTINGIN WMNS

Routing is a most key quality of the wireless mesh networking because it enables messages to pass from one node to another and finally reach the ultimate goal. Every intermediary node performs routing by passing along the message to the subsequently node. Part of this process involves analyzing a routing table to determine the best and correct path. Routing protocols for self-organized networks are expected to provide some functions like detecting and responding to changes in network topology and services, providing management, constructing and selecting routes, maximizing the capacity of the network and minimizing the packet delivery delays [11].

Routing is a term that throughout which the packet can transfer from source to ultimate destination. Due to self-configured and self-knowledge features of WMNs, it is probable that in WMN the nodes can choose a best path routinely. Efficient communication in WMN depends on these routing decisions. For efficient routing different

routing protocols are used for network route. The packet switched network nature of WMN make role of routing protocol more important. For ad-hoc network recently many routing protocols are used [2].

IV. SUPPORTING ROUTING PROTOCOL IN WMNS

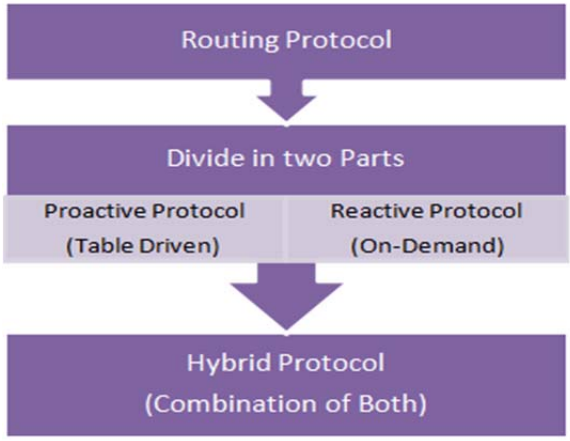

Fig. 3 Classification of Routing Protocol

A. Proactive Protocol-

1. In proactive routing protocols, each knot continues a record of destination and update its route to them by analyze episodic topology transmit from other knots. When a package arrive, the knot checks its direction-finding table and onwards the package accordingly [12].
2. Proactive protocols are not appropriate for huge networks as they need to maintain node entries for each and every node in the routing table. Routing table periodically update while topology of network being changed.
3. These protocols maintain diverse number of routing tables changeable from protocol to protocol.[12]

Example: Optimize Link State Routing Protocol (OLSR), Destination Sequenced Distance Vector (DSDV).

B. Reactive Protocol-

1. Find out routs when required.
2. No routing construction formed Priori.
3. Reactive protocols seek to set up routes on-demand.
4. Reactive Protocol has lesser overhead since routes are resolute on demand [13].

Example: Ad hoc On-Demand Vector (AODV),
Dynamic Source Routing (DSR).

C. Hybrid Protocol-

1. Hybrid Wireless Mesh Protocol (HWMP) defined in IEEE802.11 is a vital routing protocol for a Wireless Mesh Network.
2. HRP is a hybrid protocol that separates the network into a number of zones, which makes a hierarchical protocol.
3. It is based on AODV and tree-based routing.
4. In HWMP protocol the name is Hybrid, as it wires two kinds of path choice protocols.

Example: Zone Routing Protocol (ZRP).

Dynamic Source Routing (DSR)

DSR is on demand or reactive routing protocol. It uses the source routing, accumulating the address of all the nodes between source and destination during route discovery. It consists of two phases, route discovery and route maintenance. When a node has to send a data packet to another node, it initiates a route discovery. Node floods route request(RREQ) which contains sender's address, destination's address and request ID, node receiving RREQ checks it is the destination or not or it checks route is available with him for destination node. If it is intended destination or it contains the route to destination it copies the route from RREQ into RREP send RREP (route reply) message to the sender node (upon receiving accumulate the route in cache for future routing) otherwise it checks it has seen the message before and if it is it discards message otherwise appends its own id and rebroadcast RREQ. In route maintenance phase if node discover link failure then it sends route error (RRER) message to the source node, nodes receiving the RRER message updates their cache [14].

Ad-Hoc On-demand Distance Vector Routing (AODV)

The decentralized AODV routing protocol is a reactive protocol designed for ad hoc networking with mobility support. AODV establishes route discovery in a similar way relating to the handshake communications mechanism. The AODV route discovery approach begins when a node requiring a valid link/path for packet traversal broadcasts route request (RREQ) information to the neighbors in search of a destination. Each of these neighbors also re-broadcast the RREQ to their neighbors and so on in a recursive manner until it floods the entire network topology with the RREQ [15].

Optimized Link State Protocol (OLSR)

Optimized Link State Protocol (OLSR) is a proactive routing protocol, so the routes are always immediately accessible when needed. OLSR is an optimization adaptation of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To shrink the possible overhead in the network protocol uses Multipoint Relays (MPR)[16]. Unlike the AODV, it floods the entire network with topology messages for the information about the available route without the need to take cognizance of the network load and node mobility [15].

Destination- Sequenced Distance-Vector Routing (DSDV)

A variation of Bellman- Ford algorithm implemented in RIP (Routing Information Protocol) modified for self-configuring networks. Each node maintains its personal routing table with the information about network topology and the cost of the links between the nodes. The DSDV protocol requires all mobile nodes to publicize its own routing table to all of its current neighbors. Since the nodes are mobile, the entries can vary energetically over time and maintain table consistency. The route advertisements should be made whenever there is any change in the

neighborhood or periodically. Every mobile node agrees to forward route advertising messages from other mobile nodes. DSDV is also called a table driven routing protocol that is an improved version of the distributed Bellman-Ford algorithm. In all table driven protocols every node maintains a table that contains the next hop to arrive at all destinations. To maintain the tables up to date they are exchanged between neighboring nodes at regular intervals or when a major topology changes are observed. [17][18].

Zone Routing Protocol (ZRP)

The Zone Routing Protocol was the first Hybrid routing protocol. It was proposed to reduce the control overhead of Proactive routing protocol and to decrease the latency of Reactive routing protocol [19]. The ZRP (Zone Routing Protocol) join the benefits of the practical and imprudent move toward by preserve an up-to-date topological chart of a zone centered on every knot. The Zone Routing Protocol, as its name implies, is based on the concept of zones. A node that has a packet to checks whether the destination is inside its local zone using information provided by IARP. In that case, the packet can be routed proactively. Reactive routing is used if the destination is outside the zone. The reactive routing process is divided into two phases: the route request phase and the route reply phase [22].

V. SECURITY ISSUES IN WIRELESS MESH NETWORKS

High level security issues for WMNs are fundamentally equal to security necessities for any other communication structure, and contain following attributes:

Availability

Availability ensures the survivability of network services despite attacks. Availability does not come to mind as a security concern as quickly as do confidentiality and integrity. But the assurance of availability is very much a security issue.

Authenticity

Authenticity enables a node to ensure the identity of the peer node it is communicating with. Without authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes.

Integrity

The concept of integrity ensures that the contents of data or correspondences are preserved intact through the transfer from sender to receiver. Integrity embodies the guarantee that a message sent is the message received, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways: by the intentional alteration of the data for vandalism or revenge or by the unintentional alteration of the data caused by operator input, computer system, or faulty application errors.

Confidentiality

The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. Whether the data contains trade secrets for commercial business, secret classified government information, or financial records, confidentiality implies that data is protected from breaches from unauthorized persons and the damage that would be done to the organization, person, and governmental body by such breaches [20].

Accountability

Accountability aims are to detect the malicious users, sometimes it is necessary to deny network access to them via revoking, so that malicious users can be ejected.

Heterogeneity

This approach takes the advantage of heterogeneous resources of each node, exploiting the nodes capacity to execute network functionalities [21].

VI. WORMHOLE ATTACK

In a wormhole attack two or more nodes are connected to each another by means of medium which is not available to normal nodes, with the help of out of band channel the nodes are capable to communicate with one another above a range in which normal nodes cannot [23]. Simply, Wormhole Attack is a sever kind of attack in Wireless Mesh Network where two or more attackers are coupled by low latency, high speed, off-channel link, called wormhole tunnel, also called tunneling attack. Once tunnel is recognized, the attacker collects data packets using the low latency link and replays at the other end**.**

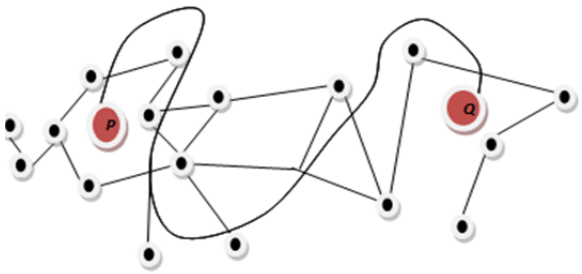

Fig. 4 Wormhole Attack

---- Malevolent Nodes

---- Genuine Nodes

---- Malevolent link

A. Effects of Wormhole Attack:

Results of wormhole success can be very overwhelming. Here some of the special effects are listed below.

1. Get illegal access,
2. Interrupt routing,
3. Initiate denial-of-service attacks (DoS),
4. Split message keys,
5. Degrades services at physical layer,

B. Outcomes of Wormhole Attack:

Formerly a successful wormhole attack is launched there are definite symptoms that can be observed in the network, some of the outcomes are:

1. Abrupt decreases in hops,
2. Longer circulation delays,
3. Decrease in network expenditure,
4. Greeting of multiple copies of same message.

VII. PROPOSED SYSTEM

Methodology-

The proposed routing technique is an enhancement of the traditional routing protocol namely AODV. In order to perform the detection and prevention of the wormhole attack the following process is taken place.

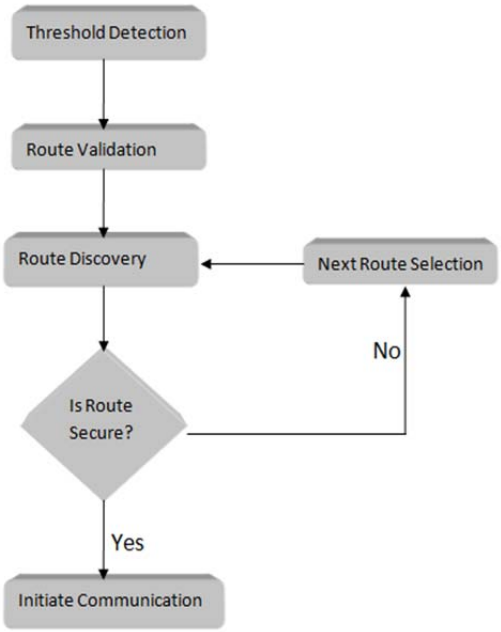

Fig. 5 Checks for Secure route Communications

The proposed routing process is taken place in the given manner in figure. Each and every steps of the proposed routing protocol can be described as:

1. Threshold Estimate: In this phase an AODV based network is configured and using the different sessions a history is managed for each host.

Node id	Number of broadcast

$$B_t = \frac{1}{n}\sum_{i=0}^{n} Broadcast_i$$

In addition of that the RTT (Round Trip Time) between two nodes are estimated using the following formula.

$$RTT = \frac{T_2 - T_1}{2H}$$

Where the T_1 is time of which the source node sends the RREQ and T_2 is the time when source get the reply. Additionally the H is number of hop between source and destination.

2. Route Discovery: In this phase the routing protocol is initiate a communication session for that purpose first the source router send a RREQ message and waits for reply. As the source router get the route reply RREP packets. The entire routes are listed in source router. According to the surveys the malicious attacker finds on the first routes always thus first routes are discarded in most of the prevention technique. But in this process the first route is also validated.

3. Route Validation: In order to validate the first route in the source router's routing table a dummy packet with highest and random sequence number is transmitted to the next hop and waits for the acknowledgement from the target machine.

The proposed system is implemented with the help of AODV routing protocol modification and using the NS2 network simulator and their performance is measured in terms of the following performance parameters:

Throughput

Network throughput is the standard rate of successful release of a message over a communication medium. This data may be broadcast over a physical or logical link, or pass by a definite network node. The throughput is calculated in terms of bit/s or bps and occasionally in terms of data packets per time slot or data packets per second.

Packet Delivery Ratio(PDR)

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$Packet\ Delivery\ Ratio = \frac{Total\ Arrived\ Packets}{Total\ Sent\ Packets}$$

End to End delay (EED)

The standard time taken by a data package to appear in the target. It also contains the wait caused by route detection procedure. Only the data packages that efficiently deliver to the target that counted by

$$\sum \frac{ArriveTime - Sendtiime}{NumberofConnections}$$

So the validation procedure is taken place in the following manner.

Now if a malicious node found in the first route the process stop evaluation of next routers and select next route to perform the communication.

If (node.boradcast>=B_t&&$RTT \leq currentRTT$)
{
Node labeled as malicious node;
}
Else If(node.broadcast<=B_t&&$RTT \leq currentRTT$)
{
Node labeled as malicious node;
}
Else If (node.boradcast<=B_t&&$RTT \geq currentRTT$)
{
Node is legitimate secure and adds to route;
}

VIII. CONCLUSION

Wireless Mesh Networks are susceptible to wide range of security attacks because of their open area deployment undefended environment. In Wormhole attacks, as colluding nodes regularly replays the authentic data packets, and detection of these packets much difficult. This survey paper initiate key defense threats in WMN and also explore different wormhole detection and prevention techniques, and how these solutions are capable to safe the network, consequently, each method and techniques has its own potency and weaknesses and there is no complete wormhole detection technique that can detect all wormhole threats. So the finally, by evaluate the pros and cons of obtainable techniques the open research challenges in wireless mesh network are studied.

ACKNOWLEDGMENT

I would like to sincerely thank Mr. Vijay Birchha, HOD, dept of Computer Science, SVCE, for his valuable suggestions and guidance. I would also like to thank to our related faculty members for their comments and inspirations.

REFERENCES

[1] Rakesh Matam and Somanath Tripathy "WRSR: wormhole-resistant secure routing for wireless mesh networks", *EURASIP Journal on Wireless Communications and Networking*, 2013.

[2] Binish Raza, Faiza Qaiser, and Muhammad Ahsan Raza, "Study of Routing Protocols in Wireless Mesh Networks", *International Journal of Academic Scientific Research (IJASR),* Volume 2,pp. 19-26 (May-June 2014).

[3] Ian F. Akyildiz, Xudong Wang, and Weilin Wang, Wireless mesh networks: a survey", *Computer Networks and ISDN Systems*, pp.445–487, 2005.

[4] Hu, Y. Perrig, A., and Johnson D., Packet Leashes: "A DefenseAgainst Wormhole Attacks in Wireless Network",*In Proceedingsof the 22nd IEEE International Conference Computer and Communications*, Volume 3, pp.1976–1986, April 2003.

[5] N. Song, L. Quin, and X. Li., "Wormhole Attack Detection in Wireless Ad hoc Networks: A Statistical Analysis Approach". *In Proceedings of the 19thIEEE International Parallel and Distributed Processing Symposium*, pp. 8-15, 2005.

[6] L. Hu and D. Evans, Using directional antennas to avert wormhole attack" in *NDSS (Network and Distributed System Security Symposium),*San Diego, 2004.

[7] H.S. Chiu and K.S. Lui."DELPHI: wormhole discovery device for ad hoc wireless network", *1st International Symposium on Wireless Pervasive Computing*, pp. 6–11, January 2006.

[8] L.Lazos and R.Poovendran, "Serloc: Secure rang-independent localization for wireless sensor network". *In Proceeding of the ACM Workshop on wireless security*, pp. 21-30, October2004.

[9] S. Ozdemir, M. Meghdadi, and Y. Guler. "A time and trust based wormhole detection algorithm for wireless sensor networks", in 3rd Information Security and Cryptology Conference (ISC'08), pp. 139-4, 2008.

[10] P Subhash andS Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks",*Third International Conference on Advanced Computing & Communication Technologies*, pp. 293-300, IEEE 2013.

[11] A.V.R.MAYURI, "Survey on Routing Metrics and Routing Protocols in Wireless Mesh Networks", *INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH (IJITR*), Volume No.2, Issue No. 4, pp.1110 – 1119, June – July 2014.

[12] Ali, S.A.V, Salem Jeyaseelan,, Hariharan S, "Enhanced Route Discovery in Mobile Ad hoc Networks", *Computing Communication & Networking Technologies (ICCCNT-IEEE)*, pp. 1–5,26th_28th July 2012, Coimbatore, India.

[13] Basu Dev Shivahare, CharuWahi, and Shalini Shivhare, "Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property", *International Journal of Emerging Technology and Advanced Engineering(IJETAE)*, Volume 2, pp. 356-359, March 2012.

[14] Ravinder Ahuja, Alisha BangaAhuja, andPawanAhuja, ,"Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs under Wormhole Attack". *In Proceedings of the 2013 IEEE Second International Conference on Image Information Processing,* pp. 699 - 702, ICIIP-2013.

[15] Ayomide Olanrewaju Ajayi, Adebisi Abimbola Adigun, andWasiuOladimejiIsmaila, "A Review of Routing Protocols for Practical Rural Wireless Mesh Networks", *International Journal of Computer Applications (IJCA),*Volume 114, pp. 14-17, March 2015.

[16] Sunil Kumar, "Reactive and Proactive Routing Protocols for Wireless Mesh Network using Multimedia Streaming", *International Conference on Recent Advances and Future Trends in Information Technology Proceedings published in (IJCA (International Journal of Computer Applications),*pp 13-17, 2012.

[17] Chems-eddine BEMMOUSSAT, Fedoua DIDI, and Mohamed FEHAM, "EFFICIENT ROUTING PROTOCOL TO SUPPORT QOS IN WIRELESSMESH NETWORK", *International Journal of Wireless & Mobile Networks (IJWMN)* Vol. 4, pp. 89-104 October 2012.

[18] Jaya Bhatt and Naveen Hemrajani, "Effective Routing Protocol (DSDV) for Mobile Ad Hoc Network", *(IJSCE) International Journal of Soft Computing and Engineering*, Volume-3, November 2013.

[19] Sandee pKaur and Supreet Kaur, "ANALYSIS OF ZONE ROUTING PROTOCOL IN MANET", *International Journal of Research in Engineering and Technology (IJRET)*, Volume: 02,pp. 520-524, Sep-2013.

[20] Siddiqui M.S. and Choong Seon Hong, "Security Issues in Wireless Mesh Networks", *IEEE2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07),* pp. 717 – 722,26-28 April 2007, Seoul, South Korea.

[21] Ratika Sachdeva andAashima Singla,"Survey on Privacy Issues and Security Attacks Wireless Mesh Networks", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSE*), Volume 3, April 2013.

[22] Parveen Sharma, "PERFORMANCE COMPARISON OF ROUTING PROTOCOLS IN WMNS"*, International Journal of Information Technology and Knowledge Management,* Volume 6, pp. 83-88, December 2012.

[23] Zubair Ahmed Khan, M. Hasan Islam,"Wormhole Attack: A new detection technique", IEEE2012.