HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

NAODV: A Routing Protocol to Prevent Wormhole Attack in Ad-hoc Network

***Raksha Mehra*[*], *Gourav Shrivastava*[†] *and Amrit Suman*[‡]**

Abstract

An ad-hoc network is a network which has no predefined infrastructure & topology. The nodes can move freely in network. There is no any central administrator to control transmission and the movement of nodes. These dynamic parameters makes it Complex & Challenging. Which results various security issues are in form of the black hole attack, wormhole attack and eavesdropping. In all these attacks these malicious nodes either broadcast some wrong information about route or drops the packet. These attacks can be either active or passive. In active attack malicious nodes can change original information, but in passive attack nodes can only analyse the traffic. Some effects of malicious nodes are Black hole,

[*]Department of Computer Science & Engineering, RKDF Institute of Technology, Bhopal, M.P., INDIA
[†]Department of Computer Science & Engineering, RKDF Institute of Technology, Bhopal, M.P., INDIA
[‡]Department of Computer Science & Engineering, LNCTS, Bhopal, M.P., INDIA

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

Denial of service, Routing table overflow, Impersonation, Energy consumption & Information disclosure. This paper presents a new approach of routing which can detect and from wormhole attack in ad-hoc network. This protocol has been developed in QualNet 5.0.

Keywords

Routing Protocols, Wireless Networks, Ad-hoc Networks, Wormhole Attack

Introduction

The growth in the use of wireless [1] communications over the last few years is quite substantial and as compared to other technologies, it's huge.

1. The main advantage of MANET is the capability of the mobile node to commune with the rest of the humanity as being mobile. The protocols (routing) [2], must be circulated, because a mid host to the routing protocol for Mobile Ad Hoc Network make the direction-finding decisions. It is not central administrator so introduces a restricted access or even to a single point of malfunction allowing for the limited resources of the movable nodes.

2. They must be adaptive to the incessantly changing topology due to mobility.

3. They must work out the routes in a fast, ring free, best possible resource usage and up to date manner. Furthermore, they must keep the process of route preservation as local as possible.

4. Finally, they should provide some level of quality of service (QoS) and remain as much ready to lend hand information as possible about only the limited and sure network topology.

MANETs [1, 2] are set of mobile nodes, which are vigorously form a provisional network without pre-existing network transportation or any centralized supervision. These nodes can be illogically placed and are liberated to move indiscriminately at any given instance. Every movable node take steps itself as a router. Since there is no central supervision, so MANET is often called autonomous. MANET implies that the topology may be active and with the intention of routing of interchange through a multi-hop path is obligatory if all nodes are to be able to converse. A key concern in MANETs is the obligation that the routing protocols have to be capable for respond fast to topological

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

transform in the network. At the similar time due to the restricted bandwidth offered through mobile radio interface it is necessary that the total of manage traffic generated by the routing protocols is kept at a smallest amount. A number of protocols have been deal with these problems of routing in MANET. These protocols be separated into two module depending upon the sort of necessity and the existing resources, when a node get a route to a target:

1. **Proactive** protocols [3, 4] are differentiate by all nodes sustain routes to all target in the network at all period. As a result using a proactive protocol a node is instantly able to path (or drop) a packet. Examples of proactive protocols contain the `FISHEYE 1`. [5], the `OLSR` [6] and the `STAR` [7]. Hybrid protocols [8] are those protocols which have uniqueness of both reactive and proactive. Example of hybrid protocol includes (`DYMO`) [9].

2. **Reactive** protocols [4] are exemplified as the nodes acquire and preserve routes ON-demand. In general, when a route to an unknown target is compulsory by a node, a query is region removal form offer the much better outcome any animated view from ordinary images. Flooded onto the network and respond, containing probable routes to the target, are returned. Examples of reactive protocols include the `AODV` [9, 13] and `DSR` [10, 14].

Security always implies the classification of potential attacks, threats and vulnerabilities of a definite system. Attacks that can just be perform against a Mobile Ad hoc Network. Attacks can be classified into reactive and proactive attacks. A reactive attack does not interrupt the procedure of a routing protocol, but only try to discover important information by listening to routing traffic, which makes it very complicated to detect. A proactive attack is an effort to indecently change data, increase authentication, or acquire permission by inserting fake packets into the data stream or modify packets conversion through the network. Proactive attack can be auxiliary divided into external and internal attacks. An external attack is one reason by nodes that do not fit in to the network. An internal attack is one from compromise or takeover nodes that belong to the network. Internal attacks are typically more rigorous, since malicious nodes already belong to the network as authorized parties. Therefore, such nodes are confined with the network security mechanisms and essential services. In this paper we are presenting a new routing protocol NAODV, the modify version of AODV to detect and prevent from wormhole attack in mobile ad-hoc network.

The organization of paper is as follows, section 1 is the introduction of ad-hoc

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

network, section 2 defines the wormhole attacks section 3 presents some related work of previous papers. Section 4 is the description of NAODV protocol, section 5 presents the results and section 6 concludes the paper.

Wormhole Attack

An attacker get packets at one position in the network, `tunnels` them to a different position in the network and then replays them from this point. Tunnel packets received in one position of the network and replay them in another position the attacker can have no key objects. All it necessitates is two transceivers and one high quality out-of-band channel. Most packets will be routed to the wormhole [**?**]. The wormhole can drop packets or more cleverly, selectively forward packets to avoid detection.

Related Work

Yi-Chun Hu et. al. [15] presented a general mechanism called packet leashes, for identify and defensive against wormhole attacks, and also presented a definite protocol, called `TIK` that implements leashes. Author also discussed, the topology-based wormhole detection, and show it is impossible for these approaches to detect some wormhole topologies. Author says in certain conditions, bounding the distance between the sender and receiver cannot stop wormhole attacks; for example, when obstacles prevent conversation between two nodes that would be in transmission range, a distance-based design would still allow wormholes between the source (sender) and destination (receiver). A network that uses position information to create a environmental leash could control even these kinds of wormholes. To get done this, each node would have a radio transmission model. A receiver could verify that every probable location of the source.

$$(sender)(a\delta + v(tr - ts + 2\Delta)radiusaroundps) \tag{1}$$

can reach every probable location of the destination

$$(receiver)(a\delta + v(tr - ts + 2\Delta)radiusaroundpr) \tag{2}$$

can reach every probable location of the destination. As a result A MAC layer protocol using TIK proficiently protects against replay, spoofing, and wormhole attacks, and ensures strong freshness. TIK is implementable with existing technologies, and does not require noteworthy additional processing overhead at the MAC layer, since the authentication of each packet can be performed on the host CPU.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

Sun Choiet. al. [16] developed an efficient method called Wormhole Attack Prevention (WAP) without using dedicated hardware. The WAP not only detects the forged route but also adopts protective measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery stage. Two formulas are considered to conclude whether or not the nodes have mobility. If the nodes are fixed like sensor node, the WPT (Wormhole Prevention Timer) is predictable by:

$$WPT = (2 * TransmissionRange(TR))/Vp \tag{3}$$

Here, TR denotes a distance that a packet can travel and Vp denotes the propagation speed of a packet. It is assumed that the maximum propagation speed of the radio signal is the speed of light and the delay from sending and receiving packets is negligible.

On the other hand, if the nodes have mobility with an average velocity of Vn, the distance that packet can travel may be different. The greatest transmission distance of a packet is calculated by

$$Radius = Vn(2 * TR)/V_p \tag{4}$$

As a result, when network are produced in the mobile environment, the WPT of nodes is given by

$$WPT = (2 * Vn * TR)/(V_p)^2 \tag{5}$$

By using equation 3, 5, when a node over hears its neighbour node's retransmission, it checks whether the packet has arrived before the WPT expired. If a unknown wormhole attack is launched, the packet broadcast time between two fake neighbor nodes may be longer than the standard transmission time of one hop. Therefore, it can detect a route through a wormhole tunnel.

Gunhee Leeet. al. [17] proposed an efficient wormhole attack protection method that can suitably detect wormhole attacks. Each node maintains its neighbours information. According to the information, each node can recognize replayed packet that ahead by two attackers. Author considers the effectiveness of the projected method and the effectiveness of the approach by using interchange and memory space quantify.

For the proposed method, author builds a list of neighbours and shares a session key with each neighbour.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

Each entry in the list contains two 4byte identities. Thus, for the list, if there are neighbours for each node in a network, memory used for the list amounts to n (n (1+p) +1) bytes. Every node forwarding a packet attaches its identity and a MAC. The next node, then, checks whether the forwarder is a neighbour. The method drops the replayed packet, and it advertises the exit of the wormhole.

Xia Wang et. al. [18] projected an end-to-end detection of wormhole attack (EDWA) in wireless ad-hoc networks. Author first presents the wormhole detection which is based on the nominal hop count estimation among source and destination. If the hop count of a received direct route is much smaller than the expected value an aware of wormhole attack is raised at the source node. Then the source node will initiate a wormhole TRACING practice to identify the two end points of the wormhole. Finally, a legal route is selected for data communication. For the through path estimation sender measures its position Is, reads the destination's position id, and estimates the smallest Euclidean distance from the sender to the receiver using the formula:

$$d >= ||ld - ls|| - 2 * vmax + \delta \tag{6}$$

The greatest Euclidean distance between the source and the destination is

$$d <= ||ld - ls|| - 2 * vmax + \delta \tag{7}$$

The broadcast time t can be calculated as:

$$t = (||ld - ls||)/(V + vmax) \tag{8}$$

Which assumes that the highest transmission speed of broadcasting signal is the speed of light and the sending and receiving delay are minor. As the speed of light V is much superior than vma, author get the inference of Euclidean distance from the source to the destination as:

$$d = ||ld - ls|| + \delta \tag{9}$$

Author assumed a consistent allotment for the mobile nodes in the wireless ad hoc networks and the thickness function is known. To make possible the discussion author specify the following notations:
urnax: highest moving rate of a mobile node
V: speed of light
d: Euclidean distance between a source and a destination
lld: location of source and receiver, respectively

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

r: transmission range
h:estimation of hop count of the shortest path between the source and destination without wormhole attack
h: received hop count value from ROUTE REPLY packet
t: propagation time between source and destination
6: the maximum relative error in location measurement

ZHUB in et.al. [19] developed a new scheme DWDV(Defending Wormhole in DV-hop)which is based on wormhole attack in DV-hop that defends Wormhole attack. Determining Wormhole attack : When the anchor gets a hop, it can judge whether the hop is normal through inequality .

$$Hop < hop_{least} \tag{10}$$

When the inequality [20] is right, it means the distance of some pair of neighbored nodes is bigger than radius. This shows that the link is abnormal and the attack exists. If inequality is untenable, the wormhole attack may exist. But the attack is not so serious, some nodes can get Valid position and others cannot. Correcting the least hop count under attack: If n nodes are homogeneously placed in a quadratic field wx w. The area for per node can be calculated as equation .This area can be quantized as a square with the side length an equation.

$$b = (w * w)/n, a = \sqrt{b} \tag{11}$$

NAODV

The `NAODV` relies on the scheme that usually the wormhole nodes contribute in the routing in a frequent way as they attract most of the traffic. As a result, each node will be allocated a cost depending in its involvement in routing. The cost function is preferred to be exponential in authority of two such that to rapidly amplify the cost of already used nodes. In addition preventing the network since the wormhole attack, the scheme offer a load balance between nodes to avoid exhausting nodes that are constantly cooperative in routing.

The basic idea behind the wormhole attack is that the malicious (wormhole) nodes pull the traffic by advertising shortest or short paths, with minimum number of hops. It is therefore more likely possible to have those wormhole routes participate in routing packets. From this perspective, the modification of the NAODV protocol in such a way to disable the malicious nodes to attract the traffic all the time and be able to process it maliciously. Hence, each node will

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

be assigned a cost depending on its contributions in routing using the following cost function.

$$r(i)_{new} = n + r(i)_{old} \tag{12}$$

Where, r(i) is the rate (cost) of a node i firstly r(i) = 0.
n is the number of period a node has contributes in routing to a assured destination, initially n = 0. This function takes into consideration the number of times a node has participated in routing for a certain source and the node's cost will be increased accordingly.

One concerns the RREQs, the other concerns the added cost function. To start with, it was mentioned earlier in the default NAODV protocol description that if a node receives a RREQ, which it has already processed, it discards the RREQ and does not forward it. This step should be modified as author need to One concerns the RREQs, the other concerns the added cost function. To start with, it was mentioned earlier in the default NAODV protocol description that if a node receives a RREQ, which it has already processed, it discards the RREQ and does not forward it. This step should be modified as author need to have multiple options of routing paths for the same request originated by the source. It follows that a node should process all arrived RREQs forwarded to it by different previous hops. A new cost field should be added to the RREQs and RREPs (signaling packets), and to the nodes routing tables as well. Now if a source node needs a route to the destination, it broadcasts the RREQ packets, which will be now processed differently at intermediate nodes, and a hop by hop decision is made. The following algorithm and flow chart describe this hop-based decision.

1. A Packet is received by node (S) from Node (D) observing for a route for destination.

2. Node (D) extracts object (Source/Destination) from packet (If the packet is a Route Request then the object is the source, if the packet is a Route Replay, then the object is the Destination).

3. Node (D) examines in routing table for other node (X) having a fresh path to the Destination.

4. If the node (X) is not found or if the route is not different, an entry for the Destination node is added to the routing table of node (D).

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

5. If the node (D) is found in the routing table, and has a route to the destination the following should be verified:
   - How many times node (D) has used node (X) as a next hop (R1).
   - How many times node (D) has used node (S) as a next hop (R2).
   - Compare R1 and R2.
   - Update the routing table.
   - Add node (D)'s cost to the packet and forward it to the destination node. Destination node (Source/Destination) accepts the coming packet determines the final cost and compares with its routing table to select the path with minimum cost.

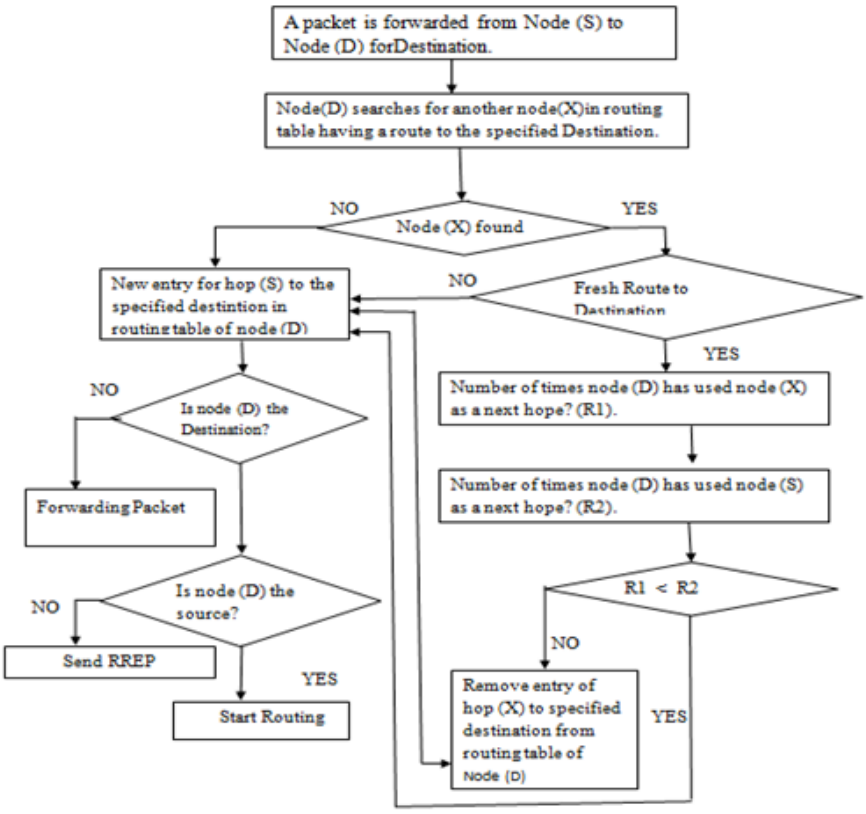

Figure 1: *Flow chart for NAODV*

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

Results

Execution of NAODV protocol is executed in QualNet 5.0 [17]; to begin with number of nodes are 50, Simulation time was in used 200 seconds. All circumstances have been designed in 1500 m x 1500 m area. Mobility representation used is Random Way Point (RWP). In this representation a mobile node is originally placed in a unsystematic location in the simulation area, and then stimulated in a randomly chosen direction among at a random speed between [SpeedMin, SpeedMax]. The association proceeds for an unambiguous amount of time or distance, and the procedure is repeated a determined number of times. We choose Min speed = 5 m/s, Max speed = 30m/s, and pause time = 5s to 30s.
The Performance metrics used for this works are as follows:

1. **The Performance metrics used for this works are as follows:**
2. **Throughput** [21, 22] is the degree of the number of packets effectively transmitted to their final target per unit time. It is the ratio between the numbers of sent packets vs. received packets.
3. **AverageEnd to End Delay** [21, 23] indicates the average time taken by packets to reach one end to another end (Source to Destination).
4. **Packet Loss** [24, 25] is the Ratio of communicated packets that may have been rejected or lost in the network to the total number of packet sent.

The Performance Metrics

The results of implementation by different variations are following:

Analysis of Throughput for NAODV, AODV, DSR with variation in Pause Time

Refer figure 2: It can be observed by throughput of NAODV is better than the DSR and AODV when pause time is kept 10, 20, 30, 40, 50 and 60.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

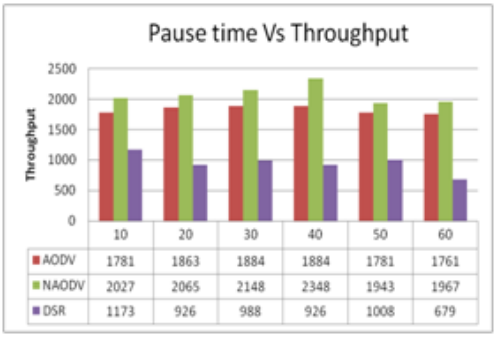

Figure 2: *Throughput v/s Pause Time: shows throughput of protocols when pause time varies.*

Analysis of End-to-End delay for NAODV, DSR, AODV with variations in Pause Time

Refer figure 3: It can be observed that End to End delay of NAODV is less than other than two protocols, when pause time is kept 10, 20, 30, 40, 50 and 60.

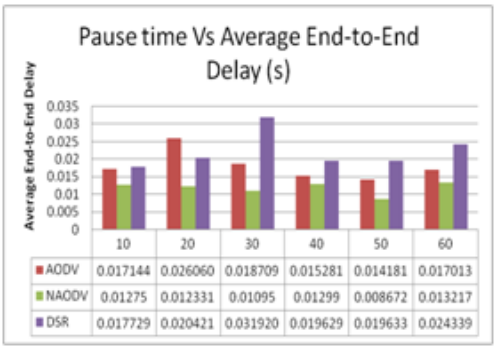

Figure 3: *Calculating End to End delay v/s Pause Time:shows End to End delay of protocols when pause time varies.*

Analysis of Total Packets Received for NAODV, DSR, AODV with variation in Pause Time

Refer figure 4: It can be observed that total packets received by NAODV are greater than other two protocols, when pause time is kept 10, 20, 30, 40, 50 and 60.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

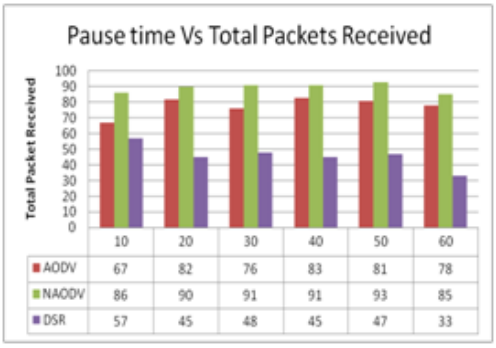

Figure 4: *Pause time v/s Total Packets Received:shows Total Packets Received of protocols when pause time varies.*

Analysis of Average Jitter for NAODV, DSR, AODV with variation in Pause Time

Refer figure 5 It can be observed that average jitter of NAODV is less than both DSR, AODV when pause time is kept 10, 20, 30,40 50 and 60.

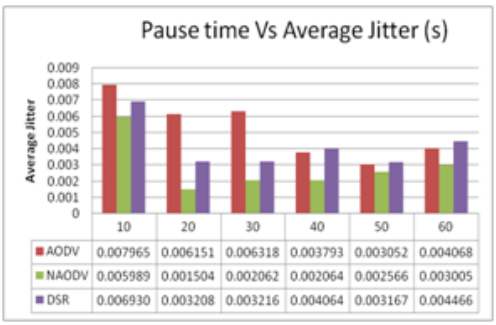

Figure 5: *Pause time v/s Average Jitter(s): shows average jitter of protocols when pause time varies.*

Analysis of Throughput for NAODV, DSR, AODV with variation in Node Speed

Refer figure 6: It can be observed that throughput NAODV is better than DSR and AODV, when speed of node in network is kept 10, 20, 30, 40, 50 and 60.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

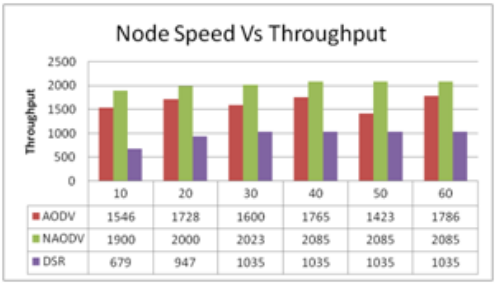

Figure 6: *Node Speed v/s Throughput: Shows throughput of protocols when nodes speed in network varies.*

Analysis of End-to-End Delay for NAODV, DSR, AODV with variation in Node Speed

Refer figure 7 It can be observed that average end-to-end delay of NAODV is less than AODV and DSR, when speed of node in network is kept 10, 20, 30, 40, 50 and 60.

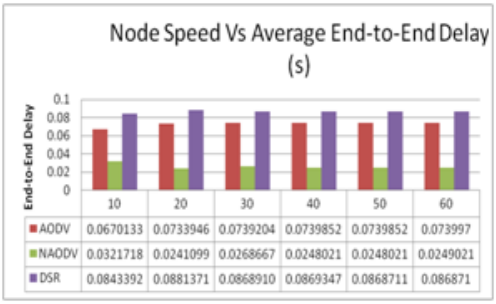

Figure 7: *Node Speed v/s Average End-to-End Delay(s): Shows average end-to-end delay of protocols when node speeds in network varies.*

Analysis of Maximum Packets Received NAODV, DSR, AODV with variation in Node Speed

Refer figure 8: It can be observed that average jitter of network using NAODV is less than DSR and AODV. It can also observed that average jitter of DSR is less than other protocol when speed of node in network is 10 to 60 mps.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 3, May 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

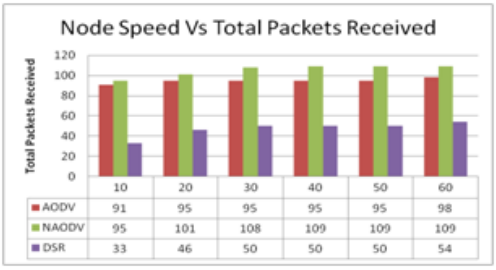

Figure 8: *: Node Speed v/s Average Jitter(s): Shows average jitter of protocols when node speed in network varies.*

Analysis of Average Jitter for NAODV, DSR, AODV with variations in Node Speed

Refer figure 9:It can be observed that a total packet received by network using NAODV is better when node speed is 10 to 60 mps.

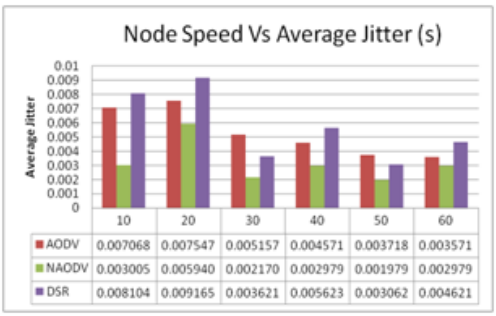

Figure 9: *Node Speed v/s Total Packets Received: Shows total packets received of protocols when node speeds in network varies.*

Conclusion

This paper presents a routing protocol NAODV, for detection and prevention of worm-hole attack in different scenario. This implementation and analysis is performed in QualNet 5.0. There are four performance matrices were used for analysis they are throughput, average jitter, end-to-end delay and total packet received. The result has been analysed with variation in speed of node in network and pause time of network. It is observed that the results of NAODV is better than comparision of AODV and DSR. In some cases NAODV is not performing well, but most of the results shows NAODV is better than other.

References

[1] M. Frodigh, P. Johansson, and P. Larsson.`Wireless ad hoc networking: the art of networking without a network`, Ericsson Review, No.4, 2000, pp. 248-263.

[2] G.V.S. Raju and G. Hernandez, `Routing in Ad hoc networks`, in proceedings of the IEEESMC International Conference, October 2002.

[3] Daniel Lang, `On the Evaluation and Classification of Routing Protocols for Mobile Ad Hoc Networks`, 2006.

[4] Rama Murti, `Wireless Networking`, 2008.

[5] Julian Hsu Julian Hsu, Sameer Bhatia, Mineo Takai, Rajive Bagrodia, `Performance of mobile ad hoc networking protocol in realistic scenario`, 2005.

[6] `Existing MANET Routing Protocols and Metrics used Towards the Efficiency and Reliability - An Overview`, Shafinaz Buruhanudeen, Proceedings of the IEEE Malaysia International Conference on Communications,14-17 May 2007, Penang, Malaysia 1-4244-1094-0/07, 2007 IEEE.

[7] A. Boomarani Malany, V. R. Sarma Dhulipala and R. M. Chandrasekaran, `Throughput and Delay Comparisonof MANET Routing Protocols`, Int. J. Open Problems Compt. Math., Vol. 2, No. 3, September 2009 ISSN 1998-6262; Copyright ICSRS Publication, 2009

[8] Layuan, Li Chunlin, Yaun Peiyan, `Performance evaluationand simulation of routing protocols in ad hoc networks`, Computer Communication, February 2007.

[9] Yi-Chun Hu, Adrian Perrig, `A Survey on Secure Wireless Ad Hoc Routing`, IEEE Security and Privacy, 1540-7993/04 2004 IEEE, May/June 2004.

[10] D. Djenouri, A. Derhab, and N. Badache, `Ad hoc networks routing protocols and mobility`, Int. Arab J. Inf. Technol. 3(2):126-133, 2006

[11] Rajiv Misra, C. R. Mandal, `Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad HocNetworks in Constrained Situation`, IEEE 2005.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

[12] Ioannis Broustis, Gentian Jakllari, Thomas Repantis, Mart Molle, `A Performance Comparison of Routing Protocols for Large-Scale Wireless Mobile Ad Hoc Networks`, Department of Computer Science & Engineering University of California, Riverside 2004.

[13] Xin Yu, `Distributed Cache Updating for the DynamicSource Routing Protocol`, IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 609-626, Jun., 2006.

[14] Yi-Chun Hu, Adrian Perrig, `Wormhole Attacks in Wireless Networks`, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[15] Sun Choi, `WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks`, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008.

[16] Gunhee Lee, Dong-kyoo Kim, `An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks`, International Conference on Information Security and Assurance, 2008.

[17] Xia Wang, `An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks`, 31st Annual International Computer Software and Applications Conference, 2007 IEEE.

[18] ZHU Bin, `Defending Wormhole Attack in APS DV-hop`.

[19] D. Niculescu and B. Nath, `Ad hoc positioning system (APS)`, Technical Report DCS-TR-435, Department of Computer Science, Rutgers University (2001).

[20] T. S. Rappaport. `Wireless Communications: Principles and Practice`, Prentice-Hall, 1996.

[21] Charles E.Perkins. `Ad hoc Networking`, Addison-Wedey, 2001.

[22] Daniel Lang , `On the Evaluation and Classification of Routing Protocols for Mobile Ad Hoc Networks`, 2006.

[23] A. Lindgren, `Infrastructured Ad Hoc Networks`, Proc. 2002 Int'l Workshop on Ad Hoc Networking, Vancouver, August 2002.

[24] J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, `A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols`, Proc. Fourth ACM MobiCom, pp. 85-97, 1998.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-443-8

[25] Qualnet Simulator Documentation. `Qualnet 5.0 User's Guide`, Scalable Network Technologies, Inc., Los Angeles, CA 90045, 2006.

[26] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, `Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method`. International Journal of Network Security, Vol.5, No.3, PP.338346, Nov. 2007.