Elimination of Wormhole Attacks in Ad-Hoc Networks using DSR Protocol with Detection Packet

Manish kumar[1], Prof. S. R. Yadav[2]

[1]PG Scholar,MITS, Bhopal (India), [2]Head P.G., CSE,MITS, Bhopal (India)

Abstract - The improving reputation and custom of wireless expertise is creating a call for more safe and sound wireless networks. In MANET, data communication is performed within an un-trusted wireless background. A many types of attack have been recognized and comparable solutions have been considered. In wormhole attack, an aggressor record package at one site into the network, sequence them to another site and retransmits them there into the set of connections. Existing works on wormhole attacks have listening carefully only on recognition and used particular hardware such as directional antennas or tremendously precise clocks. More fresh task has dissimilarity of jump distance at station, generate information with two areas handing out bit, count to arrive at next hop and AODV for path establishment, public key encryption technique are also used. In this paper, explain a normal system, without use of hardware, site information and time harmonization called detection packet for detecting infected system in network. Detection Packet has three areas: dispensation bit, count to reach next hop and time stamp. Timestamp is used for powerfully finding with conformance at wormhole harass. Here finding packet can easily be included in the wide variety of ad hoc routing strategy with only considerable alter in the previous protocol to protect against wormhole attack. Here DSR technique is use for path establishment and NS2 for simulations.

Keywords - Wireless Ad-Hoc Network, Wormhole Attack, Tunnel, Performance Analysis, Routing Protocol, MANET Security.

1. INTRODUCTION

The improving reputation and usage of wireless expertise is implementing a need for extra secure wireless ad hoc networks. Wireless internetworks are perfectly susceptible to a more powerful assault known as the wormhole attack. This thesis researched and developed a new method that detect and secure prevent wormhole attacks on a wireless ad hoc network environment. A few predefined technique searches wormhole attacks but they accept extremely specialized equipments. This paper objective to implements a resistance alongside wormhole attacks while does not want as a important quantity of particular equipment. In this original method, new packet is implemented with new field and result is gain with conformance. Means we get double security for uncovering of wormhole attacks in a wireless ad hoc network. The analysis of this thesis results is here expensive insight for new methods in treatment wormhole attacks in the area of wireless protection.

2. SYSTEM MODEL

Ad hoc network has significant features that make it not only differentiate from characteristic wired network, but also horizontal to more security threats. The premise of shaping an ad hoc environment is to support wireless transmission among heterogeneous devices, anytime and anywhere, with as minimum as or no infrastructure. Security of ad hoc environment is question due to its unique features such as transportation less network, wireless communication, dynamic topology, and not have of own-stabilization belongings. External vulnerabilities such as eavesdropping and self-motivated network and interior constraints such as limited desirable computational and storage limited capabilities pose challenges in implementing a protected ad hoc network. Therefore, basic security necessities of MANET are accessibility, validation, veracity, confidentiality, permission, and trust management.

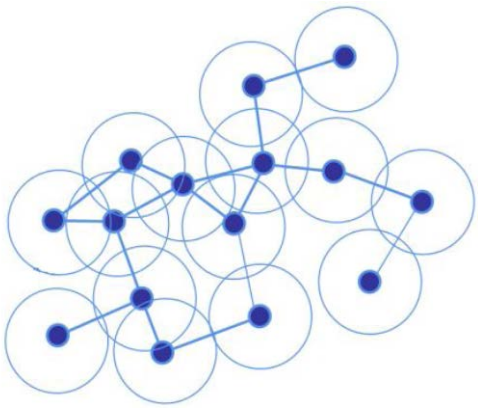

Figure 1.1: Basic Representation of an Ad-Hoc Network

2.1 Types of MANET:

(1) Vehicular Ad hoc Networks (VANETs) are used for transmission among different vehicles and between vehicles and roadside apparatus.

(2) Internet based Mobile Ad Hoc Networks (iMANET) are ad hoc environment that communicate mobile stations and fixed Internet-gateway points.

2.2 MANET Features:

Infrastructure Least: Unlike manual networks there is no pre-uploaded layout in ad hoc environment. The stations themselves are take care for where and when to be placed. Mobile points in straight radio series of one additional can transmitted directly.

Natural Changes in Network Topology: Ad-hoc network consist points that may subsequently change their positions. Therefore, the topology in these communications scenario is more highly dynamic. As a result traditional security mechanism and routing protocols can't be used in such an environment. This mandates the more dynamic model that can handle the demand of the situation.

Effects of Wireless Transmission: As the transmission is through wireless medium, it is possible for any intruder to trap the communication easily. An intruder such as an impersonator can collapse the entire network pretending any node of the network.

Lack of Own Stabilization Property: Routing protocols should be capable to improve from molest in finite time. An impostor or intruder should not be capable to enduringly disable a network by injecting a smaller number of mal-informed routing information.

Multicast Routing: Implementing of multicast routing strategy for a fixed changing MANET workplace. Quality of Service (QoS): Supporting fixed QoS for multiple multimedia issues in frequently changing network places.

Internetworking: Communication between wired network and MANET while maintaining harmony.

Power Consumption: The necessary conservation of powers and discovery of power save routing protocol.

2.3 The Wormhole Attack

Definition: Basically, Wormhole attack is most frightening and dangerous attacks. A wormhole attack is usually applied by pair of malicious point. Two infected nodes at multiple workplace sending-receiving routing information to one-other via a specified tunnel. Wormhole points can successfully implement such type of attacks without compromising any station and are inevitable. Then MANETs support authenticity and privacy protection. There are two types of wormhole attacks have been discussed in the literature: wrapped wormhole intrusion attack and exposed wormhole harass. In wrapped wormhole attack, this attack can be simply mounted and without compromising any node in the network environment and in exposed wormhole attack, in which two end nodes are two compromised stations. But our concentration will focus on hidden wormhole attack. In figure 1.2, the destination station D notice that a information packet from the source station S is moved under wrapped wormhole attack, while it trusts that the information packet is delivered via station S, M1, M2, D under wrapped wormhole attack.

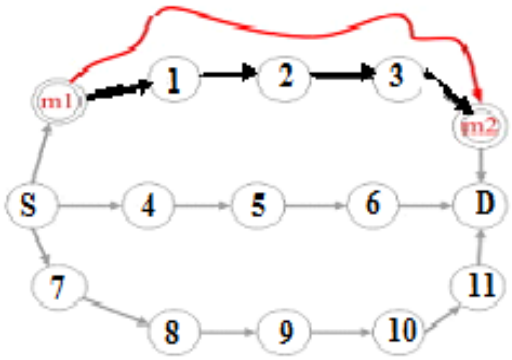

Figure 1.2: Wormhole Attack

2.4 Wormhole Attack on OSI Layer

Wormhole is attack on network protocol of the OSI layer model, because network layer protocol has routing and congestion method. Therefore, wormhole is attack on route between source and destination nodes.

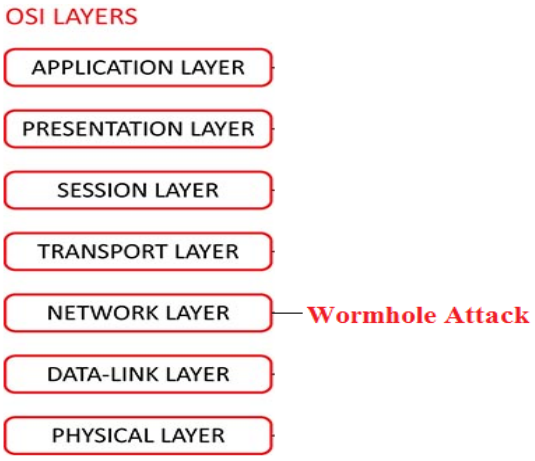

Figure 1.3: Wormhole Attack on OSI Layer

2.5 Wormhole Creation

implemented through the following three different ways:

• In any ad-hoc network model, a wormhole attack can be Sequencing of above the network layer in OSI model.

• Order implement via internal hidden infrastructure.

• Order implement via external wired infrastructure.

3. PREVIOUS WORK

The previous researches can be broadly classified into three categories.

3.1. Routing Protocol Based

The initial is to develop a well-known routing strategy, like as Ad hoc On demand Distance Vector or Dynamic Source Routing (DSR) [1], to avoid wormhole stations during path discovery, such as (Song et al., 2005 [3]; Chiu and Lui, 2006 [4]; Lee et al., 2008 [5]; Su and Boppana, 2007 [6]; Naıt-Abdesselam et al., 2007 [7]; MHA, 2011 [8]; PT, 2012 [11]; WARP, 2010 [12].

3.2. Extra Hardware Based

The second is to accept added hardware, like as a positioning scheme, a time harmonization technique or a directed aerial, in addition to updating the routing strategy. Some of these are (Khallil et al**.,** 2005 [8], 2006 [9]; Wang and Wong, 2007 [10]; packet leashes, 2003 [10]; Hu et al., 2006 [11].

3.3. Intrusion Detection System (IDS) Based

The third is to upload an intrusion detection system with or without hardware provide, such as (Gorlatova et al. [7], 2006; Azer et al., 2008 [8]; Wang, 2006 [10]; Phuong et al., 2007 [9]). Saurabh, Subrat and Dharamraj [11] introduced "WHOP: Wormhole Attack Detection Protocol using Hound Packet". WHOP is accepts the help of others stations after the way has been found wormhole in the network protocol.

4. PROPOSED METHODOLOGY

The working principal of our proposed method is explained as below:

(1) One RREQ is build by source station and broadcast it to all adjacent stations which are in its transmission array.

(2) RREQ is re-wise broadcasted by all recipient stations of RREQ until received by destination station.

(3) The source stations of RREQ eavesdrop to the rebroadcast from all its adjacent nodes, before removing such RREQ they keep testimony of their ID as next adjacent stations. All normal stations in MANETs get catalog of information as specified in the network.

(4) If receiving station of RREQ is infected, its rebroadcast is not listened by adjacent stations because it unicast RREQ to its malicious partner using out-band control, thus all its adjacent neighbors will not listen to from it and they will be not capable to record their ID.

(5) Basically RREQ is reached to recipient node through way having infected station due less count of nodes as compared to other available normal routes.

(6) The RREP information packet is created by destination station and unicast through the reverse way.

(7) The accepting node of RREP on reverse path will verify if there exists an ID of the sending station of RREP in its maintaining information, if yes it will forward the RREP to next node on reverse path towards the source point, otherwise, the recipient station regards that point as infected and is isolated and future transmission via that node is blocked.

(8) Another alternative way having no infected station is then selected for data transmission.

5. SIMULATION/EXPERIMENTAL RESULTS

Three experiments have performed to verify the effectiveness of the method. These experiments are giving below:

5.1 Packet Delivery Ratio in 50 Nodes

Mathematically, PDR is the proportion of total amount of packets reached the recipient and quantity of packet sent by the initial node. If the value of infected station increases, PDR also decreases manually. The maximum mobility of stations causes packet delivery ratio to decrease.

$$\text{PDR} = \frac{\text{Total amount of data packet received (Receiver)}}{\text{Total amount of packet sent (Source)}}$$

Attack minimizes the average Packet Delivery Ratio (shown in Red) from normal situation (shown in Blue) and the

proposed technique significantly improves the Packet Delivery Ratio by neglecting the attacker (shown in green).

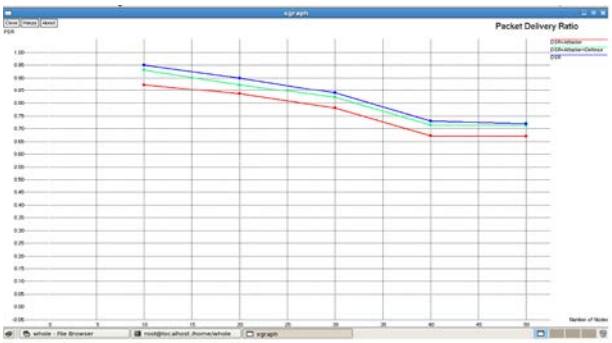

Figure 1.4: Average Packet Delivery Ratio per Route Comparison

Figure 1.4 explains the confidence of the packet delivery ratio on the number of stations in action. All way minimize with improving the count of stations in the network layer. But protection route are improve, which is compare than attacker route.

Table 1: Values of Selected Node on per Route in Packet Delivery Ratio

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	**0.97**	**0.92**	**0.944**
20	**0.91**	**0.847**	**0.896**
30	**0.86**	**0.776**	**0.883**
40	**0.78**	**0.699**	**0.747**
50	**0.75**	**0.668**	**0.716**

In table 1, some selected analysis node (10, 20, 30, 40 and 50) outcomes are available from simulation with three ways. First way is normal route as DSR without infected station in blue color. Second way is attacker route (DSR + Attacker) with infected station in red color. Third way is defense route (DSR + Attacker + Defense) where infected stations are isolated in green color.

Figure 1.5 shows that the packet delivery ratio of three distinguish path as DSR, Attacker on DSR and Defense approach on Attacker based DSR. In above graph X-axis describes the station and Y-axis describes the packet delivery ratio. Here we compare three different routes for Packet Delivery Ratio with the proposed technique. When infected station occurrence is 0 then this technique give a perfect packet delivery ratio. Normal path (blue) is evaluates 72% packet delivery ratio at station 50 in minimizing order. When infected station are present in this normal route then it is called attacker route (red) is providing 64.7% information delivery ratio at node 50 in minimizing order and when infected station are isolated then it is known as defense route (green) is providing 72.5% information delivery ratio at node 50 in minimization order but defense route are improve and provide much better packet delivery ratio judge against attacker route.

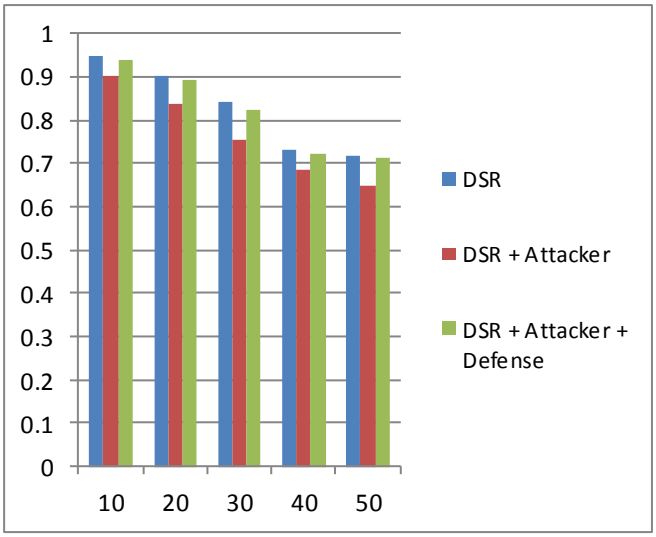

Figure 1.5: Average Packet Delivery Ratio per Route Comparison in Column Chart

5.2 Throughput in 50 Nodes

Attack decreases the average Throughput (Red) from normal situation (Blue) and proposed technique considerably regains the Throughput by neglecting the assailant (green).

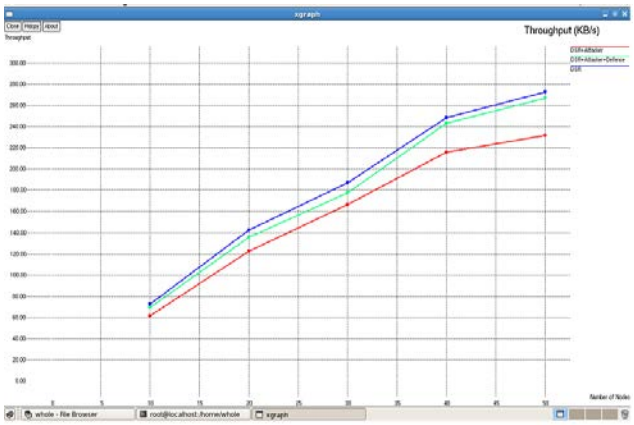

Figure 1.6: Average Throughput per path Comparison

Figure 1.6 explains the reliance of Throughput on the count of stations in deed. All routes improve with enhancing the number of stations in the set of connections and protection route are also improve contrast than attacker route. Here per station transmission is improve, therefore path is obtainable in incrementing sequence. If we are create steady traffic then all paths is obtainable in reducing sequence.

Table 2: Values of Selected station on per path in Throughput

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	**72.47**	**62.917**	**70.914**
20	**142.26**	**122.521**	**138.219**
30	**186.26**	**162.215**	**177.213**
40	**248.06**	**223.104**	**235.135**
50	**272.29**	**239.132**	**261.027**

Here in table 2, some selected analysis node (10, 20, 30, 40 and 50) results are available from the simulation with three paths. Initially path is usual path (DSR) without spiteful station in blue color. Second path is aggressor path (DSR + Attacker) with spiteful station in red color. Third path is protection path (DSR + Attacker + Defense) where spiteful stations are remote in green color.

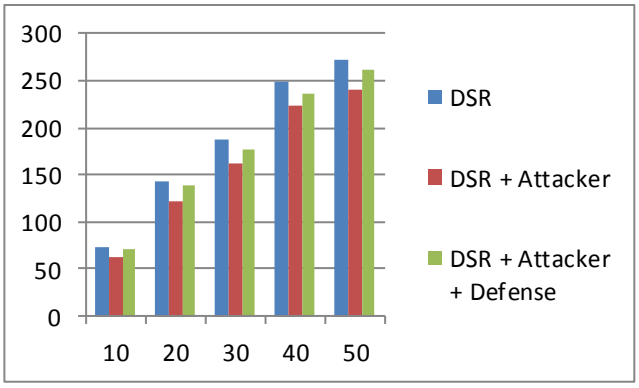

Figure 1.7: Average Throughput per path Comparison in Column Chart

Figure 1.7 describes the Throughput of three multiple paths as DSR, Attacker on DSR and Defense technique on Attack based DSR. In that X-axis describes the station and Y-axis describes the Throughput. Here we evaluate three paths for Throughput through the proposed technique. When infected station happening is 0 then this approach give increase Throughput. Usual path (blue) is supporting 272 kbps Throughput at station 50 in increasing sequence. When spiteful station are happen in this usual path then it is known as attacker route (red) is supporting 239.27 kbps Throughput at station 50 in increasing sequence and when spiteful station are isolated then it is known defense route (green) is supporting 261.13 kbps Throughput at station 50 in increasing sequence But defense route are improve and supporting increase Throughput evaluate than aggressor route.

5.3 End to End Delay in 50 Nodes

The average delay is the elapsed duration between information sent and received. Attacks improve the End to End delay (Red) from general situation (Blue) and proposed technique considerably reduces the End to End delay by neglecting the attacker (green).

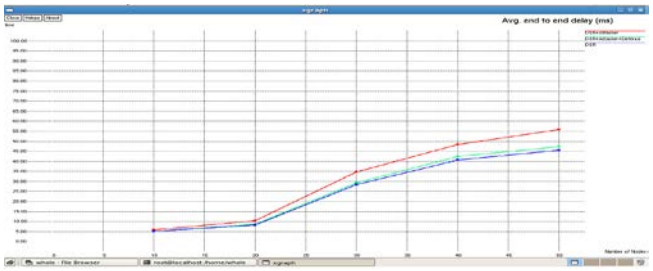

Figure 1.8: Average End to End Delay per path Comparison

Figure 1.8 shows that the dependence of End to End Delay on number of stations in feat. All routes improve with increasing the number of stations in the set of connection but protection route are reduce compare than attacker route for decrease the delay.

Table 3: Values of Selected Node on per path in End to End delay

Node	*DSR*	*DSR + Attacker*	*DSR + Attacker + Defense*
10	**5.126**	**6.192**	**5.317**
20	**8.113**	**10.231**	**8.263**
30	**28.412**	**34.217**	**29.913**
40	**40.262**	**50.362**	**41.612**
50	**45.527**	**56.416**	**46.825**

In above table 3, some selected analysis station (10, 20, 30, 40 and 50) outcomes are available from the implementation with three paths. First path is usual route (DSR) without spiteful station in blue color. Second path is attacker route

(DSR + Attacker) with infected station in red color. Third path is protection route (DSR + Attacker + Defense) where infected stations are isolated in green color.

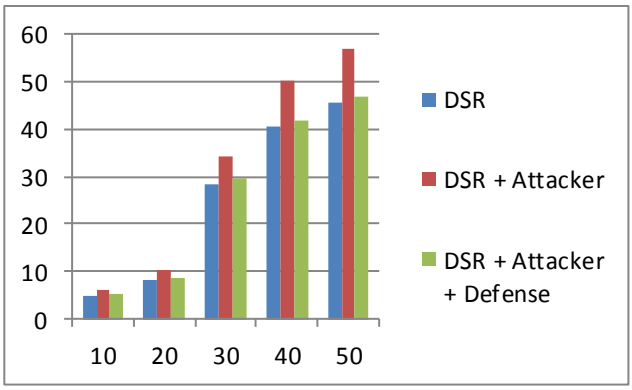

Figure 1.9: Average End to End Delay per route Comparison in Column Chart

Figure 1.9 describes the End to End Delay of three multiple paths as DSR, Attacker with DSR and Defense mechanism with Attack based DSR. In X-axis, represents the station and Y-axis represents the End to End Delay. Here we evaluate three ways for End to End Delay with the proposed technique. When infected station occurrence is 0 then this technique give minimize End to End Delay. General route (blue) is supporting 44.5% End to End Delay at station 50 in increasing sequence. When infected station are exist in this usual route then it is known as aggressor route (red) is supporting 55.6% End to End Delay at station 50 in increasing sequence and when infected station are remotely situated then it is known as protection route (green) is supporting 46.2% packet delivery ratio at station 50 in increasing sequence but protection route are minimize and supporting minimize delay compare than aggressor route.

6. CONCLUSION

There are many research area efforts to short out routing attack in wireless ad hoc networks through security consideration, service such as authentication, encryption, extra hardware sustain etc. Hence increase the time and cost of the system in existing work. In this work we present a method of recognition packet which is based on DSR [2] using implementations developed in Network Simulator 2 (NS-2)[3] to preserve beside wormhole attack in wireless ad hoc networks. In our work, wormhole attack is detected without make use of of any hardware, site information packet and clock synchronization**.** Hence reduces the time and cost of the system, recognize wormhole system and avoid them. Consequently increase Throughput, Packet Delivery Ratio (PDR) and decrease End to End Delay compare than wormhole attack route.

7.FUTURE SCOPES

In future work, we can use better and fast routing strategy for path establishment and use effective fields for detecting packet. We can enhance the table entries at recipient to get the detection of pair of malicious nodes faster and improve conformance procedure.

REFERENCES

[1] Johnson DB, Maltz DA, Hu YC. *"The dynamic source routing protocol for mobile ad-hoc network (DSR)"* July 2004.

[2] Perkins CE, Royer EM, Das SR. *"Ad hoc on-demand distance vector (AODV) routing"* IETF internet draft. MANET Working Group; Jan 2004.

[3] Ning Song, Lijun Qian, and Xiangfang Li. *"Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach"* In the proceedings of the 19th IEEE international parallel and distributed processing symposium (IPDPS'05); 2005.

[4] Hon Sun Chiu, King-Shan Lui. *"DelPHI: wormhole detection mechanism for ad hoc wireless networks"* In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.

[5] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, *"An approach to mitigate wormhole attack in wireless ad hoc networks"* In the proceedings of the international conference on information security and assurance; 2008.

[6] Xu Su and Rajendra V. Boppana. *"On mitigating in-band wormhole attacks in mobile ad hoc networks"* In the proceedings of the IEEE international conference on communications; 2007.

[7] Farid Naıt-Abdesselam, Brahim Bensaou, Jinkyu Yoo. *"Detecting and avoiding wormhole attacks in optimized link state routing protocol"* In the proceedings of the IEEE conference on wireless communications and networking; 2007.

[8] Issa Khalil, Saurabh Bagchi, Ness B. Shroff. *"LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wireless networks"* In the proceedings of the 2005 international conference on dependable systems and networks (DSN'05); 2005.

[9] Issa Khalil, Saurabh Bagchi,and Ness B. Shroff. *"MOBIWORP: mitigation of the wormhole attack in mobile*

multihop wireless networks" In the IEEE securecomm and workshops; 2006.

[10] Xia Wang and Johnny Wong, *"An end-to-end detection of wormhole attack in wireless ad-hoc networks"* In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007.

[11] Hu Yih-Chnu, Perrig Adrian, Jonhson David B. *"Wormhole attacks in wireless networks"* IEEE Journal on Selected Areas in Communication 2006.

[12] Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW. *"Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach"* In the proceedings of the IEEE conference on wireless communications and networking; 2005.

AUTHOR'S PROFILE

Manish Kumar has received his Bachelor of Engineering degree in Computer Science and Engineering from Millennium Institute of Technology and Science, Bhopal (India) in the year 2013. At present he is pursuing M.Tech. with the specialization of Computer Science and Engineering in Millennium Institute of Technology and Science, Bhopal (India). His area of interest is Computer networking, Cloud Computing, and Image Processing.

Prof. S. R. Yadav has received his Bachelor of Engineering in Computer Science and Engineering from G.I.E.T. Gunupur under B.U. Orissa in the year 2006. M.Tech. in Computer Science and Engineering From P.G. Department of Computer Science Engineering under B.U. Berhampur, Orissa in the year 2009. M.B.A. in HR From Academy of Management Bhopal under B.U. Bhopal, M.P. in the year 2014.He is a Ph.D. Scholar of Computer science and engineering PAHER Univ. Udaipur, Rajasthan, India. At present he is working as an Associate Professor at Millennium Institute of Technology and Science, Bhopal.(India). His areas of interests are Data Mining, Intrusion Detection System using Data Mining and Neural Networks.