RESEARCH ARTICLE OPEN ACCESS

Performance analyses of wormhole attack in Cognitive Radio Network (CRN)

Prabhjot * Er.Pooja Rani**
*(M.tech Student ,Department of CSE, Rayat & Bahra, Mohali Campus,Tehsil- Kharar,Punjab-140104,)
** (Associate Professor, Department of IT, Rayat & Bahra, Mohali Campus,Tehsil- Kharar,Punjab-140104)

ABSTRACT-
Mobile wirelesses networks are generally open to various attacks like information and physical security attacks than fixed wired networks. Securing wireless ad hoc networks is particularly more difficult for many of the reasons for example vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology etc. After that we initialize the number of nodes. Then implement protocol for the communication of nodes. Due to these protocols communication start. And this will be then implemented in CRNs which stand for cognitive radio network in which channel sensing is done. By the use of CRN security will be improved and performance will be enhanced. Find the malicious nodes occur in the network. One malicious node uses routing protocol to claim itself of being shortest path to last node but drops routing packets and doesn’t send packets to its neighbors. In last evaluate the parameters.

Keywords-Delay, Jitter, PDR, Throughput

I. INTRODUCTION OF MANET’S

A Mobile Ad-hoc Network (MANET) is a set of remote versatile hubs shaping an element self-sufficient system. Hubs speak with one another without the mediation of concentrated access focuses or base stations. In such a system, every hub demonstrations both as a switch and as a host. Because of the restricted transmission scope of remote system interfaces, numerous bounces are expected to trade information between hubs in the system. Portable Ad hoc Network is the quick becoming innovation from the previous 20 years. The addition in their notoriety is a result of the simplicity of arrangement, foundation less and their element nature. Manet’s made another set of requests to be actualized and to give effective better end to end correspondence. The Dynamic Source Routing (DSR) Protocol is a source routed on-interest directing convention [7]. A hub keeps up course reserves containing the source courses that it is mindful of. The hub overhauls entrances in the course reserve when it researches new courses. In its bundle head, every given directing parcel has a complete and requested hub list which the bundle will pass definitely [2].

A MANET is a kind of specially appointed system that can change areas and design itself on the fly. Since MANETS are portable, they utilize remote associations with join with different systems. This can be a standard Wi-Fi association, or an alternate medium, for example, a cell or satellite transmission [3]. A few MANETs are confined to neighborhood remote gadgets, (for example, a gathering of PCs), others may be joined with the Internet. Case in point, A VANET (Vehicular Ad Hoc Network), is a kind of MANET that permits vehicles to speak with roadside gear. While the vehicles might not have a direct Internet association, the remote roadside gear may be joined with the Internet, permitting information from the vehicles to be sent over the Internet [2]. The vehicle information may be utilized to gauge movement conditions or stay informed regarding trucking armadas. As a result of the element way of MANETs, they are regularly not extremely secure, so it is critical to be careful what information is sent over a MANET [4].

1.1 Congestion MANET

Congestion is a circumstance in communication organizes in which an excess of packets are exhibit in a piece of the subnet. Congestion may happens when the load on the system (number of packets send to the system) is more prominent than the limit of the system (number of packets a system can handle) [1]. Congestion prompts packet losses and data transfer capacity corruption and waste time and vitality on congestion recuperation .In Internet when congestion happens it is regularly focused on a single switch, because of the imparted medium of the MANET congestion won't over-burden the versatile hubs yet has an impact on the whole scope area. When the routing protocols in MANET are definitely not conscious about the congestion, it brings about the accompanying issues [18].

- **Long delay:** This holds up the methodology of locating the congestion. At the point when the congestion is more thorough, it is better to choose a substitute new way. Anyway the predominating on demand routing protocol defers the route seeking procedure [2].
- **High overhead:** More handling and correspondence attempts are needed for another route disclosure. In the event that the multipath directing is used, it needs extra exertion for maintaining the multi-ways paying little mind to the presence of alternate route [6].

1.2 Characteristics of MANETs

- **Dynamic topologies:** Nodes are free to move arbitrarily; thus, the network topology--which is typically multichip--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional, unidirectional links.
- **Bandwidth-constrained, variable capacity links:** Wireless links will continue to have significantly lower capacity than their hardwired counterparts [3]. In addition, the realized throughput of wireless communications after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
- **Energy-constrained operation**: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. The most important system design criteria for optimization may be energy conservation.
- **Limited physical security:** Mobile wireless networks are generally more prone to physical security threats than are fixed cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats [4]. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

1.3 SECURITY GOALS

Security includes a set of speculations that are enough financed. In MANET, all systems administration capacities, for example, steering and parcel sending, are performed by hubs themselves in a self-organizing way. Therefore, securing a versatile promotion -hoc system is extremely difficult. The objectives to assess if versatile adhoc system is secure or not are as per the following:

1. **Availability:** Accessibility implies the benefits are open to approved gatherings at fitting times. Accessibility applies both to information and to administrations [1]. It guarantees the survivability of system administration regardless of refusal of administration assault.
2. **Confidentiality**: It guarantees that computer related resources are gotten to just by approved gatherings. That is, just the individuals who thought to have admittance to something will really get that get to. To keep up secrecy of some private data, we have to keep them mystery from all elements that do not have benefit to get to them. Secrecy is frequently called mystery or protection [8].
3. **Integrity:** Trustworthiness implies that benefits can be altered just by approved gatherings or just in approved way. Change incorporates composing, evolving status, erasing and making. Trustworthiness guarantees that a message being exchanged is never defiled.
4. **Authentication**: Confirmation empowers a hub to guarantee the personality of associate hub it is corresponding with. Validation is basically certification that members in correspondence are confirmed and not impersonators. Validness is guaranteed in light of the fact that just the true blue sender can create a message that will unscramble legitimately with the shared key [11].
5. **Authorization**: This property relegates diverse access rights to diverse sorts of clients. For instance a system administration can be performed by system overseer just.

1.4 ATTACKS IN MANET

Securing remote impromptu systems is an exceedingly difficult issue. Understanding conceivable type of assaults is dependably the first step towards creating great security arrangements. Security of correspondence in MANET is vital for secure transmission of information [4]. Absence of any focal co-appointment system and imparted remote medium makes MANET more defenseless against advanced/digital assaults than wired system there are a number of assaults that influence MANET. These assaults can be characterized into two sorts:

1. **External Attack:** Outer assaults are done by hubs that don't have a place with the system. It causes blockage sends false steering data or reasons inaccessibility of administrations.
2. **Internal Attack:** Inward assaults are from bargained hubs that are a piece of the system. In an inward assault the noxious hub from the system increases unapproved access and mimics as a veritable hub. It can investigate activity between different hubs and may take an interest in other system exercises.

1.5 Wormhole Attack

Wormhole Attacks In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wireless or wired link with much less latency than the default links used by the network, and then relays them to another location in the network. In this paper, we assume that a wormhole is bi-directional with two endpoints, although multi-end wormholes are possible in theory [12]. A wormhole receives a message at its "origin end" and transmits it at its "destination end." Note that the designation of wormhole ends as origin and destination are dependent on the context. We also assume a wormhole is passive (i.e., it does not send a message without receiving an inbound message) and static (i.e., it does not move) [13].

1.5.1 Wormhole Detection Algorithm

Our wormhole geographic distributed detection (WGDD) algorithm uses a hop counting technique as a probe procedure. After running the probe procedure, each network node collects the set of hop counts of its neighbor nodes that are within one/k hops from it. (The hop count is the minimum number of node-to-node transmissions to reach the node from a bootstrap node.) Next, the node runs Dijkstra's (or an equivalent) algorithm to obtain the shortest path for each pair of nodes, and reconstructs a local map using multidimensional scaling (MDS) [16]. Finally, a "diameter" feature is used to detect wormholes by identifying distortions in local maps.
The main steps involved in the wormhole detection algorithm are described below:

1.5.2 Probe Procedure

Since a wormhole attack is passive, it can only occur when a message is being transmitted in the region near a wormhole. To detect a wormhole attack, we use a probe procedure that floods the network with messages from a bootstrap node to enable all network nodes to count the hop distance from themselves to the bootstrap node. The probe procedure is based on the hop coordinates technique [15]. Bootstrap Node: The bootstrap node x creates a probe message with (i = idx) to flood the network. Next, the bootstrap node drops all probe messages that originated from it. The bootstrap node has the hop coordinate hopx = 0 and offset = 0. Other Nodes: The probe procedure is presented in Procedure XX. In the procedure, node calculate its hop distance. Node b is a neighbor of node a; hopa is the minimum number of hops to reach node a from the bootstrap node (x) and its initial value is MAXINT. The combination of hopa and offset is the hop coordinate for node a. Na is the set of nodes that can be reached from node an in one hop, and |Na| is the number of nodes in Na [15].

1.5.3 Local Map Computation Procedure

In this step, each node computes a local map for its neighbors based on the hop coordinates computed in the previous step. After the hop coordinates are generated by the probe procedure, each node requests its neighbor nodes that are within one/k hops to send it their hop coordinates. After a node receives the hop coordinates from its neighbors, it computes the shortest paths between all pairs of nodes one/k hops away using Dijkstra's algorithm (or a similar algorithm) [13]. Next, multidimensional scaling (MDS) is applied to the (|Na|+1 × |Na|+1) shortest path matrix to retain the first two (or three) largest Eigen values and eigenvectors for constructing a 2-D (or 3-D) local map. Note that |Na| is the number of nodes that can be reached from node a in one/k hops. This step has a computational cost of O (|Na| 3 n) and a memory cost of O (|Na| 2) per node. No communication cost is associated with this step [11].

Probe procedure (for node a)

```
INPUT: message (hopb) from node b ∈ Na
for message (hopb) from any B ∈ Na and not TIMEOUT do
    if hopb < hopa then
        hopa = hopb + 1
        forward (message (hopa)) to MAC
    else
        drop (message (hopb))
    end if
end for
if |Na| == 0 then
    offseta = 0
else
    offseta = P b∈Na (hopb − (hopa−1)) +1 2(|Na|+1)
end if
return hopa and offset
```

1.6 DSR Protocol

The Dynamic Source Routing (DSR) protocol is one of the all the more for the most part acknowledged on demand directing protocol [3]. It is regular to consider the DSR convention with multiple courses since they might be fabricated amid the course disclosure by flooding. In the first DSR convention proposed in [1], the source host will choose the most limited course to the goal at first and will reserve all the substitute defeats. On the off chance that the first course breaks, the most limited staying exchange course is chosen. The methodology proceeds until all courses break, and then another course disclosure is started. In the second DSR convention, all transitional hubs are presently outfitted with a disjoint, interchange course. In the event that an information parcel is sent into a transitional host and the connection associating with the following host is broken, the exchange course from the middle of the road hub will be utilized for sending the all the later information bundles. Since some information bundles may be lost because of a connection break and the message about the information misfortune may not be sent again to the source have, the losing information bundles may not be detest and be lost for all time in the second DSR convention in [3]. Since of the likelihood of losing information parcels, we consider that the second DSR convention can't be utilized as a reasonable one [2].We note that an intriguing investigative model is created for breaking down the execution of DSR conventions. The execution utilized as a part of the investigation is the time interim between course disclosures for an information transmission in an on-interest DSR convention. This time interim between course disclosures is likewise the lifetime of the numerous courses utilized for the information transmission. Note that the lifetime for an information transmission changes progressively. On the off chance that the lifetime for an information transmission is shorter than the lifetime of numerous courses, it is not important to have long lifetime of different courses following the information transmission will finish before the begin of the following course disclosure [4]. Then again, the lifetime of an information transmission may be longer enough which may require more than two course revelations. The execution metric utilized as a part of [1] does not reflect the execution of the DSR conventions well.

There are two processes for route discovery and maintenance which are described below.

1. **Route discovery process in DSR-** At the point when a source hub needs to begin information transmission with a hub in the system, it checks its directing store. At the point when there is no course accessible to the objective in its store or course is lapsed, it shows RREQ [3]. At the point when objective is placed or any halfway hub that has crisp enough course to the end of the line hub, RREP is produced. At the point when the source hub gets the RREP it redesigns its stores and the movement is steered through the course [2].

2. Route maintenance in DSR-At the point when the transmission of information began, it is the obligation of the hub that is transmitting information to affirm the following jump got the information alongside source course [1]. The hub creates a course mistake message, on the off chance that it doesn't get any affirmation to the originator hub. The originator hub again performs new course disclosure process.

In this paper, we create a thorough expository model for the execution investigation of the numerous course DSR conventions for MANET [2]. At first, we present two execution measurements. The first metric is the likelihood that the lifetime of various courses is bigger than the lifetime of an information transmission [6]. It is simple to see that the bigger the likelihood is, the better the execution of a various course DSR convention is. We call the likelihood of a fruitful information transmission. The second metric is the likelihood that the various courses can be utilized for the following information transmission. Note that in the various course DSR conventions, the lifetime of various courses for a source S to goal D may be longer than the time interim between two information transmissions. It implies that a few courses utilized for an information transmission might likewise be accessible for the following information transmission [4]. The second metric is utilized to study the likelihood of utilizing various courses for the following information transmission, while the first metric demonstrates the likelihood of utilizing numerous courses for one information transmission. We infer both the likelihood of an effective information transmission and the likelihood that the various courses can be utilized for the following information transmission for the general case over n different courses. These systematic results give experiences into mechanics of the various DSR steering convention. It is likewise helpful for the configuration and usage of the on-interest directing for MANET.

1.7 Flow of work

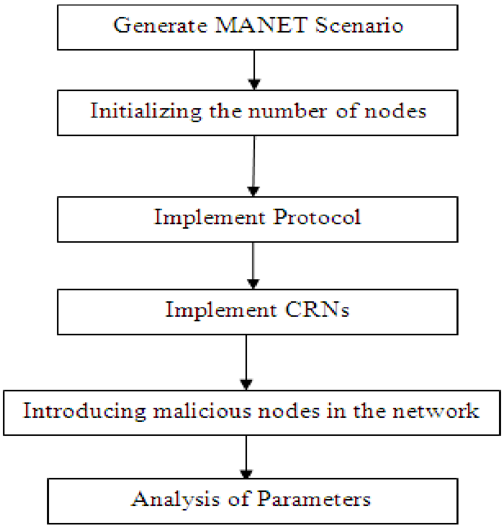

Fig.1 Flow of work

II. ALGORITHMIC STEPS

Step 1. Generate wireless scenario
Step 2. Initialize number of nodes
Step 3. Implement CRN
Step 4. Detect wormhole attack
a). Source send RREQ message.
b). RREQ received by intermediate nodes and then they send it to destination node.
c). Intermediate nodes update their routing table.

d). When destination received RREQ it sends RREP to source node.
e). When source node receives RREP it also record the route information in which hop count is stored.
f). Source node send additional message to destination which contain neighbor list and hop count.
g). Source neighbor list is SNL (i).
h). Destination neighbor list is DNL (j).
i). Comparison of both neighbor lists is done and hop count is compared.
j). If any mismatch occurred then there is attack and announcement is done regarding that.
Step 5. Detected node is blacklisted from network.
Step 6. Parameter evaluation

III. RESULTS AND DISCUSSIONS

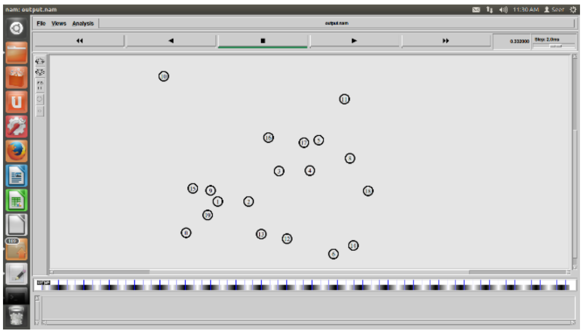

Fig.2 Representation of nodes

In this scenario the nodes take their respective positions.

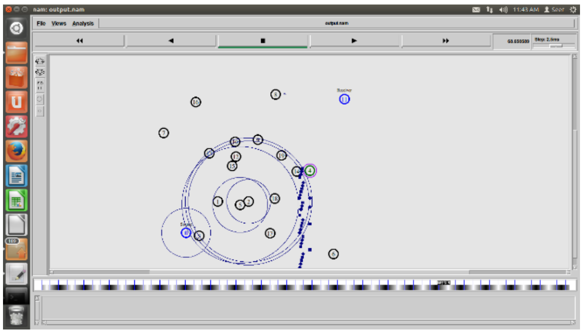

Fig.3 Representation of attacker

In this figure source and destination are defined. Node 14 starts sending the request to node 10. Node 10 is not sending request to next hop and hence, node 10 starts dropping data.

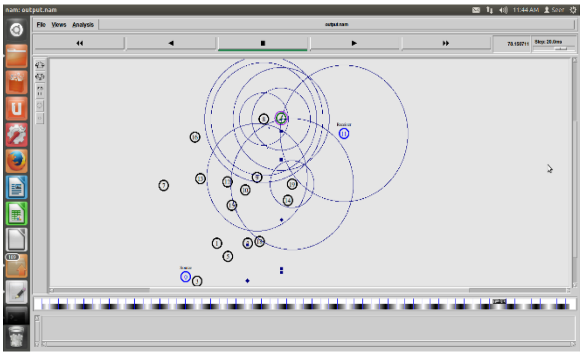

Fig.4 Applying CRCN

In this scenario it is found that node 4 is attacker. CRCN is applied for testing of node 4. Node 4 is blacklisted and sent out of the network.

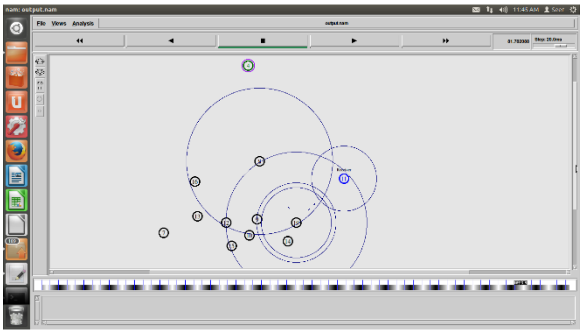

Fig.5 Representation Deletion of attacker

In this scenario remove the attacker that discarded the packets.

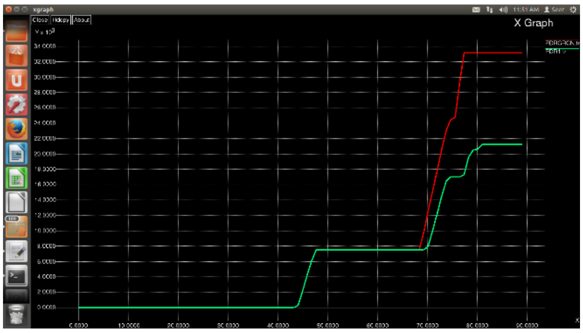

Fig.6 Represents PDR

This figure represents PDR with CRCN and without CRCN. The results for with CRCN are better as compared to without CRCN.

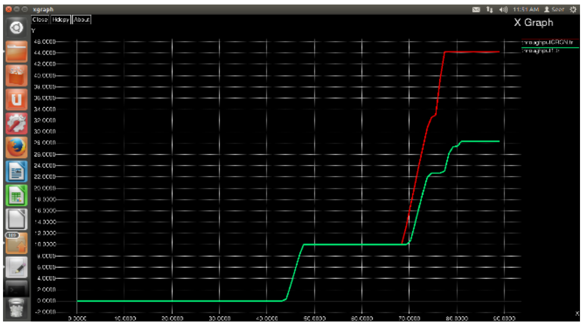

Fig.7 Represents throughput

Throughput is total number of successful bites received. This graph represents throughput

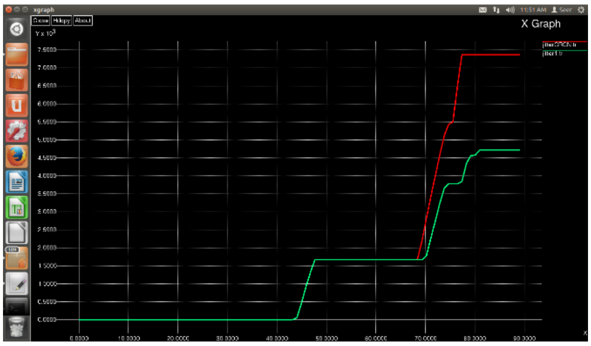

Fig.8 Represents jitter

This figure represents the jitter value with CRCN and without CRCN. Jitter is the deviation from true periodicity of a presumed periodic signal

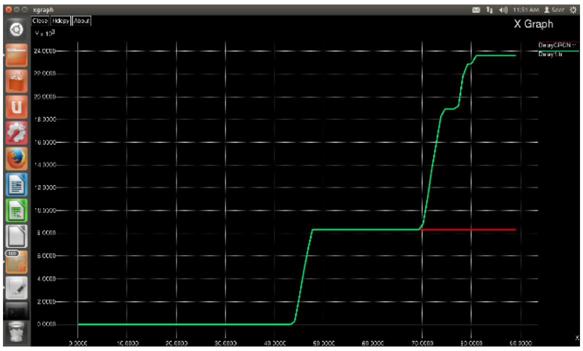

Fig .9 Represents Delay

This figure represents delay of nodes. With CRCN delay is lesser as compared to without CRCN hence, after applying CRCN result are better.

IV. CONCLUSION

Wormhole is one of the serious attacks. In this work network performance is analyzed under wormhole attack with or without cognitive radio cognitive network. This analysis is done on the bases of quality of service parameters like throughput, packet delivery ratio, delay and jitter. It is examine that for throughput, packet delivery ratio and delay CRCN gives better result but for jitter it gives high value as compare to without cognitive network. In future wormhole attack may be removed with other approach in cognitive network and also by using security mechanism it is prevented to occur.

REFERENCES

[1] Dong-Li Zhang**,** Wen-cheng Jiao, Zheng Jian-Ling "Research and improvement of Dsr protocol in Ad Hoc Network" *Industrial and Information Systems,2010*, vol.1, pp. 242-244.

[2] Zhiyong Shi, Shenquan Zhu, Zhenyu Zhang "Study on application of DSR protocol to mobile communication system" *IEEE* in *Mobile Technology, Applications and Systems, ,2005*, pp. 2 -5.

[3] Varshney , T, Katiyar, A. , Sharma, P. "Performance improvement of MANET under DSR protocol using swarm optimization" *Intelligent Computing Techniques* in *Issues and Challenges 2014*, pp. 58-63.

[4] Jhuria, M., Singh, S. "Improve Performance DSR Protocol by Application of Mobile Agent" *IEEE* in *Communication Systems and Network Technologies (CSNT),, 2014*, pp. 336-340.

[5] Ahmad, S, Awan, I. , Waqqas, A. ;,Ahmad, B. "Performance Analysis of DSR & Extended DSR Protocols" *International Conference* in *Modeling & Simulation,2008*, pp. 191-196.

[6] Shen Ming-yu, Li Cang-yuan, "Research and Analysis on Secure DSR Routing Protocol Based on Strand Space" *IEEE* in *Electrical and Control Engineering (ICECE)***,** *2010*, pp. 2917 – 2920.

[7] Yu-Liang Chang, Ching-Chi Hsu, "Connection-Oriented Routing in Ad Hoc Networks Based on Dynamic Group Infrastructur" *Fifth Symposium on Computers and Communications*, pp. 587-593.

[8] Ming-Hong Jiang, Rong-Hong Jan, "An EÆcient Multiple Paths Routing Protocol for Ad-hoc Net- works" *15th International Conference on Information Networking, 2001*, pp. 544-549.

[9] A. Nasipuri, R. Castaneda and S. Das, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks"*Mobile Networks and Applications*, vol. 6, pp. 339-349,2001.

[10] Vincent D. Park and M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks" pp. 1405-1413.

[11] Vincent D. Park and M. Scott Corson, "A Performance Comparison of the Temporally-Ordered Routing Algorithm and Ideal Link-State Routing" *IEEE Symposium on Computers and Communication 1998*, pp. 592-598.

[12] Revathi Venkataraman1, M. Pushpalatha1, T. Rama Rao,Rishav Khemka "A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks" *International Journal of Recent Trends in Engineering*, Vol. 1,pp. 220-222.

[13] Yurong Xu, Guanling Chen, James Ford,Fillia Makedon "Detecting wormhole attacks in wireless sensor networks" pp. 208-219.

[14] Sadeghi, M., Yahya, S. "Analysis of Wormhole attack on MANETs using different MANET routing protocols" *Fourth International Conference on Ubiquitous and Future Networks (ICUFN), 2012,*pp. 301 – 305.

[15] Khan, Z.A., Islam, M.H. "Wormhole attack: A new detection technique" *International Conference on Emerging Technologies (ICET), 2012,* pp. 1 – 6.

[16] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" *Third International Conference on Advanced Computing & Communication Technologies,2012*,pp. 283-287.

[17] Ravinder Ahuja,Alisha Banga Ahuja, Pawan Ahuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack" *IEEE Second International Conference on image processing,2013*,pp. 699-702.

[18] Mishra Durgesh Kumar (Acropolis Institute of Technology and Research, Indore, India). Chandel Mahakal Singh (Arjun Institute of Advaced Studies and Research Centre, Indore, India), Sheikh Rashid. *Security Issues in MANET: A Review.*