A Review on Mobile Ad-Hoc Networks Routing Protocols.

Angad Bharti, Hirdesh Varshney
Computer Science and Engineering,
Bansal Institute of Engineering and Technology, Lucknow, India

Abstract-- Ad Hoc device are widely recognized and helpful as a result of infrastructure much less nature. Ad-hoc Network is a meeting of hubs, wherein singular hubs corporate by means of sending packets for every different to permit hubs to deliver beyond direct transmission range. Security is principally worry with a selected cease goal to provide ensured correspondence between cell nodes in antagonistic environments. Countless conventions for MANET has been proposed to empower brisk and effective gadget advent and rebuilding MANET (Mobile Ad-hoc Network) alludes to a multi-hop packet primarily based wi-fi network constructed from an association of flexible hubs that can bring and flow in the interim , without utilising any kind of settled stressed out foundation . MANET'S are without a doubt self arranging and flexible systems that may be fashioned and distorted on-the-fly without the want of any focused business enterprise. It by way of and huge works via TV the information and applied air as medium. It's telecasting nature and transmission medium likewise help assailant to disturb system. Numerous sort of attack need to be feasible on such Mobile Ad Hoc Network. The accentuation of this paper to study wormhole attack, a few detection approach and exceptional strategies to save you network from those attack.

Keywords: AODV, MANET, Intrusion Detection, and Worm Hole Attack,.

1. Introduction:

A Mobile Adhoc Network is a set of impartial cell nodes that can communicate to every different through radio waves. The cellular nodes which might be in radio variety of every other can at once speak, while others wishes the useful resource of intermediate nodes to direction their packets. Each of the node has a wi-fi interface to speak with every other. [1] These networks are completely distributed, and may paintings at any vicinity with out the assist of any fixed infrastructure as get entry to points or base stations.

Mobile advert hoc networks are self reliant systems comprised of a number of cell nodes that communicate using wireless transmission. They are self-organized, self-configured and self managed infrastructure-less networks. This sort of network has the advantage of being capable of be installation and deployed fast as it has a easy infrastructure set-up and no vital administration. Obvious examples are within the navy or the emergency offerings. One situation is establishing conversation among numerous sellers in a disaster healing operation in which e.G. Fire fighters want to connect to neighborhood ambulances and visitors control in circumstances where the normal conversation infrastructure is destroyed or otherwise rendered unusable. In such situations a collection of cellular nodes with wireless community interface can form a transitory community. These networks are particularly beneficial to those cellular users who want to talk in conditions where no fixed stressed out infrastructures are available. However, the salient feature of making a network 'at the fly' without requiring any prearranged infrastructure gave cell ad hoc networks an liked interest in each industrial and military systems.

2. Related Work:

In multi-hop wireless systems, the want for cooperation among nodes to relay each other's packets exposes them to a wide variety of protection assaults. A especially devastating attack is the wormhole assault, wherein a malicious node information control visitors at one location and tunnels it to any other compromised node, probable far away, which replays it regionally. Routing safety in ad hoc networks is frequently equated with sturdy and feasible node authentication and light-weight cryptography. Unfortunately, the wormhole attack can rarely be defeated by way of crypto graphical measures, as wormhole attackers do no longer create separate packets. They absolutely replay packets already existing on the community, which skip the cryptographic assessments. Existing works on wormhole detection have regularly focused on detection using specialised hardware, such as directional antennas, and so on. In this work, we present a cluster based counter-degree for the wormhole attack, that alleviates these drawbacks and correctly mitigates the wormhole assault in MANET. Simulation results on MATLab showcase the effectiveness of the proposed set of rules in detecting wormhole attacks by Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki (2009) [1].

In this paintings, a new cluster based totally wormhole detection approach has been proposed. In multi-hop wi-fi structures, the need for cooperation among nodes to relay every different's packets exposes them to a huge variety of security threats together with the wormhole assault. A quantity of recent works were studied before presenting this new methodology. The proposed solution unlike some of its predecessors does now not require any specialized hardware like directional antennas, and so on for detecting the attackers. Or extraordinarily accurate clocks, and so forth. The simulation using 30 nodes and variable quantity of protect nodes prove the effectiveness of the proposed set of rules. Currently greater studies are being accomplished to analyze the overall performance of the proposed set of rules in presence of more than one attacker nodes.

Rutvij H. Jhaveri et. Al. (2010) [2], in line with them in this era of wi-fi gadgets, Mobile Ad-hoc Network (MANET) has turn out to be an indivisible element for communication for cellular gadgets. Therefore, hobby in research of Mobile Ad-hoc Network has been growing considering previous couple of years. In this paintings we've got discussed some primary routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a massive difficulty in MANETs as they may be infrastructure-less and self sustaining. Main objective of writing this paintings is to deal with some primary protection issues in MANET, operation of wormhole attack and securing the famous routing protocol Ad-hoc On Demand Distance Vector. Their work

could be a great help for the humans undertaking studies on actual world troubles in MANET safety.
MANETs require a reliable, efficient, scalable and most significantly, a cozy protocol as they are notably insecure, self-organizing, swiftly deployed and that they use dynamic routing. AODV is prone to assaults like amendment of sequence numbers, change of hop counts, supply path tunneling, spoofing and fabrication of errors messages. Although fabrication of source routes (cache poisoning) isn't viable in AODV while DSR is vulnerable to it. Wormhole attack is a actual threat towards AODV protocol in MANET. Therefore, truthful strategies for coming across and detection of wormhole attack should be used. We ought to understand that a few solutions might not work well inside the presence of multiple malicious node, at the same time as a few require special hardware and a few answers are very costly. So, there may be nonetheless a number of room for studies on this region to provide a greater secured MANET.

The infrastructure of a Mobile Ad hoc Network (MANET) has no routers for routing, and all nodes need to proportion the same routing protocol to assist every different when transmitting messages. However, nearly all common routing protocols at gift remember performance as first precedence, and have little protection capability in opposition to the malicious nodes. Many researches have proposed various protocols of higher safety to defend in opposition to assaults; however, every has particular defense items, and is unable to defend against unique assaults. Of all the types of attacks, the wormhole assault poses the best hazard and could be very difficult to prevent; therefore, A.Vani et. Al. (2011) [3], targeted on the wormhole assault, by combing three techniques. So that our proposed scheme has 3 strategies based on hop remember, decision anomaly, neighbor list count number methods are combined to stumble on and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to act and which to direction the packets in secured manner.
In this examine they analyzed the effects of wormhole attack in advert hoc wireless networks. They implemented an AODV protocol that simulates the conduct of wormhole attack in NS-2.In this technique we've used quite simple and effective manner of presenting security in AODV routing protocol against wormhole assault that causes the interception and confidentiality of the advert hoc wireless networks. Security in opposition to wormhole attack is furnished via using a easy wormhole set of rules. This set of rules has higher overall performance comparing to three person methods [Hop count, Anomaly based, Neighbor list methods].The solution detects the malicious nodes and isolates it from the active statistics forwarding. As from the effects we will without problems infer that the performance of the normal AODV drops under the presence of malicious program hollow assault.

In multihop wi-fi adhoc networks, cooperation among nodes to course every other's packets exposes those nodes to a wide range of security attacks. Also due to the vulnerability of the routing protocols, the wi-fi ad-hoc networks face several security dangers. A in particular severe protection assault that influences the adhoc community routing protocols, is referred to as the wormhole assault. The wormhole assault is executed as a section method released by means of one or a couple of malicious nodes. In the first segment, those malicious nodes, referred to as as wormhole nodes, try and trap valid nodes to ship records thru them by using taking part inside the network. In the second one section, wormhole nodes should make the most the information & affect the conversation by using misbehaving.
In this work Pirzada Gauhar Arfaat, Dr. A.H. Mir (2011) [4], have simulated the wormhole assault in wireless adhoc networks & Manet's. And then they evaluated & mentioned the effect on the network by using evaluating the effects with out and with wormhole assault. The Wormhole attack became simulated the use of distinctive scenarios. Thus they studied the impact of the wormhole assault at the respective networks. The parameters like throughput, packet loss and cease-to-end delay have been calculated the use of one-of-a-kind situations for evaluating the effect on wireless adhoc networks and Manet's.
Wormhole assaults in wireless adhoc networks can severely become worse the network performance and compromise the safety thru spoiling the routing protocols and weakening the security upgrades. In this work we simulated the wormhole attack in AODV in wireless adhoc networks and Manet's and studied its effect on the overall performance of the network. For this motive we changed & implemented a new AODV routing protocol which behaves as wormhole. We simulated exceptional situations, where each one has one or two wormhole nodes that use the modified "B" AODV protocol. In distinct situations we changed the area of the wormhole nodes to assess the effect. Moreover, we changed the wide variety of nodes in different topologies. The packet loss was measured. Similarly other parameters like throughput and end- to -give up delay due to wormhole attack became calculated and
effects had been produced inside the shape of graphs the usage of MS Excel 2010. The main benefit of this work is that it enlightens the vulnerabilities of the AODV protocol. Besides the take a look at will assist us to overcome the AODV protocol flaws in order that it may be made greater strong towards the assault. Also the work gives the overall dimension of the effect whilst a network is below the wormhole attack and enables in designing the topology which is extra robust. The problem of the simulation is that the size of the impact on MANETs turns into hard when the mobility of the nodes increases an excessive amount of. The possible software of this paintings is that the have a look at can help to determine the effect on different routing protocols and other layers also. Another software of our paintings is in determining the effect on sensor and mesh networks whilst under wormhole assault or other attacks as properly.

A Mobile Ad hoc Network (MANET) is a collection of self configurable cell node linked thru wi-fi hyperlinks. In MANET nodes that are in the range of each different can connect directly wherein as nodes which aren't in the area of every different depend upon the intermediate node for communication. Each node in MANET can work as a sender, receiver as well as router. Communication inside the community depends upon the trust on every other. In wormhole assaults, one malicious node tunnels packets from its region to the other malicious node. Such wormhole assaults bring about a false path with fewer. If source node chooses this fake route, malicious nodes have the choice of delivering the packets or dropping them. It is hard to locate wormhole assaults due to the fact malicious nodes impersonate valid nodes The wormhole attack is viable although the attacker has not compromised any hosts and even if all verbal exchange provides authenticity and confidentiality. In this work, Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia (2012), [5] analyzed wormhole assault nature in ad hoc and sensor networks and present methods of the defending mechanism to come across wormhole assaults without require any specialized hardware. This evaluation able to provide in setting up a

way to reduce the rate of refresh time and the reaction time to end up more faster.

In order to keep away from the trouble of the usage of special hardware, a Round Trip Time (RTT) mechanism is proposed by means of Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. A will calculate the RTT among A and all its pals. Because the RTT among fake pals is better than among two actual neighbors, node A can perceive each the faux and actual acquaintances. In this mechanism, each node calculates the RTT between itself and all its friends. This mechanism does not require any special hardware and it is easy to put into effect; but it can not stumble on uncovered attacks due to the fact fake acquaintances are created in exposed assaults. The Delay according to Hop Indicator (DelPHI) proposed with the aid of Hon Sun Chiu and King-Shan Lui, can locate both hidden and exposed wormhole assaults. In DelPHI, attempts are made to locate every available disjoint path between a sender and a receiver. Then, the postpone time and period of each direction are calculated and the common postpone time per hop alongside each direction is computed. These values are used to pick out wormhole. The course containing a wormhole link may have a more Delay in line with Hop (DPH) fee. This mechanism can hit upon both sorts of wormhole attack; however, it cannot pinpoint the location of a wormhole. Moreover, due to the fact the lengths of the routes are changed by means of each node, along with wormhole nodes, wormhole nodes can exchange the direction period in a positive manner in order that they can't be detected. Packet Leash is an approach in which some records in added to limit the maximum transmission distance of packet. There are two sorts of packet leashes: geographic leash and temporal leash. In geographic leash, whilst a node A sends a packet to any other node B, the node need to consist of its place records and sending time into the packet. B can estimate the gap between them. The geographic leash computes an upper bound on the distance, while the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes should have tight time synchronization. The maximum difference between any nodes' clocks is bounded through Δ, and this value have to be regarded to all of the nodes. By the usage of metrics mentioned above, every node checks the expiration time inside the packet and decide whether or not or no longer wormhole attacks have happened. If a packet receiving time exceed the expiration time, the packet is discarded. Unlike Packet Leash, Capkun et al. Supplied SECTOR, which does no longer require any clock synchronization and area data, by using using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to any other node B in its transmission variety via sending it a one-bit task, which A responds to immediately. By using the time of flight, A detects whether or not or no longer B is a neighbor or no longer. However, this approach makes use of special hardware that may respond to a one-bit assignment without any delay as Packet leash.

Multicast is a good technique to implement the organization verbal exchange. In recent years, some of distinct multicast protocols had been proposed for ad hoc networks. Robust and Scalable Geographic Multicast Protocol (RSGM) is one in all them. RSGM is a geographic routing protocol which routes the statistics the usage of the vicinity of the nodes. Geographic routing protocols are known to be mainly at risk of attacks. One of the maximum effective and severe assaults in adhoc networks is wormhole attack, stopping this attack has proven to be very hard. In this work, an efficient approach specifically Multicast Authentication Node Scheme is devised to detect and avoid wormhole attack inside the RSGM protocol. This technique uses cryptographic concept to stumble on and save you wormhole assault. L. Sudha Rani , R. Raja Sekhar (2012), [6], proposed machine is simulated in network simulator (NS-2). The Geographic multicasting routing mechanism has been provided on this paintings. Among the prevailing multicasting routing protocols the motive for choosing RSGM protocol is it handles empty sector problem very correctly whilst compared to the other region primarily based protocols and it has an efficient supply monitoring mechanism which avoids the periodic flooding of supply data. RSGM has the minimal manipulate overhead and joining delay. The protocol can also scale to a large organization size and a big community size, and may more efficiently support a couple of multicast groups in the network. One feasible assault on the RSGM protocol has been discussed on this paintings. The detection of such attack is difficult and is of path very a great deal critical. Multicast Authentication Node Scheme is the answer this is proposed to shield against the wormhole assault in RSGM protocol. This answer really suggests that the protocol achieves higher Packet Delivery Ratio under all circumstances with different shifting speeds, node densities, group sizes, and community sizes.

Mobile ad hoc networks (MANETs) is an infrastructure-much less , dynamic network together with a collection of wireless cellular nodes that communicate with every different without the usage of any centralized authority. Due to its essential traits, including wireless medium, dynamic topology, distributed cooperation, MANETs is at risk of diverse varieties of protection assaults like trojan horse hole, black hollow, speeding attack and so on. In this work Aarti et. Al., (2013) [7], studied mobile ad-hoc community and its traits, demanding situations, application, safety desires and different types safety assaults at exceptional layers.

Due to dynamic topology, dispensed operation and restricted bandwidth MANET is greater prone to many attacks. In this paintings, Aarti et. Al., (2013) [7] discussed MANET and its characteristics, demanding situations, advantages, application, protection desires, diverse forms of protection assaults in its routing protocols. Security attack can categorized as a energetic or passive attacks . Different safety mechanisms are delivered so that it will save you such community.

Jyoti Thalor et. Al., (2013) [8], in step with them MANET (Mobile Ad-hoc Network) refers to a multi-hop packet primarily based wi-fi network composed of a hard and fast of mobile nodes that could speak and move at the equal time , without using any form of fixed wired infrastructure . MANET'S are without a doubt self organizing and adaptive networks that may be formed and deformed on-the-fly with out the want of any centralized administration. It typically works through broadcasting the statistics and used air as medium. It's broadcasting nature and transmission medium additionally help attacker to disrupt network. Many sort of attack may be completed on such Mobile Ad Hoc Network. The emphasis of this work to study wormhole assault, a few detection technique and exceptional techniques to prevent community from these attack.

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an phantasm that faraway areas of a MANET are at once connected thru nodes that appear like pals but are certainly distant from one another. A wormhole assault is a particularly severe assault on MANET routing where attackers, related by means of a excessive-

velocity off-channel link, are strategically positioned at one of a kind ends of a community. Consider Fig 2 [8] wherein node A sends RREQ to node B , and nodes X and Y are malicious nodes having an out-of-band channel between them . Node X "tunnels" the RREQ to Y , that is valid neighbor of B. B gets two RREQ – A-X-Y-B and A-C-D-E-F-B. The first path is shorter and quicker then the second, and chosen by using B. Since the transmission between nodes has rely upon relay nodes, many routing protocols were proposed for advert hoc community. In a wormhole assault, attackers "tunnel" packets to any other location of the network bypassing everyday routes as proven in Figure 1. The ensuing course through the wormhole may additionally have lower hop depend than ordinary routes. In with this leverage, attackers the use of wormhole can without difficulty manipulate the routing precedence in MANET to carry out eavesdropping, packet change or carry out a DOS assault . The complete routing machine in MANET may even be introduced down the usage of the wormhole assault [8].

Wormhole assaults in MANET significantly degrade community performance and hazard to community security. Here we have basically surveyed the prevailing techniques as a way to assist us in future to layout a brand new approach for detecting the wormhole attack in Mobile Ad Hoc community .Overall a substantial quantity of labor has been accomplished on fixing wormhole assault trouble. We cannot say one answer is relevant to all conditions. So there's choice of answer available based totally on value, want of security might also lead higher end result, however can be highly-priced, which might also have an effect on different networks need. Similarly a few network require greater protection like army region community. A trendy solution remains lacking, even though numerous very useful solutions relevant to a few networks had been described.

Mobile Adhoc Networks(MANET's) are refers to self organizing in nature. In MANET's conversation is done through multi hops with dynamic topology. Mobile nodes ship statistics through wireless hyperlinks, this means that less relaxed environment and at risk of various assaults. There are various sorts of assaults which impact the records when it transfers from the source node to the destination node but wormhole attacks are most risky attacks and really regularly took place inside the wi-fi surroundings. In this paintings Chandandeep kaur and Dr. Navdeep Kaur, (2014) [9], mentioned the various detecting and stopping strategies for wormhole assaults.

The Mobile Ad Hoc community is greatly motivated with the aid of wormhole assault .These assaults degrade the community overall performance and risk to network safety .In this work numerous techniques are presented for detection and prevention of wormhole assaults .In destiny these techniques will help to efficiently take away the malicious nodes from the Mobile Ad Hoc networks .All above techniques based on various factors like cost ,want of security ,Quality of Service may also lead better result however can be luxurious . So they can not say that one solution is flawlessly cope with all situations .One thing may additionally have impact on the other factor .Like a few networks need greater security like whether forecasting and military vicinity might also growth the fee. From all above answers we can find the green approach to save you the wormhole attacks by way of equating all elements.

Mobile Adhoc Networks (MANET) are self organizing, decentralized networks and own dynamic topology, which lead them to attractive for routing assaults. Attacks on ad hoc networks can be labeled as passive and energetic assaults, depending on whether the normal operation of the community is disrupted or not. The security of the AODV and DSR protocol is compromised via a specific form of attack called 'Worm hollow assault'. Wormhole attack is a community layer attack discovered in MANET, which absolutely disrupts the communication channel. In This work Mohamed Otmani, and Dr. Abdellah Ezzati, (2014) [10], analysed the overall performance of AODV and DSR routing protocols with and without wormhole assault the use of Network Simulator 2. For analyzing the performance we taken into consideration total packets received, overall bytes acquired, first packet obtained, last packet received, average quit-to-quit postpone and throughput as measures.

The safety of the Ad Hoc community routing protocols continues to be an open problem and deserves greater research work. In this work, they analyzed effect of the Worm Hole attack in AODV and DSR routing. We have implemented Worm hole Attack in opposition to AODV and DSR routing protocol the usage of Network Simulator 2, for reading the overall performance we considered total packets received, general bytes received, first packet received, closing packet obtained, average give up-to-stop put off and throughput as measures. We supplied the consequences of assessment of both protocols. The effects show that DSR plays better than AODV. Wormhole attack is a actual danger towards routing protocols in MANET .The detection and evasion of wormholes in an advert-hoc community continues to be considered as destiny hard challenge.

The modern demand of MANET is its protection and robustness. MANET's operational overall performance additionally relies upon on security. An attacker can effortlessly attack on MANET because of its open nature and bandwidth constraint. Most of research were carried out on the MANET security. Wormhole attack is maximum extreme chance to security of MANET. In which far flung malicious nodes are linked to every different with excessive pace hyperlink called wormhole tunnel. Most of preceding studies paintings finished on detection and prevention of wormhole assaults makes use of packet leashes, extra hardware (GPS, Directional Antenna and so forth.) and few modifies the source code of routing protocols to improve protection. In this work, we recommend a safety model so one can hit upon and avoid the wormhole assault in MANET the usage of routing protocol i.E., AODV protocol. Gulzar Ahmad Wani, and Dr. Sanjay Jamwal (2015) [11], proposed protection model has 3 phases. In the primary segment, detection of malicious node is performed via the usage of Bogus RREQ and in second segment normal AODV operation is finished for detection of shortest course from source to destination. In the 0.33 section, over again detection of attacker is carried out via the use of delay metric if there is presences of wormhole attack then it repeats from phase one in any other case selects the shortest direction to vacation spot determined in section second.

In this Work, they have proposed a safety model in order to detects and avoids the wormhole attack in Mobile Ad-hoc Network and makes MANET unfastened from Wormhole attack. This proposed version is easy and does not use any hardware. In the primary section, it'll stumble on the malicious node in MANET via the use of Bogus RREQ and then take away the involvement of malicious node in the Network and in 2d phase practice AODV protocol for finding the shortest path to the vacation spot. In the ultimate section, it once more checks for presence of wormhole assault the use of common put off. If there may be presence of wormhole assault then start from segment one again

otherwise select the route for information transmission that turned into determined in 2d segment.

Samuel Jacob, D D Ambavade, and K T V Talele, (2015) [12] in step with them the Mobile Ad hoc Networks (MANETs) is a collection of wireless nodes which have interaction with each different via sending packets to each other or on behalf of some other node, with none vital network infrastructure to control facts routing. For verbal exchange, the nodes cooperatively forward information packets to other nodes in network by means of using the routing protocol. But, those routing protocols aren't comfy, for this reason paving the way for the MANET to be open to malicious attacks. A malicious assault that's usually found in MANET environment is wormhole assault. The objective of this work turned into to research the performance parameters of throughput, put off and packet loss in AODV with the existence of wormhole assault. Simulation outcomes have shown that the performance parameters are affected very plenty whilst there may be an assault due to wormholes.
The performance of an on- call for routing protocol i.E. AODV (Ad hoc on call for distance vector routing) is evaluated with and with out wormhole attack. Three parameters of performance i.E packet delivery ratio, throughput, and common end to cease put off had been taken into consideration. Results show that AODV performance receives badly suffering from the wormhole attack.

3. Conclusion:

As of overdue, with the appearance of globalization, the sector is seeing a lofty development of relaxed MANET association with excessive diploma of pace and accuracy. The global is converting itself into little and extensive portions of social and business structures from a solitary township to a global city which thusly makes the development with safety issues bringing approximately excessive reliability degree to the give up to stop customers. System attack region and reliable directing is necessary for the destiny economic achievement and device protection. Delicate figuring techniques, for instance, fluffy motive, neural systems, hereditary calculations are being embraced in demonstrating to decisively delineate trendy MANET frameworks. In this paper, an endeavor has been made to audit the utilizations of slicing area method based totally fashions utilized as part of identity of pernicious hubs in MANET frameworks in view of fashions to be specific Geographical/Temporal rope, RTT, DELPHI, E2IW and TAODV packages. It is located that AODV based totally exceptional fashions are widely utilized as a part of overdue years for assessment of notable level steering along with assault disclosure, with maximum restricted course following in MANET frameworks with streamlining on the premise of gadget and hub behavior criteria. The survey shows that grouping primarily based models provide sensible gauges especially resulting from heat hollow attack.

References:

[1] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.
[2] Rutvij H. Jhaveri et. al., "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
[3] A.Vani et. al., " A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011.
[4] Pirzada Gauhar Arfaat, Dr. A.H. Mir, "The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.
[5] Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.
[6] L. Sudha Rani , R.Raja Sekhar, "Detection And Prevention Of Wormhole Attack In Stateless Multicasting", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.
[7] Aarti et. al., "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
[8] Jyoti Thalor et. al., "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.
[9] Chandandeep kaur and Dr.Navdeep Kaur, "Detection and Prevention Techniques for Wormhole Attacks", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4926-4929.
[10] Mohamed Otmani, and Dr. Abdellah Ezzati, "Effects Of Wormhole Attack On AODV And DSR Routing Protocol Through The Using NS2 Simulator", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014).
[11] Gulzar Ahmad Wani, and Dr. Sanjay Jamwal, "Security Model to Detect and Avoid Wormhole Attack Using AODV Protocol", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1044-1049.
[12] Samuel Jacob, D D Ambavade, and K T V Talele, "Performance Evaluation of Wormhole Attack In AODV" Int. Journal of Engineering Research and Applications, Vol. 5, Issue 1, (Part -6) January 2015, pp.70-72.