International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

The performance evaluation of Adjusted Probabilistic Flooding on AODV protocol based on flooding mechanism in MANETs

Khushboo Sharma
Department of Computer Science and Engineering
Radharaman Institute of Technology and Science
Madhya Pradesh, Bhopal, India

Anurag Jain
Department of Computer Science and Engineering
Radharaman Institute of Technology and Science
Madhya Pradesh, Bhopal, India

***Abstract*---A Mobile ad-hoc network (MANET) is transient set of connections which is set up by wireless movable computers (or nodes) moving randomly in the spaces that have no network infrastructure. Mobile Ad-Hoc Networks are self-directed and decentralized wireless systems. Data transmission between two nodes in MANET's, requires multiple hops as nodes broadcast range is inadequate. Mobility of the different nodes makes the state even more cumbersome. MANETs regularly experience the ill effects of security assaults on account of its highlights like open medium, transforming its topology of Black hole Assault in MANE. This paper leads the emphasis on the detection and prevention of the flooding attacks in AODV protocol. AODV is an on-demand routing protocol that works on RREQ message Broadcasting. Flooding Attacks Blocks the transmission of network by overloading (Congestion) the nodes.**

Keywords---Flooding Attack; Congestion; AODV; Multiple Hops; MANET; Security Threats.

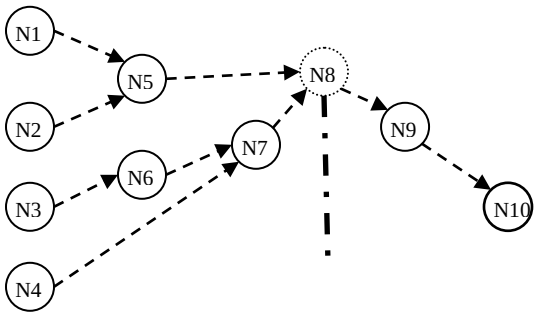
I. INTRODUCTION

Compared to wired networks, MANET has distinctive characteristics such as infrastructure-less, decentralized, multi-hop, self-organized network. In a mobile ad hoc network, nodes move arbitrarily, so the network may experiences impulsive topology changes where fixed infrastructure is not easily acquired. With the lack of pre-established infrastructure mean no router, no access point, etc. Two nodes communicate with one another in a peer-to-peer fashion. Various impromptu directing conventions like DSR, AODV, LAR, ZRP, and so on., depend on flooding for scattering course disclosure, course support, or topology overhaul packets. [1]

Numerous routing protocols have been developed for MANETS like AODV, DSR, OLSR etc. Security of Mobile Ad-Hoc Network is the major imperative concern for the essential functionality of network. The accessibility of system administrations, privacy and honesty of the information can information can be attained to by guaranteeing that security issues have been met The MANETs work without a concentrated organization where the hubs speak with one another on the premise of common trust. These factors and integrity of the data in the network can be achieved by assuring the changed battle field status for the MANETs against the security threats, because of this characteristic MANETs more vulnerable to be browbeaten by an attacker inside the network.

In flooding attacks [2], an assailant debilitates the system assets, for example, data transmission and to expend a hub's assets e.g. computational and battery power or to upset the directing operation to bring about extreme corruption in system execution. In AODV convention, a malignant hub can send a substantial number of RREQs in a brief time to a destination hub that does not exist in the system. Because these RREQs will not get any reply, these RREQs will flood the entire network. As a result, the node battery power, and this can lead to denial-of-service to other users as the network will get congested.

Efficient flooding schemes are diverse from the broadcast mechanisms discussed in [1] Broadcasting is used in transmission of huge amount of data or stream media data. In contract, flooding is used in dissemination of control packets instead of data packets, which is a one-off Operation. When RREQ message is broadcast in the network then the nodes which receives the RREQ message sends the acknowledgment in the form of RREP, this process is continued till any of the nodes is not ready for the process.



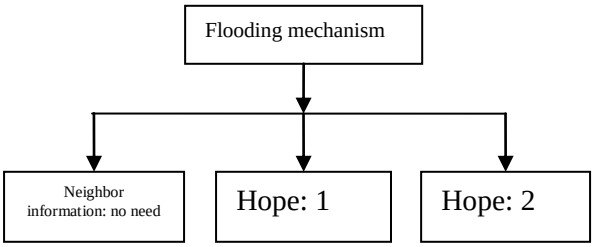


Figure 1: (a) Flooding in mobile nodes, (b) Flooding mechanism

II. RELATED WORK

Bin Xiao et al gave an Active Detecting Method against SYN Flooding Attack. SYN flooding assaults are a far reaching kind of Distributed Denial-of-Service (DDoS) attack. The procedure offered in this paper catches brutal marks utilizing a dynamic examining plan that guarantees the ingenious early discovery. The dynamic examining plan acquires the postponement of switches by sending bundles containing exceptional Time-to-Live set at the IP headers. The outcome of the probe are used to achieve SYN flooding detection, which is reliable and with little transparency. [11]

Bhuvaneshwari .k et al gave A Profile based Detection Scheme for flooding attacks in AODV for MANET. In PDS, the Flooding assault is propelled by changing as far as possible requirement for the malignant hubs. The expected location technique (PDS) goes for identifying the flooding assault on MANET. The PDS move towards using dynamic profile based traffic analysis to make out misbehaving nodes and detach them. The PDS approach has two different phases of operations, detection phase and isolation phase. [12]

Ruchita Meher et al gave a point assessment of various counter based schemes using neighborhood information to accomplish good performance in MANETs and condense the broadcast storm problem. This paper gives the outline of broadcasting in MANET. Broadcasting in MANET typically depends on the flooding mechanism where the source node delivers a packet to its neighborhood node which is just intact to it. In broadcasting mechanism, every node which receives a packet which is being broadcasted and similar will be merely re-transmits it to all its neighbors. Hence, we can say that broadcasting done during flooding is generally very expensive which results in contention, severe transmission redundancy and collisions in the network such a state, is said to be the broadcast storm problem. [13]

Karthik Lakshminarayanan et al, this paper focus on IP flooding attack. Objective is to make the throughput bend as near to ideal to give control to has over the bundles they get. The best conceivable reaction to this occasion Taming IP Packet Flooding Attacks A. Abstain from accepting bundles at subjective ports Internet hosts can get spontaneous parcels at ports where no administration runs a host ought to get parcels just at ports on which it is listening or as a component of a built association. Though these packets are dropped by the kernel, they devour network bandwidth and may influence other services. Thus, a host should receive packets only at ports on which it is listening or as part of an conventional connection. [14]

Ms. Neetu Singh Chouhan et al, Worked on Flooding Attacks Prevention in MANET, in this paper they have developed Flooding Attack Prevention (FAP), a protection against the Ad Hoc Flooding Attack in portable ad hoc networks. When the intruder broadcasts exceeding packets of Route Request, the direct neighbors of the intruder trace the behavior of sender and verify its trust by a trust function. Once the threshold is exceeded, nodes contradict any future request packets from the intruder. The consequences of this accomplishment show FAP can prevent the Ad Hoc Flooding attack efficiently. [15]

Madhavi, S.et al, their study consider the hello flooding attack. Due to constant flooding of the hello packets by the malicious node, the adjoining node will not be capable to process other packets. The operation of the valid node is preoccupied and destroys the networking operation. Nonexistence of hello packet during the periodical hello period may lead to wrong supposition which says that adjoin node has been moved away. As a result the transitional neighbor nodes sends Route Error (RERR) message and the source node again starts the route discovery process. In a arbitrary manner the hello interval values are changed and transmit the changed values to the other nodes in the network in a protected manner. This study identifies and prevents the flooding attack. [16]

Dimitris Geneiatakis et al worked on Utilizing bloom filters for detecting flooding attacks against SIP based services. This paper inspects flooding assaults contrary to VoIP architectures that use the Session Initiation Protocol (SIP) as their flagging convention. The attention is on the configuration and achievement of the suitable discovery technique. Especially, a blossom channel based screen is offered and another metric, named session separation is acquainted in place with present a proficient insurance plan against flooding assaults. The proposed plan is assessed through trial proving ground building design under various situations. The results of the evaluation exhibit that the required time to detect such an attack is insignificant and also that the number of false alarms is close to zero. [17]

Mohamed A. Abdelshafy et al, gave a scheme for Resisting Flooding Attacks on AODV. This paper introduces a simple mechanism to oppose such attacks that can be included into any routing protocol which is reactive. It is not expensive in cryptography and authentication mechanisms, but to categorize the nodes as malicious it relies on the locally used timers and thresholds. No modifications are done to the packet formats, so the overhead is a little measure of computation at hubs, and no extra correspondence. NS2 simulator is used to evaluate network's performance using AODV under flooding attacks with and without their mechanism; this considerably reduces the consequences of a flooding attack. [18]

Gaurav Sharma et al, worked on Congestion Control in AD Hoc Network. In this paper they have established a simple flow counting algorithm .The paper concludes a plan which is a set of congestion control mechanisms in wireless network and accomplishment is done through simulation on various network constraint such as unstable queue length and number of sender increased. The result shows the routine of congestion control mechanisms and how mechanism behaves when we augment number of sender and usages. [19]

Bhuvaneshwari. K et al, worked on the Impact of Flooding attack on MANET and give emphasis to Performance Degradation. The NS2 network simulator is used to assess the impact of flooding attack on AODV. Flooding attack is simulated in ns2 by using the timer based approach in AODV routing protocol. This approach is managed by time. As per RFC the rate limit for RREQ is defined as 10 per sec. This is overwritten by using the Flood generator function. This function will keep on generating the RREQ irrespective of the rate limit. Hence over a phase of time the network has supplementary number of RREQ targeting the destination. [20]

III. PROBLEM STATEMENT

After studying the literature of different previous related work done found that the some proposed methodologies efficiently reduces the end to end delay, saving computation power and network overhead also but, if the intruder has the idea about the threshold value then it can bypass which can degrade the performance of the network.

IV. METHODOLOGY

In this paper, we are planning to discover the flooding nodes; it is a kind of denial of service (DoS) attack. Such type of attack consumes more bandwidth, increase congestion and also decrease the resource utilization of the network. We will apply some security techniques which can effectively detect such kind of nodes and the simulation analysis of the proposed methodology will be done in well known network simulator NS2.34. For comparing of simulated result will use standard performance measuring parameters that are: Throughput, PDR (packet delivery ratio), average end to end delay, normalized routing load etc. and in the anticipated approach we will categorize the most useable path and bottleneck node, then provide security for that node by using some security mechanism as well as sustain run time dynamic buffer.

Flooding Mechanism

Basically it is categorized in 3 main parts based on information that is stored in the nodes when flooding takes place. [3]

1. No need of neighbor information
2. 1-hop neighbor information
3. 2-hop neighbor information

A. No need of neighbor information [1]

As name implies itself, in this mechanisms, flooding does not look into neighbor node information it merely broadcasts control packets to its associated node and associated node send message to their immediate node in the wireless network.

1) Pure Flooding

Blind flooding also acknowledged as Pure flooding, in which all the nodes retransmits the received message when it receives it for the first time starting at the source node.

2) Probabilistic flooding scheme(PFS)

Basic conception of PFS is each node forwards message with probability P on receiving it for first time. If P=1, its representing pure flooding. So when node receiving RREQ(route request) packet, it retransmit with probability Prt and with probability (1-Prt) it decline the packet.

B. 1-hop neighbor node information [1]

1-hop neighbor node information has 5 different version of method to use it which is mentioned below.

1) Flooding with self-pruning(FSP)

FSP is simplest receiver-based flooding schemed anticipated by Lim and Kim [4]. Sender sent a message by attaching its entire 1-hop neighbor. A receiver compares with node list message of its own 1-hop neighbor. If node is in the list, then doing nothing otherwise forwards the message to sender.

2) Edge forwarding

Edge forwarding tries to decrease flooding traffic by borrowing location knowledge so that broadcast

retransmission is restricted to nodes near the boundary of each.

3) Vertex forwarding

Vertex forwarding flooding schemes [5], which minimizes the flooding traffic by borrowing location knowledge of 1-hop neighbor nodes.

4) Efficient Flooding based on 1-hop Information(EF1)

It is a 1-hop neighbor information schemes which is simple to execute and light-weight in overhead [6]. In EF1, assume the network is linked and characterize it in graph form where each node has same transmission range. EF1 scheme divides into 3 parts: 1) forwarding node selection- node select subset 2) forwarding node optimization- by removing already covered node 3) Mobility handling - response on topology change.

5) Comprehensive Efficient Flooding (CEF)

CEF [7] is optimizing routine by utilizing directional antenna over the Efficient Flooding Algorithm Using Directional Antennas (EFDA) [8]. CEF improves upon EF1, in that the optimized forwarding node selection algorithm in EF1 is customized, and held boundary combine algorithm and forwarding node selection algorithm which is executed in EF1 unchanged.

C. 2-hop neighbor node information [1]

In this scheme, each node has the information about the 2-hop neighbors. To receive the information of 2-hop neighbors, one way is each node attaches the inventory of it's their neighbors, while sending its HELLO messages. Simply it calculates 1-hop and 2-hop neighbor sets. Once a node has the information of its 1-hop and 2-hop neighbor sets, it can pick a bare minimum number of 1-hop neighbors that covers all its 2-hop neighbors.

1) Selecting the Multipoint Relay (MPR) [1]

In this scheme, MRP is to lessen the overhead of flooding by dropping superfluous retransmission. Each node select set of nodes which may retransmit its message, selected node referred as "Multipoint Relay". Technique begin with select a bare minimum number of 1-hop neighbors whose coverage areas covers all its 2-hop neighbors.

2) Connecting Dominating Set (CDS) [1]

A dominating set (DS) can be said as a subset of all the nodes which either in the set or at least one neighbor in the set. Routing in MANET's can be done competently via CDS.

Parameters

- *Throughput:*

Network throughput is the rate of successful message delivery over a communication channel.
Throughput = packet sent/ total data
Total data = packet sent + packet lost

- *Packet Delivery ratio:*

The ratio of packets that are effectively delivered to a destination compared to the total number of packets sent.
Packet Delay Ratio = ∑ Number of packet receive / ∑ Number of packet send

- Packet Loss:

Aggregate number of parcels dropped amid the during the transition.
Packet lost = Number of packet send – Number of packet received.

- Network load:

The total traffic on the network which includes the outgoing and incoming packets both.

- End to End delay:

End to end delay time comprises all the delay taken by router to seek out the path in network utilization, proliferation postponement, handling defer and End to end delay for parcel p. [10]
End to end delay = start time - end time

TYPE OF ATTACKS IN NETWORK

- *PASSIVE ATTACKS*

Passive attacks don't mean to upset the operation of the specific system; it means they do tend to modify the packets. Different types of passive attacks are as follows:

- Traffic Monitoring
- Eavesdropping
- Traffic Analysis
- SYN flooding [9]

- *ACTIVE ATTACKS*

An active attack causes modification of data stream or formation of false stream. They have the capacity to adjust the ordinary system operation. Following are the various types of active attacks:

1. Wormhole attack
2. Black hole attack
3. Rushing attack
4. Location disclosure attack
5. Flooding attack
6. Replay attack[9]
7. Sinkhole attack
8. Spoofing

Some well-known fabrication attacks are described here:
1) Black hole attacks: A black hole is a malicious node that mistakenly answers for course asks for without

having a dynamic course to the destination. It misuses the steering convention to promote itself as having a decent and legitimate way to a destination hub. It tries to turn into some piece of a dynamic course, if there is a possibility. It has terrible proposition of upsetting information bundles being sent to the destination hub or hindering the course revelation process

2) Gray hole attacks: A gray hole may forward all parcels to guaranteed hubs yet may drop bundles originating from or bound to exact hubs. In other kind of assault, hub may carry on malignantly for quite a while however later on it carries on totally typical. Now and again, a hub may combine the conduct of assaults talked about above. Because of this vagueness in conduct of dim gap, this sort of assaults is all the harder when contrasted with black hole attack.

3) Wormhole attacks: In this type of attacks, the assailant disturbs directing by short-circuiting the standard stream of steering parcels. Wormhole attacks could be possible with one hub moreover. In any case for the most part, two or more assailants unite by means of a connection called "wormhole join". They limit parcels toward one side and replay them at the flip side utilizing private high velocity system. Wormhole assaults are similarly simple to send yet may bring about awesome harm to the system.

4) Flooding Attack in AODV: In flooding attacks [2], an attacker tries to drain the network resources, for example bandwidth and to devour a node's resources e.g. computational and battery power or to interrupt the routing operation to cause severe deprivation in network performance. These attacks may also leads towards the failure of the whole network. [10]

V. EXPECTED OUTCOMES

Flooding attack degrade the performance of the network interfaces, buffer, RREQ packet and network life time also but there is some technique which is able to detect it and helps to increase the network life time and performance but it decreases the battery efficiency and utilization of resources. So in my work, develop the technique which helps to increase the battery lifetime and proper use of resources which leads to the increase in the efficiency by decreasing the load of the network.

VI. CONCLUSION

Wireless ad hoc network has dynamic topology and self configuring network, due to these features it is more susceptible to security attacks flooding attack is in one of them. In this presents the literature for the prevention of flooding attack and scrutinize that the methods are capable to protect the network, it too increases the network life time and performance but it decreases the battery efficiency and utilization of resources. So in future work, develop such technique which helps to boost the battery lifetime and proper consumption of the network resources. Thus routing in MANET has to be dependable and accurate, most important it has to be secure so that any malicious node cannot affect the security and performance of network. Also regarding some other issues like power consumption, bandwidth utilization etc. There are other numbers of concerns which are very difficult to combine with MANET.

REFERENCES

[1] Ashwin G. Raiyani and Prof. Amit M. Lathigara "Probabilistic and Neighbor Knowledge based flooding mechanism for AODV",2014 Fourth International Conference on Advanced Computing & Communication Technologies.

[2] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, Pathik Shah, Madhvi Sadhwani, "AODVSEC: A Novel Approach to Secure Ad hoc On Demand Distance Vector (AODV) Routing Protocol from insider attacks in MANETs", International Journal of Computer Networks & Communications (IJCNC), Vol. 4 No. 4, 2012.

[3] Ashwin G. Raiyani, Amit M. Lathigara "Probabilistic and Neighbor Knowledge based flooding mechanism for AODV", 2014 Fourth International Conference on Advanced Computing & Communication Technologies. In proceeding of IEEE explore.

[4] H. Lim and C. Kim, "Multicast Tree Construction and Flooding in Wireless Ad Hoc Networks," In Proc. of the ACM Int'l Workshop on Modeling, Analysis and Simulation of Wireless and Mobile System (MSWIM), pp 61-68, Aug. 2000.

[5] Xinxin Liu, Xiaohua Jia, Hai Liu, and Li Feng, "A Location Aided Flooding Protocol for Wireless Ad Hoc Networks", MSN 2007, LNCS 4864, pp.302-313, 2007.

[6] Hai Liu, Pengjun Wan, Xiaohua Jia, Xinxin Liu and Frances Yao, "Efficient Flooding Scheme Based on 1-hop Information in Ad Hoc Networks", in proceedings IEEE infocom, Communications Society subject, 2006.

[7] Xianlong Jiao, Xiaodong Wang, and Xingming Zhou, "A comprehensive Efficient Flooding Algorithm Using Directional Antennas for Mobile Ad Hoc Networks", APPT 2007, LNCS 4847, pp.525-534, 2007.

[8] X. Jiao, X. Wang, X. Zhou, "Efficient Flooding for Wireless Ad Hoc Networks with Directional Antennas" In: Proceedings of ISCIT, 2007.

[9] "Performance Evaluation of AODV routing Protocol under Black Hole attack with varying Black hole nodes", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

[10] Rajiv Misra and C.R. Mandal, "Performance Comparison of ADOV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation".

[11] Bin Xia et al "An Active Detecting Method Against SYN Flooding Attack", The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, Computer School, Wuhan University, Wuhan 430072, Hubei, China.

[12] Bhuvaneshwari .k1,et al,"Profile based Detection Scheme for flooding attack in AODV based MANET", 1Scholar, Department of Information Science Engineering Oxford College of Engineering, Bangalore, India.

[13] Ruchita Meher,et al" Review Paper on Flooding Attack in MANET", Computer engineering, MGMCET kamothe Navi Mumbai, India.

[14] Karthik Lakshminarayanan et al," Taming IP Packet Flooding Attacks", UC Berkeley.
[15] Ms. Neetu Singh Chouhan et al," Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering (IJCTEE).
[16] Madhavi, S.et al," FLOODING ATTACK AWARE SECURE AODV", Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Namakkal, Tamil Nadu, India.
[17] Dimitris Geneiatakis*et al," Utilizing bloom filters for detecting flooding attacks against SIP based services", Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR-83200 Samos, Greece.
[18] Mohamed A.et al," Resisting Flooding Attacks on AODV", School of Mathematical & Computer Sciences Heriot-Watt University, Edinburgh, UK.
[19] Gaurav Sharma* et al," Congestion Control in Adhoc Network", SKIET, Kurukshetra University SKIET,Kurushetra,University Kurukshetra, India.
[20] Bhuvaneshwari. K et al," Examination of Impact of Flooding attack onMANET and to accentuate on Performance Degradation", Scholar, Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India.