ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Securing Mobile Adhoc Network Routing Protocol Using NS-2 Simulator

Avni Verma[*1], Prof. Nitin Tiwari[2]

M. Tech Research Scholar, Department of Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India[*1]

Department of Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: Mobile uncommonly named frameworks will appear in circumstances where the centers of the frameworks are missing and have by zero physical security against modifying. The remote center points of MANET are in this way powerless to deal and are particularly vulnerable against refusal of organization (DOS) attacks moved by malevolent center points or intruders. Flooding attack is one such sort of DOS ambush, in which a haggled center point surges the entire framework by sending a far reaching number of fake RREQs to nonexistent center points in the framework, in this way realizing framework stop up. In this paper, the security of MANET AODV guiding tradition is inquired about by recognizing the impact of flooding strike on it. A generation examination of the effects of flooding attack on the execution of the AODV directing protocol is presented using self-assertive waypoint compactness demonstrate The re-enactment environment is completed by using the NS-2 framework test framework. It is watched that as a result of the closeness of such dangerous centers, ordinary rate of bundle disaster in the framework, typical coordinating overhead and ordinary transmission limit requirement− all grows, thusly debasing the execution of MANET basically.

KEYWORDS: AODV; flooding attack; malicious nodes; MANET; NS-2 simulation; packet loss; wireless security

I. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a gathering of remote versatile hosts, which has no stationary foundation or base station for communication. Each individual node imparts past their immediate remote transmission range by collaborating with each other and sending bundles through multi-jump joins. The hubs go about as switches for sending and accepting parcels to/from different hubs. Specially appointed systems administrations are broadly use for military purposes, fiasco help, mine site operation, and so forth. For such applications, a safe and solid correspondence is essential. Directing in specially appointed systems [2] [3] [4] has been a testing assignment following the time when remote systems appeared. Because of the high versatility of hubs, obstruction, multipath spread and way misfortune, there is no settled topology in MANET. Consequently an element directing convention is required for these systems to work legitimately. Dynamic Routing Protocol can be delegated Proactive and Reactive Routing Protocols: The proactive (table-driven) steering conventions like DSDV [5], and so on keep up the directing data to each other hub in the system, even before it is required.

The responsive (on-interest) directing conventions like AODV [6], DSR [7] and so forth, don't keep up the steering data's to different hubs in the system, until and unless required. This kind of conventions finds a course on interest by flooding the system with Route Request parcels. Much of the time, the on-interest (receptive) steering conventions have demonstrated to perform preferable with essentially bring down overheads over the intermittent (proactive) directing conventions. This is on account of the on-interest conventions can respond rapidly to the powerfully evolving topology, while lessening the directing overhead in those territories of the system, where changes are less successive. In this paper, the emphasis is predominantly on the responsive steering conventions (to be specific AODV) for MANET. Every single available center in uniquely delegated frameworks take an enthusiasm for coordinating and sending, with a particular final objective to help the total framework throughput. Hence, powerful operation of MANET is possible if and just if all the taking an interest center points totally partake in correspondence. As a result of the non-appearance of a settled base station, the uncommonly selected center points are constrained to

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

rely on upon each other to keep up framework reliability and handiness. Nevertheless, getting into naughtiness centers [8] [9] [10] are fit for bringing on imperative issues. A center point may act fiendishly when it is over-weight, broken, pretentious, or harmful.

A malicious center [11], in like manner cancelled exchanged center point, can upset substitute center points or even the whole framework, by moving a denial of organization ambush, by either dropping bundles or by flooding the framework with a far reaching number of RREQs to invalid destinations in the framework, in this way staying the courses of correspondence. Flooding ambush is one such kind of DOS attack, in which an exchanged off center surges the entire framework by sending endless RREQs to nonexistent center points in the framework or by spouting significant volumes of pointless DATA groups to interchange centers of the framework. This results in framework blockage, henceforth inciting a Denial of Service.

In this paper, a re-enactment investigation of effect of flooding assault in AODV [6] execution, utilizing the NS-2 system test system is given. The rest of the paper is organized as follows. In section II, an overview of the AODV routing protocol is presented, followed by a briefing about the NS-2 network simulator in Section III. The impact of flooding attack in MANET is discussed in section IV. In section V, the simulation parameters used are given, followed by the simulation results in section VI and concluding remarks in section VII

II. OVERVIEW OF AODV PROTOCOL

The Ad hoc On-demand Distance Vector (AODV) [6] steering convention is a basic and effective on-interest directing convention, in view of the separation vector approach. It is composed particularly for use in multi-bounce remote MANET situation. The convention is made out of the two fundamental instruments − "Course Discovery" and "Course Maintenance". Course disclosure depends on inquiry and answer cycles, and course data is put away in every single middle of the road hub along the course through steering table passages. Course Request (RREQ) message is shown by a hub requiring a course to another hub and Route Reply (RREP) message is unicasted back to the wellspring of RREQ. Arrangement numbers are utilized for each steering table passage to figure out if the directing data is a la mode. This averts steering circles. AODV incorporates the course upkeep system to handle the dynamic system topology. Courses are kept up by utilizing Route Error (RERR) message, which is sent to inform different hubs around a connection disappointment. Hi messages are sent in occasional reference points for identifying and observing the connections to the neighbours. On the off chance that a hub S needs to send information bundles to a destination D that is not in its directing table, it will cushion the information parcels and show a Route Request (RREQ) for D into the system. The RREQ parcel will be sent by other middle of the road AODV hubs to the proposed destination hub D. On accepting the RREQ, D will send a Route Reply (RREP) on the opposite course back to S. S incorporates the known arrangement number of the destination in the RREQ parcel. The middle of the road hubs, on accepting a RREQ bundle check its directing table passages. On the off chance that it has a crisp course toward D, i.e. a course with more noteworthy arrangement number than that in the RREQ parcel, it unicast a RREP bundle back to its neighbour from which it has gotten the RREQ parcel. Else, it sets up the opposite way and after that rebroadcasts the RREQ parcel. Copy RREQ parcels got by one hub are noiselessly dropped. As the RREP parcel is spread along the converse way to the source, the transitional hubs overhaul their steering tables and set up the forward way.

III. THE NS-2 SIMULATOR

For reproduction examination, NS-2 [12] [13] was utilized for actualizing the system reenactment environment. NS-2 is an open source discrete occasion system test system focused on fundamentally to network research and instructive reason. Beforehand, NS-2 [14] was the apparatus for scholarly systems administration research. Be that as it may, it had a few disservices. It required the contribution of both oTcl and C++. For new modules and components, it required a ton of manual recoding and gatherings. NS-2 is another test system. It is not an expansion of NS-2. It doesn't bolster the NS-2 APIs. It is composed altogether in C++, with discretionary Python ties. Consequently, recreation scripts can be composed either in C++ or in Python. The oTcl scripts are no more required for controlling the reenactment, in this way deserting the issues which were presented by the mix of C++ and oTcl in NS-2. In this manner, NS-2 is an all the more promptly extensible stage and much less demanding to utilize. NS-2 has cutting edge diversion highlights, which consolidate wide parameterization system and configurable introduced taking after structure, with standard respects content logs or PCAP (tcpdump). It is incredibly dissent arranged for quick coding and extension. It has a modified memory organization capacity and a beneficial article absolute/question for new practices

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

and states, for example, adding flexibility models to center points. Moreover, NS-2 has new capacities, for instance, dealing with various interfaces on center points viably, profitable use of IP tending to and more game plan with Internet traditions and frameworks and more unequivocal 802.11 models, et cetera. NS-2 joins the designing thoughts and code from GTNetS [15], which is a test framework with awesome versatility properties. The Simulation Network Architecture looks just like IP building stack. The center points in NS-2 may potentially have flexibility. The center points have "framework contraptions", which trade packages over channel and circuits Layer 1 (Physical Layer) and Layer 2 (Data Link layer). The framework devices go about as an interface with Layer 3 (Network Layer: IP, ARP). The Layer 3 reinforces the Layer 4 (Transport Layer: UDP, TCP), which is used by the Layer 5 (Application Layer) objects.

IV. EFFECT OF FLOODING ATTACK

A vindictive (traded off) hub for the most part means to dispatch a foreswearing of administration in the entire system. Flooding assault [11] [16] [17] [18] is a dissent of administration assault, in which a traded off hub surges the system by sending extensive number of fake RREQs to nonexistent hubs in the system or by spilling expansive volumes of pointless DATA parcels to alternate hubs of the system.
Flooding assault can be arranged into two sorts [17]: RREQ Flooding Attack and Data Flooding Attack.

A. RREQ Flooding Attack

The RREQ Flooding Attack is a foreswearing of-administration assault in which vindictive hubs exploit the course revelation procedure of the receptive steering conventions (e.g. AODV, DSR) in MANET. In this assault, a bargained hub expects to surge the system with a substantial number of RREQs to non-existent destinations in the system. It produces countless and telecast them to invalid destinations. Since a hub with such invalid destination hub id does not exist in the system, an answer parcel can't be created by any hub in the system and they continue flooding the RREQ bundle. . At the point when such fake RREQ parcels are shown into the system in high numbers, the system gets immersed with RREQs and can't transmit information bundles. In this way, it prompts blockage in the system. The RREQ Flooding Attack additionally brings about flood of course table in the halfway hubs so that the hubs can't get new RREQ bundle, bringing about a dissent of-administration assault. In addition, superfluously sending these fake courses ask for parcels cause wastage of valuable hub resources such as energy and bandwidth.

To reduce congestion in a network, the AODV protocol adopts some methods. RREQ_RATELIMIT [19] is the maximum allowable number of RREQs that a node can sent per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may again try to discover a route by broadcasting another RREQ, until the numbers of retries reach the maximum TTL value. The default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. However, a malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node can do so because of its self-control over its parameters. This allows it to flood the network with fake route requests, leading to a kind of DOS attack due to the network-load imposed by the fake RREQs.

B. Data Flooding Attack

Once an aggressor hub has set up the ways to every one of the hubs in the systems, it might bring about DATA Flooding Attack by spilling vast volumes of pointless DATA parcels to them along these ways. The over the top DATA parcels in system obstruct the system and decrease the accessible system transfer speed for correspondence among alternate hubs in the system. The destination hub gets occupied on accepting the unreasonable bundles from the assailant and can't work typically. The accessible system transfer speed for correspondence likewise gets depleted, so that alternate hubs can't speak with each other because of the blockage in the system. Also, the procedure of getting the assault parcels expends a considerable measure of asset in all the transitional hubs. On the off chance that an assailant joins both sorts of flooding assaults, it will bring about the entire system smashing.

Because of flooding assault, a non-vindictive bona fide hub can't reasonably serve different hubs because of the system load forced by the fake RREQs and pointless information parcels.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

This prompts a few issues, as takes after:

- Wastage of bandwidth
- Wastage of nodes' processing time, thus increasing the overhead
- Overflow of the routing table entries, causing exhaustion of an important network resource like memory
- Exhaustion of the nodes' battery power
- degraded throughput

Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication.

V. SIMULATION SETUP

The simulation was done using the NS-2 simulator [12], which provides a scalable simulation environment for wireless networks. In order to measure the impact of flooding attack in MANET performances, the AODV routing protocol was modified to simulate a flooding attack scenario. The simulated Network consists of 16 nodes placed randomly in 500x500 areas. For different scenarios of simulation, Constant position mobility and Random-walk 2D mobility model are used. Each node moves at a speed of 20 m/s.

The Ping application was used in the application layer. To simulate flooding attack, some malicious nodes were introduced to flood the network. These flooding nodes generated fake RREQ packets with invalid destination addresses and broadcasted them in the network at the rate of 8 packets per sec. By default, RREQ_RATELIMIT [19] of each node is 10, as proposed by RFC 3561.This RREQ_RATELIMIT was changed to 50.The simulation parameters along with their values are listed down in Table I.

TABLE I. SIMULATION PARAMETERS

Parameters	Val
routing protocol	AODV
simulation time	60s
number of mobile nodes	95
transmission area	1000 x1000
mobility model	Random-walk 2d mobility/ Constant position
traffic type	UDP
data packet size	1024Bytes
Rate	2Kbps
speed of node	20m/s
RREQ_RATELIMIT	50

VI. SIMULATION RESULT

After simulating the flooding attack in AODV, some graphs were plotted and they were used to see the simulation results when the network gets flooded by fake RREQs to invalid destinations.

For the simulation in Fig. 1, fake RREQ parcels were created and the aggregate number of unique RREQs that landed at every hub was figured. Steering Overhead indicates the aggregate number of RREQs messages (unique and also fake)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

showed in the system. The diagram in Fig. 1 portrays that the normal Routing Overhead increments with the quantity of fake RREQs. On account of these fake RREQ messages, steering table of every hub needs to keep up more sections, in this way making an additional overhead.

For Fig. 2 re-enactment, the aggregate number of information parcels that were dropped because of the RREQ flooding was figured. The chart delineates that the normal rate of information bundle misfortune increments with the expansion of fake RREQs in the system.

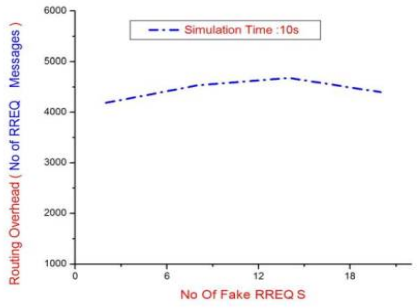

Figure 1: Number of fake RREQs vs. Routing Overhead

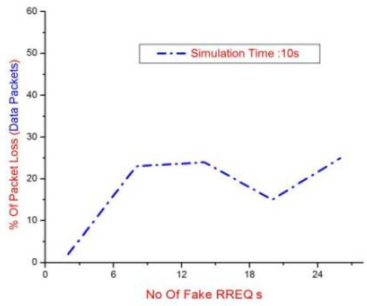

Figure 2: Number of fake RREQs vs. Percentage of data packet loss

Next, some flooding nodes were introduced, which generate eight RREQs per second. The graph in Fig. 3 depicts that with the increase in the number of flooding nodes, Routing Overhead, (i.e. Total number of original and fake RREQ packets in the network) increased drastically.

The bandwidth usage in the network was calculated, as follows:

Bandwidth usage =

(Total num of packets received/Simulation Time)*(8/1000) Bandwidth usage of a network is inversely proportional to the throughput of the network.

The graph in Fig. 4 depicts that the average bandwidth usage of the network increases as more flooding nodes join the network. Because of this flooding attack, average bandwidth usage of the network increases considerably, thus decreasing the network throughput.

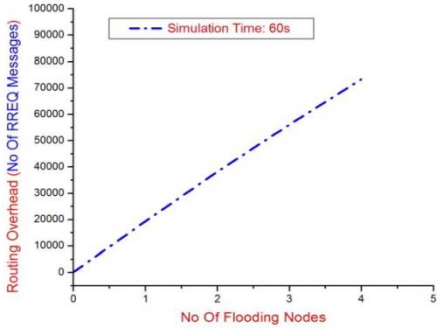

Figure 3: Number of flooding nodes vs. routing overhead

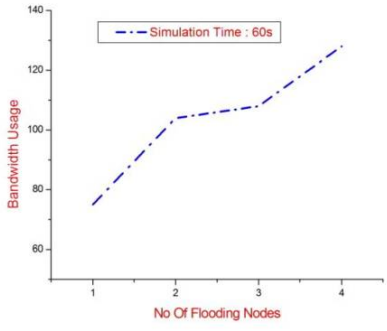

Figure 4: Number of Flooding Nodes vs. Bandwidth Usage

Fig. 5 shows the average percentage of data packet loss due to the presence of flooding nodes in the network. The graph depicts that the average percentage of data packet loss in the network increases with the number of flooding nodes. Due to the flooding attack, the network gets congested, resulting in a loss of RREQ packets as well.

The graph in Fig.6 depicts that as the number of flooding nodes in the network Increases, the average packet loss (both data and routing packets) also increases in the network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

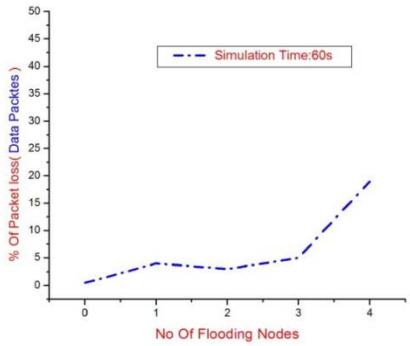

Figure 5: Number of Flooding Nodes vs. Percentage of Data Packet Loss

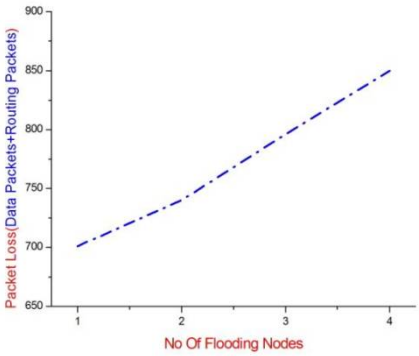

Figure 6. Number of Flooding Nodes vs. Percentage of Overall Packet Loss (Data and Routing Packets)

VII. CONCLUSION

In this paper, AODV directing convention in MANET was explored by distinguishing the effect of flooding assault on it. The flooding assault in AODV convention was reproduced utilizing the NS-2 system test system. Be that as it may, comparative results can likewise be found when utilizing the DSR [7] steering convention. It was seen that the nearness of pernicious flooding hubs in MANET can influence the execution of the general remote system and can go about as one of the real security dangers. From the recreation, it can be inferred that because of the broad flooding in the system, normal rate of bundle misfortune, normal steering overhead and normal transfer speed requirement− all builds, along these lines diminishing the general system throughput.

A solid observing system must be executed in the versatile hubs of MANET for the ID and disconnection of the bargained flooding hubs from the system. Some kind of impetus component may likewise be joined in the system to authorize participation among every one of the hubs in MANET to enhance the general system execution.

In future work, a notoriety based trust system is proposed, which opposes bad conduct in the system by propelling the hubs to upgrade participation and therefore enhance the system execution.

REFERENCES

[1] S Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”. Internet Request for comment RFC 2501, Jan 1999.
[2] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.
[3] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, “Routing security in ad hoc wireless networks”, Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.
[4] Krishna Gorantala, “Routing Protocols in Mobile Ad-hoc Networks”.June 15, 2006, Master’s Thesis in Computing Science, 10 credits; Supervisor at CS-UmU: Thomas Nilsson; Examiner: Per Lindstrom.
[5] C. Perkins and P Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers”. In ACM SIGCOMM’94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234 -244.
[6] C.E. Perkins, E. Belding Royer, and S.R. Das, “Ad hoc On demand distance vector (AODV) routing”, IETF RFC 3561, July 2003.
[7] D.Johnson, Y. Hu and D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.
[8] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, “Mitigating routing misbehaviour in mobile ad hoc networks”. International Conference on Mobile Computing and Networking, Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, Boston, Massachusetts, United States, pgs. 255 – 265.
[9] A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols".IETF RFC4593. Status Informational, October, 2006.
[10] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks,” in Wireless/Mobile Network Security, Springer, 2008.
[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.
[12] “The NS-2 Network Simulator", http://www.nsnam.org/
[13] Elias Weingartner, Hendrik vom Lehn, Klaus Wehrle, “A performance comparison of recent network simulators". In Proceedings of the IEEE International Conference on Communications 2009 (ICC 2009), Dresden, Germany, 2009.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

[14] "The NS-2 Network Simulator", http://www.isi.edu/nsnam/ns
[15] G. Riley, "Large scale network simulations with GTNetS", in Proceedings of the 2003 Winter Simulation Conference, 2003.
[16] S. Sanyal, A. Abraham, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N.Mody, "Security scheme for distributed DOS in mobile ad hoc Networks", 6th International Workshop on Distributed Computing (IWDC'04), vol. 3326, LNCS, Springer, 2004, pp. 541.
[17] P. Yi, Z. Dai, Y. Zhong, S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), April 2005, pp. 657-662.
[18] Z. Eu and W. Seah, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan, January 2006.
[19] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF- MANETterms-00.txt, November 1997.