Survey of Detection and Prevention Mechanism for Flooding Attacks in MANETs

Er. Nitin Mohil[1], Ms. Kanta Dhankhar[2]

[1]ECE Department, ISTK, Kurukshetra University Kurukshetra, Haryana, INDIA
[2]CSE Department, ISTK, Kurukshetra University Kurukshetra, Haryana, INDIA
Email: mohil73.nitin@gmail.com[1], Kanta.dhankhar@gmail.com[2]

Abstract-Today MANETs has reached to its pinnacle, as the demand for the MANETs are increasing day by day, due to the increasing demand for MANETs in various areas such as in Military operations, in flood affected areas etc., threat of security has also increased. MANETs has no protection from harms, so information can be accessed by both authorized network users and catty attackers because MANETs don't have centralized administration. In the presence of catty nodes, the main problem in MANETs is to design the rich security solution that can protect MANETs from various routing attacks. Flooding attack is kind of the security threat in which source node sends huge amount of data, Root request (RREQ) and Sync packet to destination node, then receiver will be engaged in receiving the excessive amount of Data, RREQ and Sync packets from the attacker and cannot work properly. In this paper a survey of Different mechanisms to detect and prevent the Flooding attacks in MANETs is proposed.

Index Terms- MANETs, Attacks, Detection, Prevention.

1. INTRODUCTION

Mobile Adhoc networks are special purpose network created by set of dynamic wireless nodes which can transfer information by hop or multi hop through any intermediate node using dynamic routing through temporary network design for special purpose.

Most mobile devices use radio or infrared frequencies for their communications which leads to a very limited transmission range. Usually the transmission range is increased by using multi-hop routing paths. In that case a device sends its packets to its neighbour devices, i.e. devices that are in transmission range.

Ad-hoc networks are temporary networks because they are formed to fulfil a special purpose and cease to exist after fulfilling this purpose. Mobile devices might arbitrarily join or leave the network at any time, thus ad hoc networks have a dynamic infrastructure.

To achieve the ambitious goal of providing ubiquitous connectivity, ad hoc networks have special properties that distinguish them from other networks. The properties of MANETs have been discussed **[5]** in the following.

- **Dynamic topologies**

Nodes are free to move arbitrarily; thus, the network topology—which is typically multi-hop—may change randomly and rapidly at unpredictable times. Adjustment of transmission and reception parameters such as power may also impact the topology.

- **Bandwidth-constrained**

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently.

- **Power-constrained operation**

Some or all of the nodes in a MANET may rely on batteries for their energy. For these nodes, the most important system design criteria for optimization may be that of power conservation.

- **Limited physical security**

Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired nets. Existing link security techniques are often applied within wireless networks to reduce security threats.

The whole paper comprises of six sections, the 1st section provides the introduction, 2nd section provides the information about the different routing protocols such as Ad-hoc on demand distance vector (AODV) and Optimized link state routing (OLSR) protocols etc., 3rd section provides the overview to the different types of Routing attacks in the MANETs and brief introduction to the flooding attack, 4th section provides the information regarding the different detection schemes for MANETs routing attacks, the 5th section provides the information regarding the different prevention schemes for MANETs routing attacks and the 6th section provides conclusion to the whole paper.

2. ROUTING PROTOCOLS

A Routing Protocols is a touch stone that control how nodes determine which way is chosen to send packets between computing devices in MANETs. Basically there are two types of Routing Protocols Proactive or table driven which are DSDV, OLSR and reactive or on demand which are AODV, DSR.

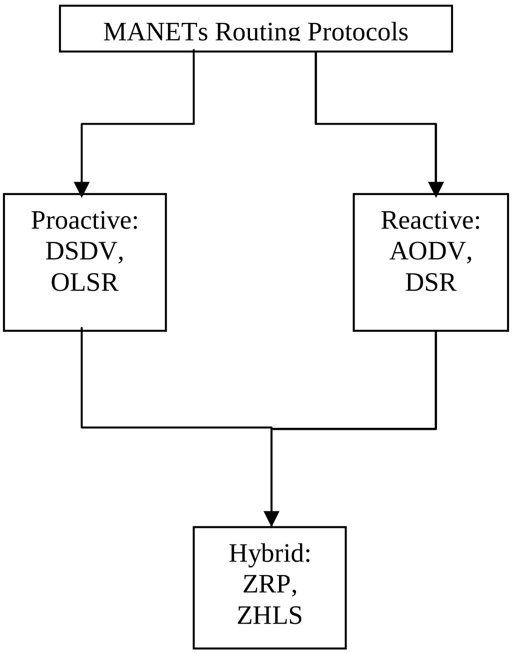

Fig.1. MANETs Routing Protocols

Reactive protocols [12] invoke a route determination procedure on demand only. Thus, when a route is needed, some sort of global search procedure is employed. The family of classical flooding algorithms belong to the reactive group.

The advantage of the proactive schemes is that, once a route is needed, there is little delay until the route is determined. In reactive protocols, because route information may not be available at the time a datagram is received, the delay to determine a route can be quite significant. Furthermore, the global flood-search procedure of the reactive protocols requires significant control traffic. Because of this long delay and excessive control traffic, pure reactive routing protocols may not be applicable to real-time communication. However, pure proactive schemes are likewise not appropriate for the ad hoc networking environment, as they continuously use a large portion of the network capacity to keep the routing information current.

There exist another one protocol which having the properties of both Proactive and active protocols is called Hybrid protocol (ZRP).

Since nodes in an ad hoc network move quite fast, and as the changes may be more frequent than the route requests, most of this routing information is never even used! This results in a further waste of the wireless network capacity. What is needed is a protocol that, on one hand, initiates the route determination procedure on-demand, but at limited search cost. The protocol described in this draft, termed the "Zone Routing Protocol (ZRP)".

2.1. *AODV (Ad-hoc on demand protocol)*

Ad-hoc on-demand Distance Vector routing protocol [9] uses on-demand route discovery technique to ensure loop free, single path, hop by hop distance vector routing. AODV operates in two sub phases. Route discovery Phase is initiated by a source node not having valid route to a destination node to which it wants to send data. Route maintenance phase for handling dynamic topology in MANET changes as the node moves or when some error persists. When a node wishes to send data to some destination it floods Route Request (RREQ) messages to all its neighbouring nodes. An intermediate node receiving RREQ updates its routing table with reverse route entry to the source node if RREQ is unique. Source id and broadcast id determines uniqueness of a RREQ packet. An intermediate node can further rebroadcasts RREQ to its neighbours or unicasts RREP message back to the source node if it already has unexpired route to that destination in its routing table otherwise destination node replies.

In AODV, a node can receive multiple RREP messages for one route discovery message sent but it maintains only one entry per destination in its routing table. An intermediate node always forwards first RREP message received after making entry for forward path towards destination in its routing table and second RREP for a particular RREQ is used for updating table and forwarded only if RREP has higher destination sequence number for the destination or hop count is smaller in case of same destination sequence number otherwise RREPs are suppressed. Higher sequence number ensures fresher route. HELLO messages are exchanged for maintaining neighbourhood connectivity.

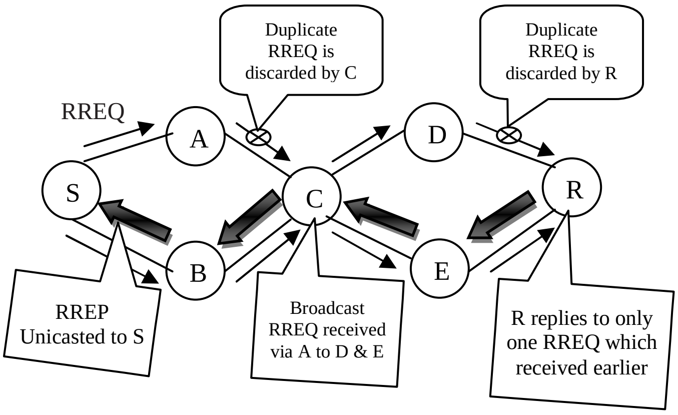
Duplicate RREQ is discarded by C
Duplicate RREQ is discarded by R
RREQ
A
D
S
C
R
B
E
RREP Unicasted to S
Broadcast RREQ received via A to D & E
R replies to only one RREQ which received earlier

Fig.2. AODV Route discovery

In Fig. 2, source node S initiates route discovery message broadcasting to node A and B. Node C discards duplicate RREQ and further rebroadcasts RREQ received from B to node E and D. Destination node R replies to first RREQ received from E and discards duplicate RREQ by D. So reply is unicasted back to source node and each node maintains single path both in forward and reverse direction.

The routing table entry corresponds to fields as shown in Fig-3. AODV uses a timer-based technique to remove stale routes. Each routing entry is associated with a lifetime of a route known as route expiration timeout. This timer is refreshed whenever a route is used.

Destination ID	Sequence Number	Hop count	Lifetime of a route	Next hop

Fig.3. Routing Table Entry in AODV

Once a route is established between source and destination nodes it is maintained in routing table as long as source needs this route for data transfer and timer does not expires. Whenever a source node moves during active session of data transfer a new route discovery process is initiated and if an intermediate or destination node moves or a link break, RERR message including lists of unreachable destinations along with their sequence numbers is broadcasted back to source node. Each node upon receiving a RERR message from a downstream neighbour and using failed link must invalidate the route and source node reinitiates new route discovery. RERR message is rebroadcasted if at least one destination becomes unreachable.

2.2. *OLSR (Optimized Link State Routing)*

OLSR [7] is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs, to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes.

Also, OLSR does not require sequenced delivery of messages. Each control message contains a sequence number which is incremented for each message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission.

2.3. *ZRP (Zone Routing Protocol)*

Zone Routing Protocol (ZRP) is a hybrid routing protocol suitable for a wide variety of mobile ad-hoc networks, especially those with large network spans and diverse mobility patterns. Each node proactively maintains routes within a local region (referred to as the routing zone). Knowledge of the routing zone topology is leveraged by the ZRP to improve the efficiency of a globally reactive route query/reply mechanism. The proactive maintenance of routing zones also helps improve the quality of discovered routes.

In the Zone Routing protocol, a proactive routing protocol provides a detailed and fresh view of each node's surrounding local topology (routing zone) at the local level. The knowledge of local topology is used to support services such as proactive route maintenance, unidirectional link discovery and guided message distribution. One particular message distribution service, called border casting, directs queries throughout the network across overlapping routing zones. Border casting is used in place of traditional broadcasting to improve the efficiency of a global reactive routing protocol.

The benefits provided by routing zones, compared with the overhead of proactively tracking routing zone topology, determine the optimal framework configuration. As network conditions change, the framework can be dynamically reconfigured through adjustment of each node's routing zone

3. MANETs ROUTIMG ATTACKS

MANET is a collection of mobile nodes, sometimes nodes in MANET can be bad or malicious and these bad nodes cannot forward the packets due to their aim of conserving network resources such as band width, battery etc. by the denial of service.

There are mainly two types of attacks in MANET Active and Passive [1].

3.1. *Active Attacks*

In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks (as compared to passive attacks) disturb the operations of the network and can be so severe that they can bring down the entire network or degrade the network performance significantly, as in the case of denial of service attacks.

3.2. *Passive Attacks*

Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. This in turn can lead to the disclosure of critical information about the network or nodes such as the network topology, the location of nodes or the identity of important nodes.

Active and passive attacks are further classified as shown in Fig. 4.

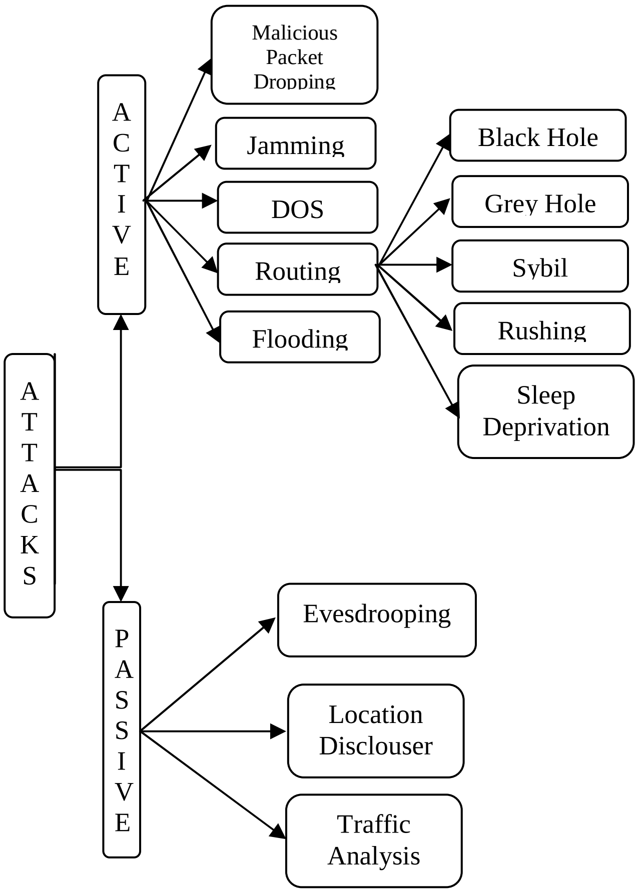

Fig.4. MANET Routing Attacks

3.1.1. *Flooding Attacks*

It is a type of active attack in which source node sends large amount of data, Root request (RREQ) and Sync packet to destination node, destination node will then be engaged in receiving the excessive Data, RREQ and Sync packets from the attacker and cannot work properly.

3.1.1.1 *Root Request (RREQ) Flooding*

The aim of the Root Request Flooding attack [3] is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. In the authors show that a flooding attacks can decrease throughput by 84 percent.

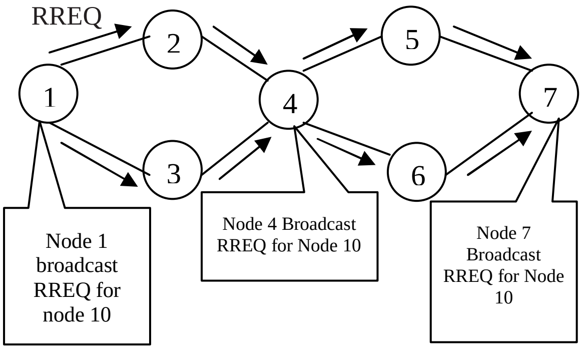
RREQ
1
2
3
4
5
6
7
Node 1 broadcast RREQ for node 10
Node 4 Broadcast RREQ for Node 10
Node 7 Broadcast RREQ for Node 10

Fig.5. RREQ Flooding Attack

In RREQ Flooding Attack attacker node will broadcast RREQ packet with fake destination address or non-existing node in the network as shown in Fig 5 here node 1 is attacker node and it will flood the network with non-existing node in the network which is node 10.

3.1.1.2 *Data Flooding Attack*

When nodes in MANETs find the correct routing path, source nodes send the data packets through that route. In data flooding attack [2], the attacker first maintains the routes to destination node, then sends frequently the useless data packets. The destination node will then be engaged in receiving the excessive data packets from the attacker and cannot work properly. The attacker packets engage the network and stop the processing of legitimate data packets.

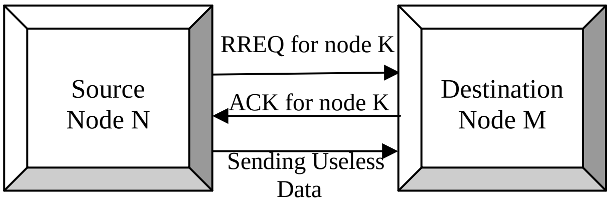

Fig.6. Data Flooding Attack

In Data flooding firstly source node sending root request to destination when it receive acknowledgment for route to destination after that source or attacker will flood the network by sending excessive amount of data packets to destination as shown in Fig 6.

3.1.1.3 *Sync Flooding*

In Sync Flooding [10] a malicious node sends a huge number of SYNC packets to a destination node. The destination node sends back SYNC+ACK packets and keeps the entry for the incomplete connection request. The attacker never sends ACK so a large amount of memory of victim node is consumed for storing pending requests and node may come to a halt even.

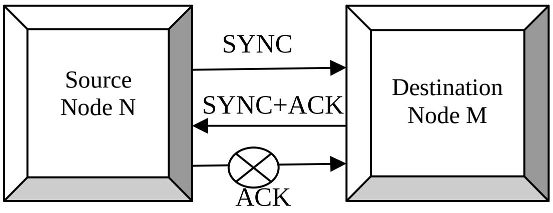

Fig.7. Sync Flooding Attack

4. DETECTION SCHEMES FOR FLOODING ATTACKS

In this section different detection methods to find out the attacks in the network will be discussed. These schemes or methods use to defend network from malicious activities or attacks. With the help of these methods, the incorrect or malicious activities in the network can be detected. Detection schemes basically involves monitoring the network resources for collecting audit data (set of data of the network regarding user activities or network events) with the help of this audit data attacks can be detected. These detection schemes [1] can be categorize in to three categories

I) Misuse Detection or Knowledge Based Intrusion Detection.
II) Anomaly Based or Behavior Based Intrusion Detection.
III) Specification Based Intrusion Detection.

4.1. *Knowledge Based Intrusion Detection*

This type of system maintains information data base that contains information about well-known attacks. In this scheme current data from the network is taken and compared with the data stored in information data base (which contains information about different attacks). If the current data is matched with any of data stored in information data base then it will generate message that attack is recognize otherwise it consider it as unknown attack and it will update new information regarding unknown attack in Information data base as shown in Fig 8.

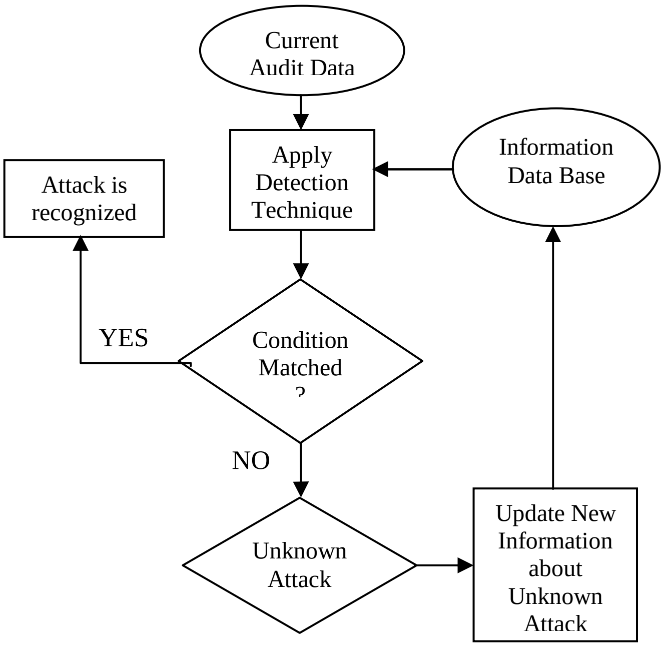

Fig.8. Knowledge Based Intrusion Detection Process

4.2. *Anomaly Based Intrusion Detection*

This type of system monitors the activities which are different from normal activities. These systems are also called Behavior Based Intrusion Detection, in this scheme information is collected about the normal behavior of the network then this collected data is compared with current audit data taken from the network to detect the attack.

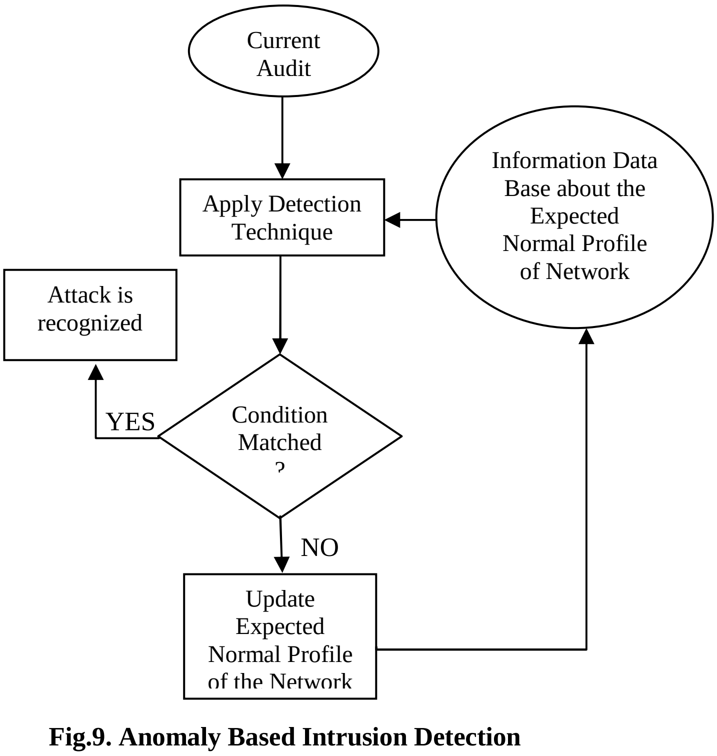

Fig.9. Anomaly Based Intrusion Detection Process

If the current audit data is match with information stored in data base about the behavior of the network then it will generate alert for attack otherwise if there is a deviation between current audit data and expected profile data then it will update expected normal profile of the network as shown in Fig. 9.

4.3 Specification Based Intrusion Detection

In this type of detection system [4][7] firstly set of specification as information data base is define and then these set of specifications are used to monitor Routing protocol operation or network layer operation to detect Attack in the network.

In this approach system observe the behavior of individual nodes and generate alert if a node violate the behavioral specifications. This detection scheme can detect all types of attacks whether it is known or unknown for system.

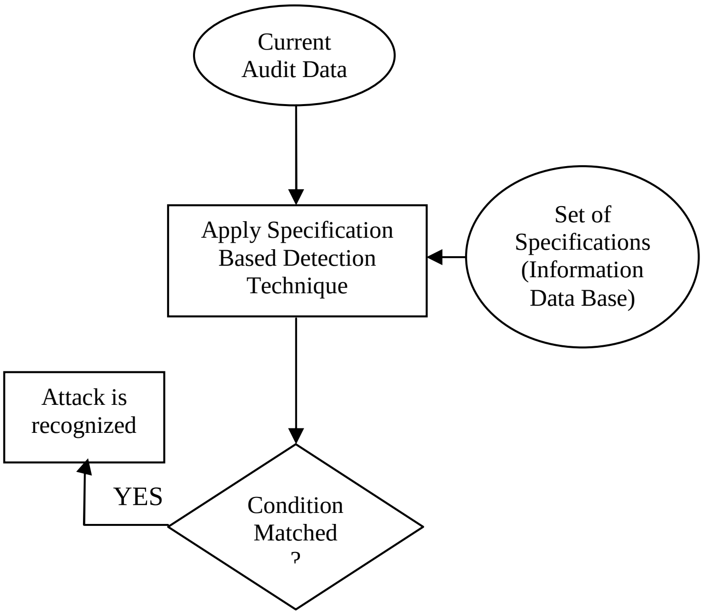
Current Audit Data
Set of Specifications (Information Data Base)
Apply Specification Based Detection Technique
Attack is recognized
YES
Condition Matched ?

Fig.10. Specification Based Intrusion Detection Process

5. PREVENTION SCHEMES FOR FLOODING ATTACKS

There are several methods available to prevent the Flooding attacks in MANETs (Mobile Ad-hoc Networks).

5.1 In [3] author proposed a new prevention scheme for the flooding attack in MANETs; in which each node maintain a count table for rate of RREQ of its neighboring nodes. If the rate of RREQ is more than predefined threshold value then the ID of that neighbor is blacklisted, but the limitation of this scheme is that it cannot prevent the attack in which rate of RREQ is below threshold.

5.3 In [11] author proposed an Adaptive technique for the flooding attack. It basically works on the statistical analysis to detect malicious RREQ flood and prevent forwarding of such packet. In this approach node maintain a count table for rate of RREQ of its neighboring nodes. If the rate of RREQ is more than predefined threshold value then the ID of that neighbor is blacklisted same as [6] , but in this method threshold is determine on the bases of statistical analysis of RREQ Floods. The main advantage of this approach is that it can also prevent flooding attacks with varying rates.

5.4 In [2] author proposed a new defense scheme against the RREQ flooding attack. Basically RREQ flooding attacker will not obey the binary exponential back off, which is normally obey by the RREQ of AODV scheme. In this scheme firstly each neighboring node is checked whether it obey binary back off for time to wait for RREP or not. Which node do not follow this criterion is identified as suspicious node and secondly rate of RREQ is checked, in this scheme two threshold values are used RREQ_RATELIMIT is considered as 1st threshold and other is (RREQ_RATELIMIT)/2 is considered as 2nd threshold. If the rate of RREQ is less than 1st threshold then the node is identified as normal node, if the rate of RREQ is lies in between 1st and 2nd threshold then the node is identified as suspicious node and add to delay queue. If the rate of RREQ is above the 2nd threshold then the node is identified as Attacker and ID of that node is broadcasted to all neighboring nodes.

5.4 In [4] author proposed a new mechanism to prevent RREQ flooding attack the author of proposed an Effective Filtering scheme against RREQ flooding attack; this scheme can detect the malicious nodes and attacker nodes, which are disturbing the network communication.

In this scheme there are two thresholds 1) RATE_NM and 2) BLACKLIST_NM, which are used to limit the RREQ message.

Here RATE_NM parameter denotes no. of RREQ that can be accepted and processed. Here each node monitors the RREQ and maintain a count table for RREQ received. Whenever a RREQ request is received a condition check is performed, if the rate of received RREQ is less than the RATE_NM then received RREQ processed normal otherwise a second condition check is performed, where received RREQ is compared with another threshold BLACKLIST_NM, if the rate of RREQ is greater than the BLACKLIST_NM then it is assume that particular node trying to flood the network with fake RREQ messages otherwise the received RREQ is add to delay queue. After identification of sender node as malicious node it will be blacklisted. The malicious node is blocked for a time period given by BLACKLIST_TIMOUT_NM after if black list time out it will be unblocked.

After adding malicious node to blacklist all the neighboring nodes of malicious node now free to entertain RREQ from other genuine nodes, if the received RREQ has rate in between RATE_NM and BLACKLIST_NM then this will de add to delay queue by doing so the node which has high attack rate will be delayed.

5.5 In [6] author proposed a new prevention scheme for RREQ flooding attack. In this scheme all nodes are categorize as Friend, Acquaintance and stranger depending upon relationship (trust level) with their neighboring nodes. Initially all nodes are stranger to each other , the trust level is a function of many parameters such as ratio of no. of packet forwarded successfully to the neighbor to the total no. of packet sent to the neighbor, average time taken to respond to a route request etc.

According to the trust level neighbors are categorize as Friend (Most trusted), Acquaintance (trusted) and stranger (not trusted).

Here the threshold trust level for stranger to become an acquaintance is represented as T_{acq} and threshold trust level for an Acquaintance to become Friend is denoted by T_{fri}.

1. If T > = T_{fr}i then node is considered as Friend node,
2. If T_{acq} < =T < T_{fri} then node is considered as Acquaintance node,
3. If 0< T <T_{acq} then node is considered as Stranger node.

To prevent RREQ flooding attack the threshold level is set for the max. no. of RREQ node can receive from its neighbors, If specified level of threshold is reached further RREQ from nodes are dropped or blacklisted.

6. CONCLUSION

MANET's are the most promising field of research but there are always security threats from attacker due to their characteristics and absence of centralized administration. This paper provides a survey of various types of Flooding attacks, their Detection and Prevention Mechanisms. Hopefully the survey presented in this paper will be helpful in designing more secure detection and prevention schemes for flooding attacks.

REFERENCES

[1] Adnan Nadeem member IEEE and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks",Communication survey & Tutorials, IEEE Volume: 15, Issue: 4, 2013.

[2] Arunmozhi Annamlai, Venkataramani Yegnanarayan, "Secured System against DDoS Attack in Mobile Adhoc Network", WSEAS Transaction on Communication Issue 9, Volume 11, September 2012.

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, "A Survy of Routing Attacks in Mobile Ad hoc Network," IEEE Wireless Communications • October 2007.

[4] Jian-Hua Song, , Fan Hong, Yu Zhang, "Effective filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", IEEE Computer Society 2006.

[5] Joseph P. Macker, a M. Scott Corsonb, "Mobile Ad Hoc Networking and the IETF", Mobile Computing and Communications Review, Volume 2, Number 1, January 1998.

[6] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", World Academy of Science, Engineering and Technology 32, 2009.

[7] T. Clausen, P. Jacquet, " Optimized Link State Routing Protocol (OLSR)", IETF October 2003.

[8] Tao Song, Calvin Ko, Chinyang Henry Tseng, Poornima Balasubramanyam, Anant Chaudhary, and Karl N. Levitt "Formal Reasoning About a Specification-Based Intrusion Detection for Dynamic Auto-configuration Protocols in Ad Hoc Networks", Springer-Verlag Berlin Heidelberg LNCS 3866, pp. 16 – 33,2006.

[9] Tarunpreet Bhatia, A. K. Verma, "Simulation and Comparative Analysis of Single Path and Multipath Routing Protocol for MANET," ANVESHANAM - THE JOURNAL OF COMPUTER SCIENCE & APPLICATIONS, VOL. II, NO. 1, AUGUST 2013-JULY 2014.

[10] Tarunpreet Bhatia and A.K. Verma, "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms," IJARCSSE,Volume 3, Issue 6, June 2013.

[11] Saman Desilva Rajendra V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks", IEEE Wireless Communications and Networking Conference, March 2005.

[12] Zygmunt J. Haas, Marc R. Pearlman,PrinceSamar, "Zone Routing Protocol", IETF July 2002.