IJCSE International Journal of Computer Sciences and Engineering Open Access
ResearchPaper Volume-03, Issue-7 E-ISSN: 2347-2693

Performance Analysis of Threshold Based Algorithms under Wormhole Attack in MANET

G.Kalpana[1*] and S.Archana[2]

[1]*Computer Science, Bharathiar University, India,*

www.ijcseonline.org

Received: 25/07/2015 Revised:31/07/2015 Accepted: 27/07/2015 Published: 31/07/2015

Abstract— An ad hoc network refers to a network connection established for a single session and does not essential a router or a wireless base station. A MANET is a collection of mobile nodes connected through wireless networks. MANET can join and leave the network dynamically. However, MANET is particularly vulnerable due to its fundamental characteristics, such as dynamic topology, distributed co-operation, and constrained capability. One main challenge on designing these networks is their vulnerability to security attacks.In this paper the performance of Threshold Based Algorithms using routing protocols AODV and DSR with wormhole attack detection have been analysed using NS2 considering various parameters such as packet delivery ratio and average throughput to evaluate its performance.

Keywords—MANET;AODV;DSR;Wormhole

I. INTRODUCTION

A MANET is a collection of mobile nodes connected through wireless networks. The nodes in MANET themselves are reliable for dynamically discovering other nodes to communicate. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of capability and topology. Each node performs their function as a router or host [1].Due to dynamic infrastructure-less nature and lack of centralized monitoring; the ad hoc networks are vulnerable to several attacks. The behavior of network and reliability is compromised by attacks on ad hoc network routing protocols. In MANET security challenges have become a primary concern to provide secure communication. Due to the Mobility of the nodes the situation becomes even more complicated [1]. Routing protocols can be classified into three categories viz., proactive, reactive and hybrid protocols. Many routing protocols such as AODV, OLSR, and DSR etc were developed for MANET. In this study, wormhole attack is compared using AODV and DSR with NS-2 simulator and the result is produced. The Network Simulator-2 is a widely used software tool for MANET. DSR (Dynamic Source Routing) is on-demand, simple and efficient routing protocol for multi-hop wireless ad hoc networks of mobile nodes [15]. AODV (Ad hoc on-demand distance vector) enables self-configuring, dynamic, multi-hop on-demand routing for mobile wireless ad hoc network. Round Trip Time is defined as which measures the time between data transmission and the receipt of a positive acknowledgment. Path tracing approach is used to find and eliminate the exact misbehaving node in the network. Secured wireless ad hoc is a highly challenging issue. As the wireless medium is vulnerable to eavesdropping and snooping, ad hoc network functionality is established through node co-operation. The attacks can be divided into two types:

-Passive attacks
-Active attacks

A. Passive attacks

A passive attack does not modify the data broadcast within the network. But it includes the unauthorized "listening" to the network traffic from it. Passive attacker does not interrupt the operation of a routing protocol but challenges to determine the important information from routed traffic [3].

B. Active attacks

Active attacks are very hard attacks on the network that prevent message flow between the nodes. Active attacks can be classified as internal or external. Active external attacks can be assumed by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more ruthless and hard to identify than external attacks [3].

II. OVERVIEW OF WORMHOLE ATTACK

Wormhole attack involves the cooperation between two attacking nodes. One attacker catches the packet and tunnels it to the other attacker. The link between the attackers is high speed communication link. These two attackers bring the topology under their control. A malicious node receives data packet at one point in the network and tunnels them to another malicious node. The tunnel exists between two malicious nodes is referred to as a wormhole.

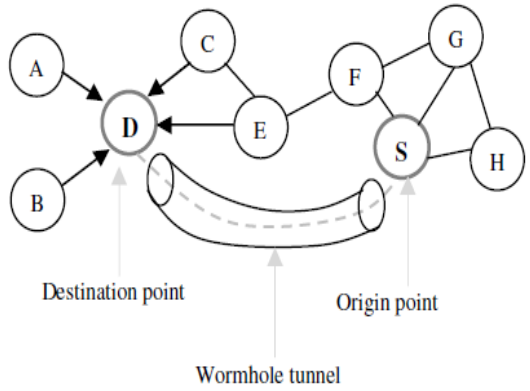

Fig.1. Wormhole Attack

In figure 1, Here D and S are the two end-points in the wormhole tunnel. D is the source node and S is the destination node. Node D is assuming that there is direct connection to node S so node D will start transmission using tunnel discovered by the attacker. This tunnel can be created by number of ways including long-range wireless transmission. An attacker records packets at one end in the network and tunnels them to other end-point in the network [10]. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV and DSR, then all the packets will be transmitted through this tunnel and no other route is discovered. If single path on-demand routing protocol such as AODV is being used in highly dynamic wireless ad hoc networks, a new route need to be discovered in response to every route break.

If the attacker creates the tunnel honestly and reliably than it will not harm the network and also provides useful service in connecting the network more efficiently [10]. The attacker can perform the attacks even if the network communication provides confidentiality and authenticity.

III. RTT CALCULATION IN AODV

Ad hoc On-Demand Distance Vector (AODV) is also an on-demand MANET routing protocol. AODV is a Reactive protocol. It is loop-free, self-configuring and scales to large numbers of mobile nodes. AODV builds routes using a route request/route reply query cycle. Basically AODV maintains two phases: Route Discovery and Route Maintenance [5]. AODV finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes.

When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the routing information is confidential, encrypted or authenticated, it can be very effective and damaging.

An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication, as AODV would be unable to find routes longer than one or two hops. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker [6]. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

The proposed detection mechanism is only based on the Round Trip Time of route request and reply message and the number of neighbours suspected nodes. This mechanism does not need any special hardware or synchronized clocks because it only considers its local clock to calculate the RTT [4]. The work consists of three phases. The first phase is to construct neighbours list for each node and the second phase is to find the route between sources to destination node and the last phase is to find the location of wormhole link.

Each node sends the route request (RREQ) message to the neighbour's node and save its time .The intermediate node also forwards the RREQ message and saves its sending time. When the RREQ message reaches the destination node, it sends route reply message (RREP) with the reserved path. When the intermediate node receives the RREP message, it saves the time of receiving of RREP. Every node save the time they forward RREQ and the time they receive RREP from the destination to calculate the RTT.

If there is no attack, the values of them are nearly the same. If the RTT value is higher than other successive nodes, it can be suspected as wormhole attack between this links.

A. Network deployment phase

Step 1: Deploy ad hoc nodes randomly to form a network.
Step 2: Neighbour list of each node is generated.

B. Malicious node detection

Step 1: Use local clock to calculate Round Trip Time.
To calculate RTT, every node will have two time stamps values which store

- Forwarding time of the request from source to destination (RREQ) i.e. the Route request.
- Receiving time of the reply to source back i.e. Route reply (RREP).

Then find RTT of each node by calculate the differences between those two stored times i.e. RTT = trep – treq.
Step 2: Compute per hop distance value using RTT values.

Step 3: Each node in a path computes per hop distance with its neighbours and compares it with the prior per hop distance.
Step 4: Calculate maximum and minimum values of RTT.
Step 5: If (RTT max < 2 RTT min)
No wormhole attack presents in the network
Else if (RTT>=threshold value)
Wormhole attack detect between the following nodes.

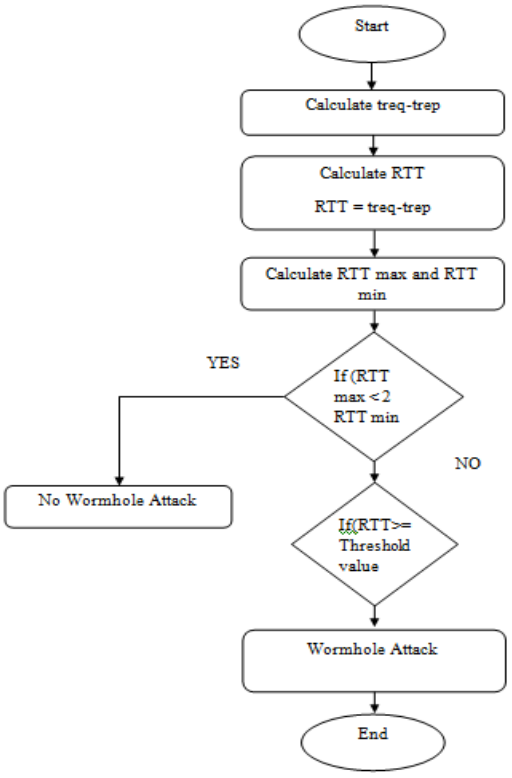

Fig.2. RTT (Round Trip Time) using AODV

IV. PATH TRACING APPORACH IN DSR

Dynamic Source Routing is also a reactive protocol. The key distinguishing feature of DSR is the use of source routing. The sender knows the complete hop-by-hop route destination. These routes are stored in route cache. It uses source routing in which source is responsible for providing information of whole path. Dynamic Source Routing protocol maintains two main mechanisms are Route Discovery and Route Maintenance. In Route discovery works by flooding the network with route request (RREQ) packets [11]. In Route Maintenance, a source puts the entire routing path in the data packet, and the packet is sent through the intermediate nodes specified in the path. DSR makes aggressive use of source routing and route caching.

In an ad-hoc network executing the DSR protocol, each packet contains the complete list of nodes that it has to traverse in order to reach the destination. This feature although excludes intermediate nodes form making any routing decisions can still be exploited to create a wormhole.

PATH TRACING (PT) ALGORITHM

Step 1: Nodes in a path computes RTT values based on the time between the RREQ sent and RREP received. The RTT computation is based on its own clock.

Step 2: Compute per hop distance value using RTT value. The computed per hop distance value and timestamp are stored in each packet header.

Step 3: These information are stored to identify the wormhole link. Each node in a path computes per hop distance with its neighbor and compares it with the prior per hop distance. If the per hop distance exceeds the maximum threshold range, RTh, go to step4.

Step 4: Check for the maximum count a link takes part in the path. If FAcount > FATh, then the link is wormhole.

Step 5: Mark the link as wormhole and the corresponding node informs other nodes to alert the network. These wormhole nodes are then isolated from the network.

This proposed algorithm involves two phases. All sending nodes compute per hop distance and time in first phase and in second phase all nodes detects the presence of wormhole using the information gathered in first phase[15].

Phase I

The source node floods the route request (RREQ) packets through nearest neighbors toward destination. When it reaches the destination, it sends back route reply (RREP) in the backward path. The node path details are stored in the DSR routing cache. In order to detect the wormhole to optimize the general DSR header by adding extra fields. Prior per hop distance field, per hop distance field and time-stamp fields are added to the header of each packet. Consider both prior per hop distance and per hop distance to compare the difference between the two distances. If the difference between prior per hop distance and per hop distance is too large that exceeds the maximum threshold value, then wormhole is detected. All nodes that participate in the routing process perform this operation. The time-stamp field is initialized to the time of the first bit of RREQ is sent. Per hop distance field can be changed by intermediary nodes but field cannot be altered by any other nodes. Every time an intermediary node obtains RREQ, it calculates per hop distance with its nearest neighbours and compares it with the prior per hop distance in the header value. After the comparison, it places per hop distance in the prior per hop distance field in the packet header and forwards RREQ to its neighbouring nodes. On obtaining RREQ, the receiver computes per hop distance with its neighbours in the backward path and it places in the packet header. Each intermediate node forwards one RREP for each RREQ. Every RREP holds the per hop distance of all

path in which it is related. In addition to per hop distance value, it also holds the timestamp of the time when taken between sending and receiving the RREQ and RREP correspondingly between two nodes. The computation of per hop distance of each node is explained in the next section.

A. Per Hop Distance Calculation

The presence of wormhole can be detected by calculating the distance between each hop in a path. We consider round trip time (RTT) value to calculate the per hop distance. RTT is defined as RREQ and RREP propagation time between the source and destination. Let us consider the RTT calculation between two nodes A and B where both the nodes are non wormhole nodes.

Variables used in RTT calculation:

Trep: Time when the first bit of RREP is received from B.

Treq: Time when the last bit of RREQ is broadcasted to A.

IPD: Intra nodal processing delay.

The Round Trip Time (RTT) between two nodes are calculated by using the estimated value of per hop distance between A and B. DAB is calculated assuming that routing signals travel with the speed of light "n". DAB =RTT= Trep – Treq – IPD. The node verifies whether B resides within its maximum acceptable transmission range RTT. The value of RTT is in the order of micro seconds and transmission range is in the order of a meter. In the same way per hop space between node B and node C, DBC is calculated where A, B, and C are consecutive neighbors of a path. The node C considers DAB as the prior per hop distance and compares with DBC. If the difference between DAB and DBC is larger than the maximum threshold range, RTh then the link with higher per hop distance is said to be wormhole. DBC - DAB > RTh The calculation of per hop distance is performed during the route discovery process in order to reduce the routing overload [15]. Every node must perform the per hop distance calculation using RTT value and store the estimated per hop distance value in packet header. The wormhole can be detected using the information in the packet header.

B. Analysis of Frequent Appearance of a Link

In order to detect the wormhole attack effectively, a link can be checked whether it participates in the routing very often. We can find frequent appearance (FAcount) of a link (Lj) in a path by using the formula, FAcount = Maximum number of times that Lj participates in a path/Total number of available links in a path = Nj/N. As there are many links in a path, it can also be used to detect wormhole attacks. If a link in a path frequently takes place in routing such that its count exceeds the frequent appearance threshold (FATh), then it is a wormhole link. The frequent appearance count information is gathered only through the monitoring and marked in cache. This method is easy to implement with reduced overhead and requirements and does not rely on tight time synchronization. Each node must calculate RTT only using its own clock.

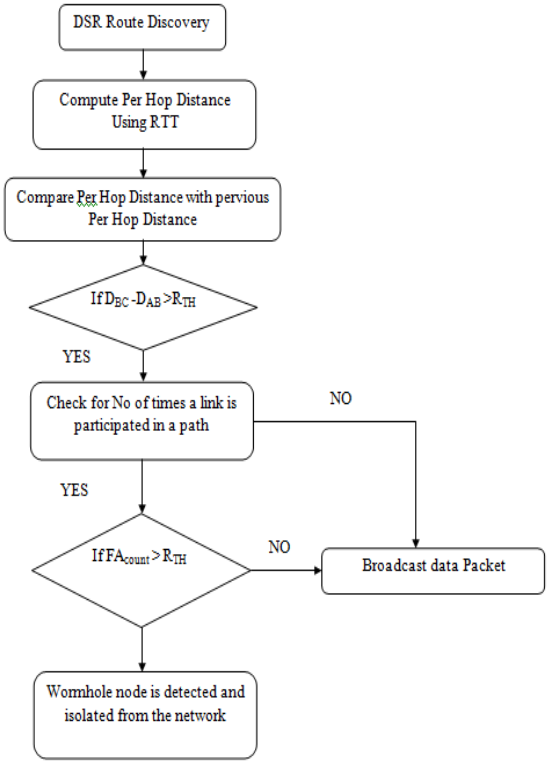

Fig.3. Path Tracing in DSR

Phase II

Each node in the network has to perform four major operations to detect the wormhole attack. Compute per hop distance and compare it with the prior per hop distance. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value. If it is larger, then the wormhole is detected and it is informed to all other nodes in the networks to provide wormhole alertness. For the confirmation of wormhole attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.

If DBC - DAB > RTh and Facount > FATh then it is a wormhole link. Per hop distance is calculated at the time of route discovery to make our method energy efficient. Many routes are discovered from the route discovery process. All nodes in each path calculate per hop distance and stores in the packet header. By analyzing the per hop distance between all nodes in a path, a wormhole can be detected. If the per hop distance exceeds the prior per hop distance through a maximum threshold range R_{th}, then the path related to that particular node is wormhole. For the effective wormhole detection, we take another parameter called frequent appearance count of a link in the path. If FAcount > FATh then it is a wormhole link. After the detection of

the wormhole, a node intimates the presence of wormhole to other nodes in the network. To prevent the wormhole node participation further, their identities are added to the wormhole list in each node. It is not necessary to compute per hop distance each time when a path is observed. This method extracts the computation energy by storing the estimated per hop distance in a cache.

V. SIMULATION BASED ANALYSIS

This section describes the simulation tool, parameters and simulation results. The performance of AODV and DSR routing protocols are evaluated on the basis of few performance metrics like packet delivery ratio, routing overhead and end-to-end delay. Simulations were conducted with the presence of wormhole attack. Threshold Algorithms namely Round Trip Time and Path Tracing were used. Different mobility scenarios were created by the model random way point.

A. Simulation Tool

In this paper, the simulation of AODV and DSR routing protocols and Threshold Algorithms with Wormhole Attack is done by using Network Simulator (NS-2) software due to its simplicity and availability. The NS instructions can be used to define the topology structure of the network and the motion of the nodes, to configure the service source and the receiver and to create the statistical data track file [9].

B. Simulation Parameters

TABLE I. SIMULATION PARAMETER

SIMULATOR	NS-2
NUMBER OF NODES	50
ROUTING PROTOCOL	AODV,DSR
SIMULATION TIME	50s
SIMULATION AREA	1000 x 1000m^2
NODE SPEED	10 m/s to 50 m/s
PACKET SIZE	512 bytes

C. Simulation Results

The figure 4 shows the impact of changing the speed, with which nodes move in an ad hoc network on the packet delivery ratio. Packet delivery ratio increases with increase in average node speed in RTT approximately 90% which remains almost same for all node speed. The Path Tracing shows a increase of 30% in delivery ratio when the average node speed increases from 10m/s to 50m/s.

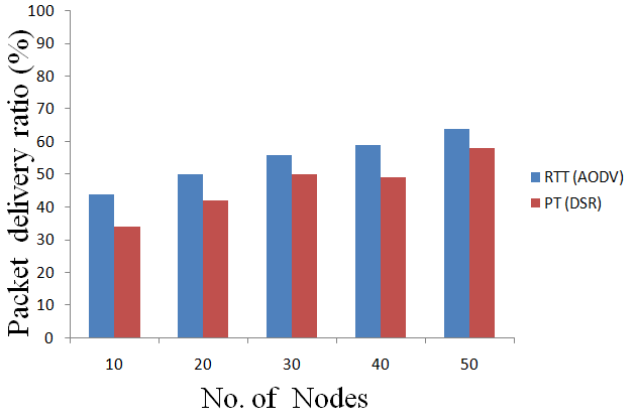

Fig.4.Packet Delivery Ratio of RTT and PT with wormhole attack

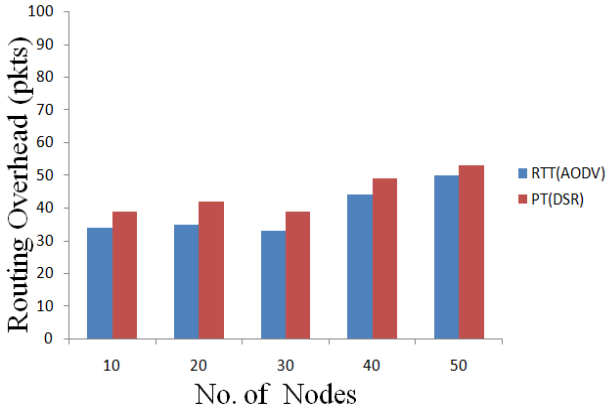

Fig.5. Routing Overhead of RTT and PT with wormhole attack

In Figure 5, effect of number of nodes on the average routing overhead is shown. Graph shows that routing overhead of RTT is less than PT in the presence of wormhole attack. From the overall observation of AODV and DSR routing protocols under wormhole attack, it is observed that DSR has lower performance in the presence of wormhole than AODV in high node density network because of additional routing overhead.

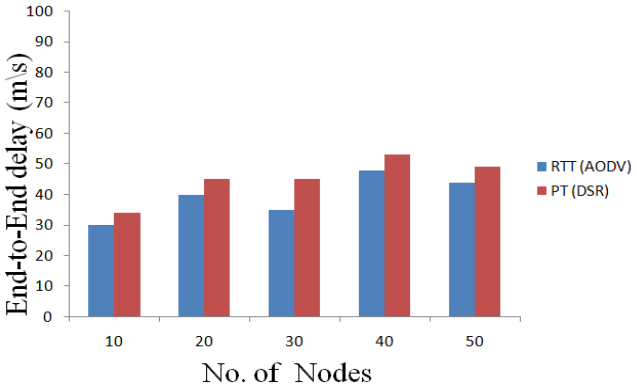

Fig.6.End-to-end delay of RTT and PT with wormhole attack

VI. CONCLUSION

In this paper, performance analysis of wormhole attacks under different scenarios taking threshold based Algorithms are simulated under NS2. Different performance metrics like Packet Delivery Ratio, Routing Overhead and Delay are used for analysis. Simulation results are based on AODV and DSR routing protocol by varying the number of nodes simultaneously. It can be concluded that AODV performs well than that of DSR. RTT calculation shows best results in packet delivery ratio, routing overhead and end-to-end delay than path tracing approach.

REFERENCES

[1] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), **pp. 1-7**, **2008**.

[2] Dipali Koshti," Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, **2011.**

[3] S.Archana, Dr.G.Kalpana, " A Survey on Security Attacks in Mobile Ad Hoc Network", National Conference on INNOVATIVE TRENDS IN INFORMATION TECHNOLOGY(NCITIT) ISBN:978-93-84743-32-1,7 FEB-**2015**

[4] Chattopadhyay, Mekhala. AN APPROACH TO DETECT WORMHOLE ATTACK IN AODV BASED MANET. Diss. Jadavpur University Kolkata-700032 India **2014.**

[5] S.Archana, Dr.G.Kalpana, "A Comparative Analysis of AODV and DSR Protocol under Wormhole Attack in MANET", International Conference on Innovation Information and Embedded and Communication System, March-**2015**

[6] Perkins CE, Royer EM, Chakeres "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF , October, **2003.**

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (**4**): Issue **(3) 265**, **2010**.

[8] F. Nait-Abdesselam, B. Bensaou, T. Taleb. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communications Magazine, 46 (4), **pp. 127 - 133**, **2008.**

[9] Network Simulator 2. http://isi. edu/nsnam/ns/

[10] Saurabh Upadhyay and Aruna Bajpai, Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, International Journal on Cryptography and Information Security(IJCIS),Vol.**2**, No.1,March **2012.**

[11] K.Santhi and Dr.M.Punithavalli "Optimized Reliable And Load Balanced Routing Protocol For Mobile Ad Hoc Networks" -Journal of Theoretical and Applied Information Technology (JATIT))-Vol.**51** No.**3** May **2013**

[12] Reshmi Maulik and Nabendu Chaki, "*A Study on Wormhole Attacks in MANET"*, International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988 Volume **3** (**2011**) pp. **271-279.**

[13] Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs", 978-1-61284-307-0/11, IEEE**, 2011**.

[14] Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile adhoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, **2010 pp 1793-8201**.

[15] R. Vembu, R. Syed Hayath, " Methodology For Comparing Reactive Routing Protocols To Detect And Prevent The Wormhole Attack Using Path Tracing Approach" IOSR Journal of Electronics and Communication Engineering(IOSR-JECE) e-ISSN: 2278-2834, p-ISSN: 2278-8735 PP **12-17.**

AUTHORS PROFILE

Dr.Kalpana.G received her MCA and M Phil degree in computer science from Bharathiar University, India in 2001 and 2004 respectively. She has received her doctorate in Computer Science from Anna University, India in the year 2014. Currently, she is an Associate Professor in the Department of Computer Science, Sri Ramakrishna College of Arts and Science for women. Her research interests are in the area of networking, MANET.

Archana.S received the M.Sc.Computer Science degree from Bharathiar University, India in 2014 . She is pursuing her Master of Philosophy (M.Phil.) in Computer Science (Full Time) at Sri Ramakrishna College of Arts and Science for Women, Bharathiar University , India. Her research area of Networking, MANET.