International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 1043-1055
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

ANALYSIS OF MANET ROUTING PROTOCOL IN PRESENCE OF WORM-HOLE ATTACK USING ANOVA TOOL

Dr.B.A.S Roopa Devi[1], N. S. Kalyan Chakravarthy[2], Dr.M.N Faruk[3]
[1] Department of Computer Science& Engineering
[1]QIS College of Engineering and Technology, Ongole, India
[2]Research scholar,Acharaya Nagarjuna University,Guntur,India
[3]Department of Information Technology
[3]QIS College of Engineering and Technology, Ongole, India

Abstract: Wireless networks play a vital role as the wireless connectivity is needed by the users irrespective of their geographic position. Adhoc wireless networks are Infrastructure-less networks and utilize the multi-hop radio relaying.There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Attacks on adhoc networks is classified into two categories namely passive and active.There are many attacks pertaining to network layer of all the attacks,the worm hole attack is one of the security threat in which the attacker receiver the packets and tunnels them to a different location in the network,where the packets may be resent into the network.There is a need for security in MANETs for transmission and communication which is quite challenging.. The scope of this paper is to study the effects of Worm hole attack in MANET using reactive routing protocol (i.e)Adhoc on-demand Distance Vector Routing Protocol.The analysis of performance of MANET routing protocol in presence of worm hole attack is taken into account. The performance of the network is measured with respect to the metrics like throughput,jitter,packet delivery ratio,packets dropped by varying the number of nodes thereby considering the scalability.The impact of wormhole attack is analysed with the ANOVA tool.

Key Words:AODV,OLSR,Proactive,Reactive,Wormhole,MANET.

1. Introduction

Mobile Ad-Hoc Networks are independent and Infrastructureless networks in which the mobile nodes act both as a host /router or both at the same time. It is a category of wireless networks that utilizes multi-hop radio relaying and also is capable of operating without the need of any infrastructure. Wireless sensor networks and wireless mesh networks are examples of Adhoc wireless networks [1].These adhoc wireless networks are stationary in nature.If the adhoc wireless network is featured with mobility then it is said to be a Mobile Adhoc Network. The mobility of nodes is random by default. However different mobility patterns can also be embedded.The routing and resource management are in a disturbed manner in which all the nodes coordinate to enable communication among themselves. Hence the mobile nodes are more complex in adhoc wireless networks [2, 3].

The security of communication in Mobile Ad-Hoc Network is the most important concern for the basic functionality of the network [4]. The unique features of MANET are open medium, dynamic topology, lack of central coordinator, cooperative algorithm. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks [5, 6]. There are different kinds of attacksWorm hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack is kind of attacks that a MANET can suffer from

2. Related Works

MANET's are dynamic, infrastructure less, these networks are very much exposed to attacks. Wireless links also make the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [7, 8]. There are different kinds of attacks which have been analyzed in the MANET and also their effect on the network. Gray hole Attack is the attack where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior.The attackers are also exploiting MANETs routing protocols in the form of flooding attack, which is done by the attacker either by using RREQ packet or data flooding [9,10,11]. The sender wants the data to be sent as soon as possible in a secure and fast way in any network, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in a strong strategic location in the network [34]. They make the use of their location i.e. they have a shortest path between the nodes. One of the most important issues in MANET is limited battery.The attackers take advantage of this flaw and try to keep the nodes active until all its energy is lost and also the node goes into permanent sleep. There are many other attacks that are vulnerable such as jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been studied [12-18].In Worm hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table [28]. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and return it [29]. In a path based detection method, every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Worm hole attack.

Worm hole attack, one of the solution proposed by Deng gives the approach of disabling the reply message by the intermediate [30]. This method avoids the intermediate node to reply which avoid in certain case the Wormhole and implements the secure protocol. The solution proposed focus on the requirement of a source node to wait unless the arrival of the RREP packet from more than two nodes [31]. When it receives multiple RREPs the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of the node [32].

3. Routing protocols in MANETs

In MANETs, nodes are not familiar with the network topology in priori. Routing protocols are responsible in establishing the paths between the mobile nodes in order to transmit data between source and destination in that path. Hence a routing protocol must be efficient enough in handling various network phenomenon's and must tolerate against different security attacks [33]. These routing protocols are broadly classified into three types based on the phenomenon in which they broadcast information.

1. Proactive or Table-Driven routing protocols
2. Reactive or On-Demand routing protocols
3. Hybrid routing protocols

3.1 Ad-Hoc on Demand Distance Vector Protocol (AODV)

AODV is a reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV uses control messages to find a route to the destination node in the network.

a. Route Discovery Mechanism in AODV

When a node "A" wants to initiate transmission with another node "G" as shown in the Fig.3.1, it will generate a Route Request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbor, and those nodes forward the control message to their neighbor nodes. This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself [19]. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. Fig.3.1 depicts the exchange of control messages between a source node and destination node.

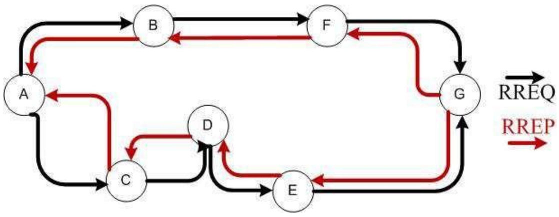

Fig.3.1 AODV Route Discovery

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbor nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node “A” to the neighbor nodes, at node “E” the link is broken between “E” and “G”, so a route error RERR message is generated at node “E” and transmitted to the source node informing the source node a route error, where “A” is source node and “G” is the destination node. The scheme is shown in the Fig.3.2 below.

b. Route Discovery Process

When a source node wants to start data transmission with another node in the network, it checks its routingcache. When there is no route available to the destination in its cache or a route is expired, it broadcasts a RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, the RREP is generated [20-23]. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

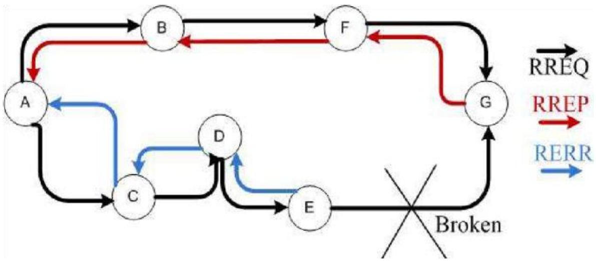

Fig.3.2AODV Route Error

c. Route Maintenance Process

When the transmission of data started, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The node generates a route error message, if it does not receive any confirmation to the originator node. The originating node again performs new route discovery process.

d. Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing (OLSR) protocol is described in RFC3626,which is a proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables.

e. Multi Point Relaying (MPR)

OLSR diffuses the network topology information by flooding the packets throughout the network. The flooding is done in such way that each node that received the packets retransmits the received packets [24-26]. These packets contain a sequence number so as to avoid loops. The receiver nodes register this sequence number making sure that the packet is retransmitted once. The basic concept of MPR is to reduce the duplication or loops of retransmissions of the packets.

Only MPR nodes broadcast route packets. The nodes within the network keep a list of MPR nodes. MPR nodes are selected within the vicinity of the source node. The selection of MPR is based on HELLO message sent between the neighbor nodes. The selection of MPR is such that, a path exists for each of its 2 hop neighbors through MPR node. Routes are established, once it is done with the source node that wants to initiate transmission can start sending data.

The whole process can be understood by looking into the Fig.3.3. The nodes shown in the figure are neighbors. "A" sends a HELLO message to the neighbor node "B". When node B receives this message, the link is asymmetric. The same is the case when B sends a HELLO message to A. When there is two way communications between both of the nodes we call the link as symmetric link. HELLO message has all the information about the neighbors. MPR node broadcast topology control (TC) message, along with link status information at a predetermined TC interval.

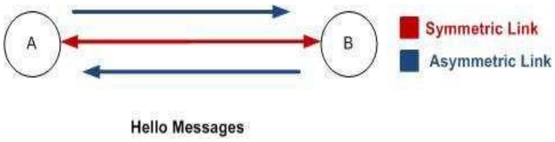

Fig.3.3 Hello Message Exchange

4. Attacks in MANET

The attacks are basically classified into two categories – Passive attacks and Active attacks. These are further sub-classified into various kinds depending upon the type of the attack such as Denial of Service attack, Fabrication attack, Modification attack, Replay attack and Impersonation attack. Passive attacks just listen to the traffic of the network to obtain vital information. These types of attacks do not affect the functioning of the network. It is difficult to identify such type of attacks as the performance of the network does not vary [27]. It is even not possible to detect the presence or the location of the attacker node in this case. The only way to prevent such type of attacks is through encryption. Whereas, active attacks aim to modify the transmitted data by adding random packets or attempt to interrupt the data flow from source to destination. The main purpose is to pull all packets towards the attacker for analysis or to obstruct the network communication. Black hole attack is one such attack which comes into this category. Among these two types of attacks, only active attacks can be accepted out at routing level. They can either be inner or outer. In order to combat these attacks, a secure environment should provide confidentiality, availability, authenticity, integrity and non-repudiation.

Wormhole attack is a kind of Denial of Service attack which misleads the routing operations even without the knowledge of the encryptions methods unlike other kinds of attacks that makes it very important to identify and also to defend against it.Wormhole attack is a severe type of attack on mobile adhoc network routing where two or more attackers are connected by high speed off-channel link called wormhole link.These wormhole attacks exists in two different modes, namely ‘hidden’ and ‘exposed’ mode, depending on whether attackers put their identity into packet headers when tunnelling and replaying packets.A pair of attackers forms ‘tunnels’ to transfer the data packets and replays them into the network. This attack affects the mobile adhoc network drastically, especially against routing protocols. The tunnel that exists between the two colluding attackers is referred as wormhole. Fig.4.1 shows the wormhole attack. Packets received by node X is replayed through node Y and vice versa.

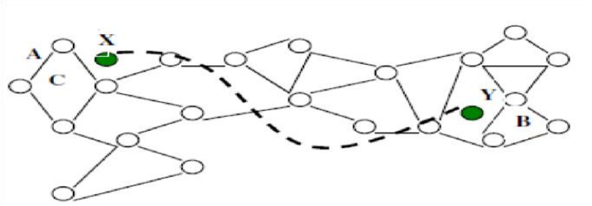

Fig. 4.1 Wormhole Attack

It takes number of hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network. The attacker can make A and B believe that they are neighbours by forwarding routing messages, and then selectively drop data messages to disrupt communication between A and B.

4.1 WORM-HOLE ATTACK IN AODV

Two types of Worm-hole attack can be described in AODV in order to distinguish the kind of Worm hole attack.

- Internal Worm hole attack
- External Worm hole attack

In an AODV Worm hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D”. The malicious node “A” then send the RREP which contains the spoofed destination address including small hop counts and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way the data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate with state of Worm hole attack**.**

5. Experimental Evaluation

This paper various performance metrics required for evaluation of protocols. To reiterate the Worm hole attack, we begin with the overview of performance metrics that includes Packets Dropped, Packet Delivery ratio, Number of Packets Forwarded, Number of Packets Received, Throughput. These matrices are important because of it performance analysis of network.

Figure employs the simulation setup of a single scenario comprising of 30 mobile nodes. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters.

Table 1. Simulator Parameters

Examined protocols	**AODV**
Simulation time	**200**
Simulation area	**1000 x 1000**
Number of Nodes	**50,60,70,80,90**
Traffic Type	**TCP**
Performance Parameter	**Throughput, Jitter,Packet Delivery Ratio,Packets Dropped**
Wireless MAC	**802.11**
Data Rate	**11 Mbps**

Furthermore, the simulation parameters are given in Table I. The Fig. 5.1 was building of normal working MANET with the normal behavior of nodes without any type of attack introduced to it (Without Attack) i.e. no malicious node introduced yet. This will lead us to observe and measure the effect of the network when there is attack carried on (With Attack) i.e. introduction of malicious nodes. In case of wormhole attack two malicious nodes are introduced in the whole network. After simulation of the scenario the graphs are analyzed in comparison with normal working protocols of AODV (without attack). The malicious node is placed in the network. This malicious node when receive any sort of packets discards out all the received data. Now in simulation we implemented the single malicious node in both AODV protocols. This paper focuses on result and its analysis based on the simulation performed in NS-2.35

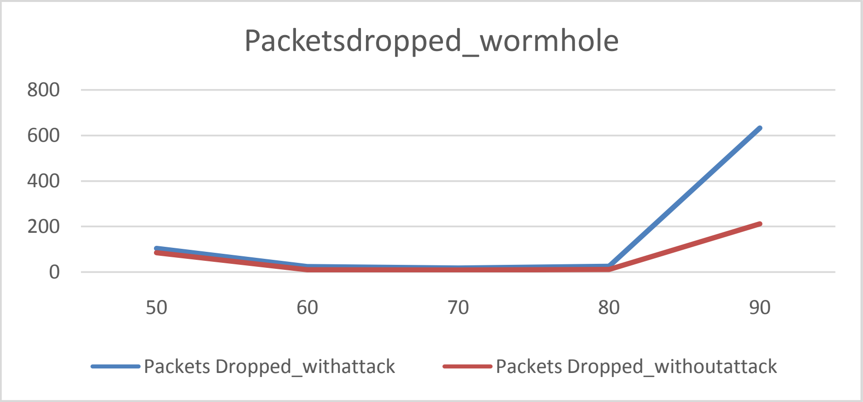

Fig. 5.1. Packet Dropped

The effect of wormhole attack on the parameter Packets dropped is prominent when the number of nodes are increased the packets dropped are also high which indicates that the impact of attack.

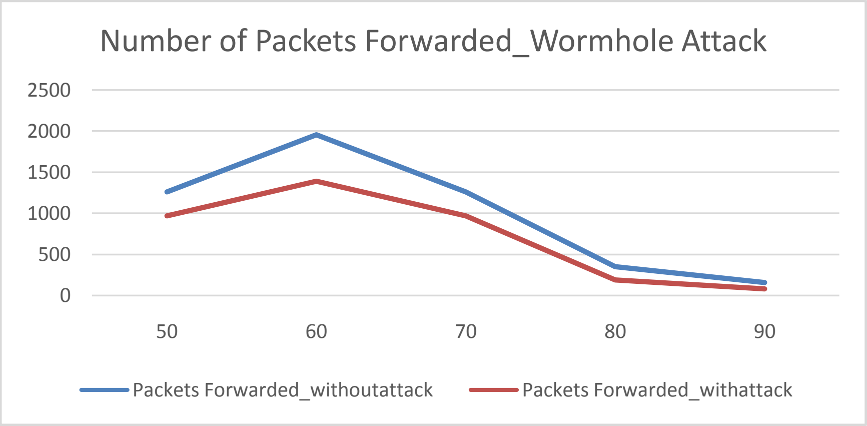

Fig. 5.2. Number of Packets Forwarded

In Fig.5.2., the Packets forwarded are also relatively less when the number of nodes are increased from 50 to 90which indicated that the malicious node does not forward packets to the next node rather tunnels it in the network creating havoc.

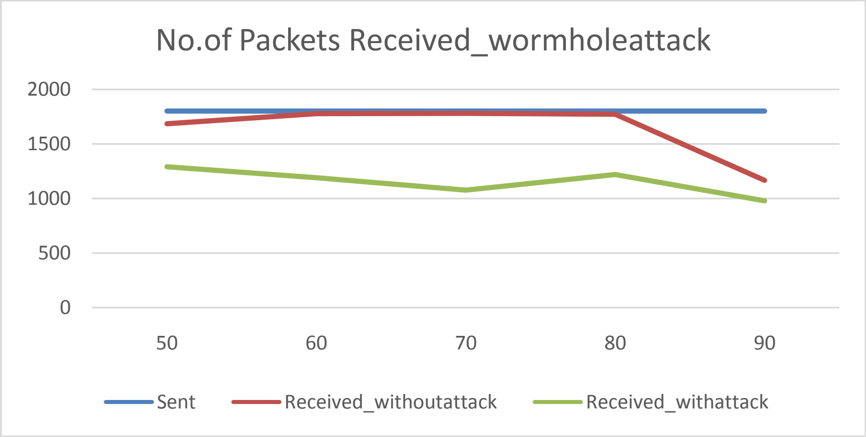

Fig. 5.3. Number of Packets Received

In Fig. 5.3. the Number of packets received when there is attack is very less compared to packets received when there is no attack. The analysis has been conducted in different scenarios where the pause time has been varied from 0 to 5 m/s and the results indicate that the impact of wormhole attack is vital even when the number of nodes are varied from 50 to 90.

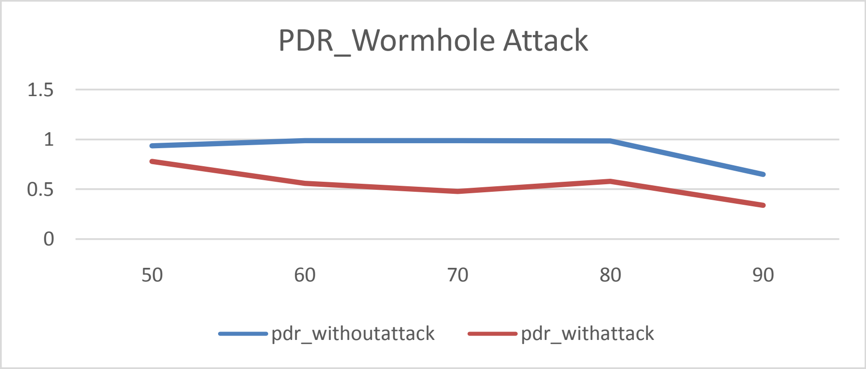

Fig. 5.4. PRD

The packet delivery ratio for different scenarios varying the number of nodes and also the pause time as well as the mobility speed has been considered. It is the ratio between the number of packets sent to packets received. The Fig.5.5 clearly depicts the effect of the wormhole attack on the metric packet delivery ratio. It is very less when compared to the scenario where there is no attack

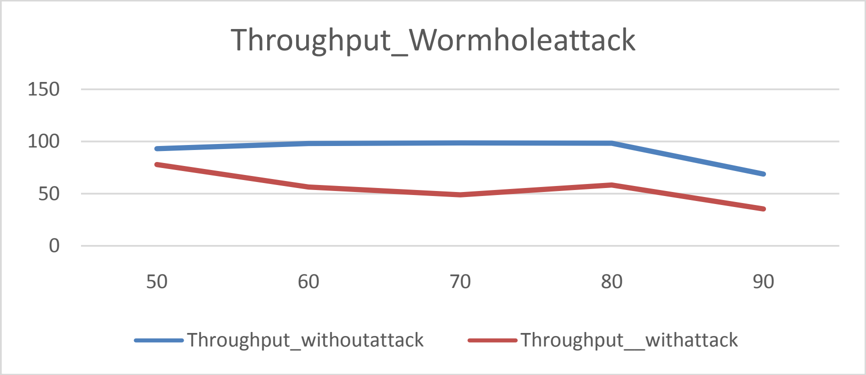

Fig. 5.5. Throughput

6. Conclusion

The analysis of this paper is that Worm Hole attack with different scenarios with respect to the parameters like Packets Dropped, Packet Delivery ratio, Number of Packets Forwarded, Number of Packets Received, Throughput. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of AODV protocol has a more severe effect when there is a higher number of nodes and in presence of wormhole. The throughput of AODV is affected when there is wormhole attack. In case of Packets Dropped however, there is an effect on AODV by the malicious node

References

[1]. B Satya Sravani, T Jagadeepak, B.A.S. Roopa Devi, B. Prabhakara Rao,Examining the performance of AODV routing protocol under black hole attack with varied node densities and mobilities,International Journal of Research in Engineering and Technology, 10, 03(2014),143-150.

[2]. B.A.S. Roopa Devi, JVR Murthy, G Narasimha, Comparative study of Routing Protocols in Mobile adhoc Networks using QualNet, International Journal of Engineering Sciences and Emerging Technologies, V6.1(2013) ,94-101.

[3]. C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network,24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[4]. Y.F.Alem, Z.C.Xuan, Preventing Worm hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection,2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[5]. Rongali Avataram, Dr B Prabhakara Rao, B.A.S. Roopa Devi, AHybrid Routing Mechanism for Fast and Secure Data Transmission in MANET, International Journal of Advanced Research in Computer and Communication Engineering,02(2013), 3058-3063.

[6]. C.E.Perkins and E.M.Royer, Ad-Hoc on Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[7]. Z.J.Hass, M.R.Pearlman, P.Samar, The Zone Routing Protocol (ZRP) for Ad Hoc Networks, 55th Proceeding of International task force, July, 2002.

[8]. Reddy Hyndavi, B Prabhakara Rao, B.A.S. Roopa Devi, An Improved technology to increase the delivery ratio using Position based Opportunistic Petal Routing Protocol (POPR) in MANET, International Journal of Advanced and Innovative Research, 03(2013), 156-161.

[9]. M.Parsons, P.Ebinger, Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks, [Online]. Available: www.cse.buffalo.edu/srds2009/dncms2009_submission_ person.pdf [Accessed: April. 10, 2010].

[10]. D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks”, International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[11]. B Satya Sravani, T Jagadeepak, B.A.S. Roopa Devi, B Prabhakara Rao, Examining the performance of AODV routing protocol under black hole attack with varied node densities and mobilities,International Journal of Research in Engineering and Technology,03(2014), 143-150.

[12]. C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, A New Solution for Resisting Gray Hole Attack in Mobile AdHoc Networks, Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[13]. S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265

[14]. T Jagadeepak, B Prabhakara Rao, BAS Roopa Devi,Investigating the performance of routing protocols using quantitative metrics in mobile ad hoc networks, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 03 (2014), 0551-10560.

[15]. B.A.S.Roopa Devi.B Satya Sravani.B, Prabhakara Rao.B, Investigating the Impact of Adaptive Risk aware Response System with DS Importance Factors in MANETS, International Journal of Advanced Research in Computer and Communication Engineering, 03 (2014),

[16]. V.Mahajan, M.Natue and A.Sethi, Analysis of Wormhole Intrusion attacks in MANETs, IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[17]. B.A.S Roopa Devi T.Shekinah, M.Radhika Mani, A Novel Approach for Reducing Routing Overhead In Mobile Ad hoc Network, International Journal of Research in Computer and Communication Technology, 03(2014),1682-1686.

[18]. H.L.Nguyen,U.T.Nguyen, Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks, International Conference on Networking, Systems, Mobile Communications and Learning Technologies, April, 2006.

[19]. BAS Roopa Devi, Dr JVR Murthy, Dr G Narasimha, Impact of Different Mobility Models on AODV Protocol in MANET with NS-2.35 and Bonnmotion-2.1, A International Journal of Advanced Research in Computer and Communication Engineering, 03(2014), 536-539

[20]. K. Biswas and Md. Liaqat Ali, Security threats in Mobile Ad-Hoc Network, Master Thesis, Blekinge Institute of Technology Sweden, 22nd March 2007

[21]. G. A. Pegueno and J. R. Rivera, Extension to MAC 802.11 for performance Improvement in MANET, Karlstads University, Sweden, December 2006

[22]. S. Lu, L. Li, K.Y. Lam, L. Jia, SAODV: A MANET Routing Protocol that can Withstand Worm Hole Attack., International Conference on Computational Intelligence and Security, 2009.

[23]. BAS Roopa Devi, JVR Murthy, G Narasimha, S Pallam Setty, Investigating the Impact of Black Hole Attack on AODV with Statistical Tool-ANOVA, International Journal of Current Engineering and Technology,05(2015), 98-103.

[24]. S. Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, Y.Nemoto,Detecting Blackhole Attack on AODV- Mobile Ad-Hoc Networks by Dynamic Learning Method, International Journal of Network Security, Vol. 5, No.3(2017), pp. 338-346.

[25]. M. Al-Shurman, S-M. Yoo, and S. Park, Worm hole Attack in Mobile Ad-Hoc Networks, ACM Southeast Regional Conf. 2004.

[26]. BAS Roopa Devi, JV R Murthy, G Narasimha, Secure zone based routing protocol for mobile adhoc networks, International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013,839-846,

[27]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks", In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer Science, California Univ., Santa Barbara, CA, USA. pp.78- 87, ISSN: 1092-1648,(2002).

[28]. Sreedhar, K.C, Faruk, M.N., Venkateswarlu, B, A Genetic TDS and BUG with Pseudo Identifier for Privacy Preservation over Incremental Datasets, *Journal of Intelligent & Fuzzy Systems*, 32, No. 4 (2017), 2863-2873.

[29]. M N Faruk, G Lakshmi Vara Prasad, G Divya, A Genetic PSO Algorithm with QoS-Aware Cluster Cloud Service Composition, *Advances in Signal Processing and Intelligent Recognition Systems*, 425, No. 6 (2015), 395-405.

[30]. M N Faruk, Koyi Lakshmi Prasad and P Srinivasulu, Cloud based Dual Auction (DA) and A* and IDA* Searching models using BH - Strategy for resource allocation in e-markets, *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, (2015), 446 – 452.

[31]. M. N. Faruk, D. Sivakumar, A Novel Approach for Resource Discovery using Random Projection on Cloud Computing Environments,*International Journal of Engineering and Technology*, 5, No. 2, (2013), 1812-1816.

[32]. M N Faruk, M Jahnavi, B A S Roopa Devi, An Optimal Healthcare Self-Diagnosis System using Cloud Framework, I*EEE International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)*, (2017), 339-344.

[33]. MN Faruk, D Sivakumar, Towards Self Configured Multi-Agent Resource Allocation Framework for Cloud Computing Environments, International Journal of Engineering and Technology, 6.920-928(2014).

[34]. M. N. Faruk, G. L.V. Prasad , C. Nalini, An Artificial Bee Colony (Abc) Model For Cloud Service Discovery And Composition, 117, No. 7 (2017), 113-125.

[35]. Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.

[36]. Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9

[37]. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[38]. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.

[39]. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[40]. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

[41]. RAJESH, M. "TRADITIONAL COURSES INTO ONLINE MOVING STRATEGY." The Online Journal of Distance Education and e-Learning 4.4 (2016).

[42]. Rajesh, M. "Object-Oriented Programming and Parallelism."

[43]. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.