International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Analysis Of Techniques For Mitigating Dos Attacks In MANET

Pooja
M.Tech (cse)
Manav Rachna International University
Faridabaad, India.

Dr. S. S. Tyagi
H.O.D(cse)
Manav Rachna International University
Faridabaad, India.

***Abstract*—A Mobile Ad-hoc network is a collection of mobile nodes that can be deployed without any centralized management infrastructure. Its operation depends on the cooperation among nodes to provide connectivity and communication routes. In non-ideal situation some nodes behaves in malicious manner, which degrades the performance of the network. Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. In mobile ad-hoc networks, by attacking the corresponding routing protocol, an attacker can easily disturb the operations of the network. In this paper we investigate the vulnerability of MANETs to DoS attacks and provide countermeasures of DoS attacks in MANET.**

***Keywords*— MANET, Security, AODV, Routing Attacks, DoS.**

I. INTRODUCTION TO MANET

In last few years mobile ad-hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. MANETs are multi hop wireless networks that do not require any central administration or existing infrastructure. MANET is self organized in nature so it has rapidly deployable capability. MANET is very useful to apply in different applications such as battlefield communication, emergency relief scenario etc.

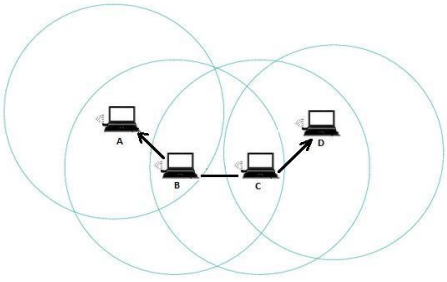

Fig. 1. Mobile Ad-Hoc Network

In MANET nodes are mobile in nature, due to the mobility, topology changes dynamically[1], which gives rise to a wide range of characteristics such as transient links, unpredictable resource availability and complex route maintenance. Challenges of MANET include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. In addition, nodes in MANETs have limited battery life, which is expended by packet transmission and reception[2]. Although security threats exist in both wired and wireless networks, the inherent nature of wireless networks such as MANETs results in them being more vulnerable to attacks. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad-hoc routing protocols, such as Ad-hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), and wireless MAC protocols, such as 802.11, typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

II. SECURITY GOALS FOR MANET

The ultimate goal of the security solutions for MANET is to provide a framework covering [23] availability, confidentially, integrity, and authentication to insure the services to the mobile user. A short explanation about these terms:-

A. Availability

Services of network should be available to authenticated users. There should be certain mechanism for protection against such kind of attacks, which makes the network resources to unavailable to authorized users like in case of DOS (Denial of service attack) attack, the availability of network and its resources would become unavailable to authenticated user .

B. Confidentiality

Protection of information which is exchanging through a MANET should be protected against any disclosure attack like eavesdropping- unauthorized reading of message and traffic analysis- done by a attacker node to find out which types of communication

is going on, like in case of war areas it becomes essential to protect and secure such kind of communication. In MANET it is very difficult to achieve the confidentiality because of intermediate nodes routing, which can easily listen the information which is being routed through them.

C. *Integrity*

The information which is transmitted should be protected against any alteration. Protection against message modification should be there.

D. *Authentication*

The resources of network should be accessed by the authenticated nodes. Some of the authentication techniques are:-

- Digital Signature: The sender node signs the message digitally which will later verify by the receiver node digitally.
- Non repudiation: Ensures that sending and receiving parties can never deny every sending & receiving of message.

III. TYPES OF SECURITY ATTACKS

A. *Passive Attacks*

In passive attack there is not any alteration in the message which is transmitted. There is an attacker (intermediated node) between sender & receiver which reads the message. This intermediate attacker node is also doing the task of network monitoring to analyze which type of communication is going on.

B. *Active Attacks*

The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also forward the RREQ (route request) though it is not an authenticated node therefore bandwidth is consumed and network is jammed by it.

IV. ROUTING ATTACKS IN MANET

There are basically two approaches to protecting MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats *a posteriori* and react accordingly.

A. *Ad-hoc On-Demand Distance Vector (AODV) Routing*

The AODV[4],[5] routing protocol shares DSR‟s on-demand characteristics in that it also discovers routes on an “as needed” basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, with one entry per destination. This is a departure from DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a route reply back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. These sequence numbers are carried by all routing packets. When a route is needed, a node broadcasts a route request message. The response message is then echoed back once the request message reaches the destination or an intermediate node finds a fresh route to the destination. For each route, a node also maintains a list of those neighbors actively using the route. A link breakage causes immediate link failure notifications to be sent to the affected neighbors. Similar to DSDV, each route table entry is tagged with a destination sequence number to avoid loop formation. Moreover, nodes are not required to maintain routes that are not active. Thus, wireless resources can be effectively utilized. However, because flooding is used for route search, communication overhead for route search is not scalable for large networks. As route maintenance considers only the link breakage and ignores the link creation, the route may become non optimal when network topology changes. Subsequent global route search is needed when the route is broken. An important feature of AODV is maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry expires if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes that use that entry to route data packets. These nodes are notified with route error packets when the next hop link breaks. Each predecessor node, in turn, forwards the route error to its own set of predecessors, thus effectively erasing all routes using the broken link.

The specification of AODV includes an optimization technique to control the RREQ flood in the route discovery process. It uses an expanding ring search initially to discover routes to an unknown destination. In the expanding ring search, increasingly larger neighborhoods are searched to find the destination. The search is controlled by the TTL field in the IP header of the route request packets. If the route to a previously known destination is needed, the prior hop-wise distance is used to optimize the search.

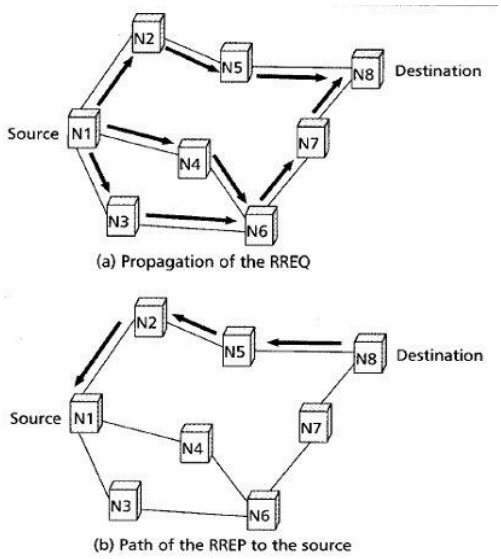

Fig 2. AODV Routing Protocol[4]

A MANET provides network connectivity between mobile nodes over potentially multi-hop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network- layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications.

The main network-layer operations in MANETs are ad-hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. The ad-hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories based on the target operation of the attacks:

- routing attacks
- packet forwarding attacks

The family of *routing attacks* refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviors are related to the routing protocol used by the MANET. For example, in the context of DSR, the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list. When distance-vector routing protocols such as AODV are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even nonexistent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case. There are still active research efforts in identifying and defeating more sophisticated and subtle routing attacks. For example, the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node. A pair of attacker nodes may create a wormhole and shortcut the normal flows between each other. In the context of on-demand ad-hoc routing protocols, the attackers may target the route maintenance process and advertise that an operational link is broken. *Packet forwarding attacks* do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded. Another type of packet forwarding attack is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET.

B. Some of the routing attacks in MANET are:

- Flooding Attack: In flooding attack, attacker exhausts the network resources such as bandwidth and to consume anode'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.

- Black Hole Attack: In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.
- Link Spoofing Attack: In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic for example, modifying or dropping the routing traffic or performing other types of DoS attacks

V. Denial Of Service

International Organization for Standardization (ISO) has given the following definition for denial of service (DoS) in the standard ISO 7498-2:1989.

Denial of service: "The prevention of authorized access to resources or the delaying of time-critical operations."

Open network architecture and shared transmission media make it possible to join a network without a physical connection. It [18]

- Attempts to "flood" a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person.

A DoS attack could be launched at any layer of ad-hoc network.

VI. Defense Mechanisms To DoS Attacks

Defense mechanisms [18] to DoS attacks are classified into two broad categories: local and global. As the name suggests, local solutions can be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions, by their very nature, require the cooperation of several Internet subnets, which typically cross company boundaries.

A. Local Solutions

Protection for individual computers falls into three areas.

- Local Filtering: The timeworn short-term solution is to try to stop the infiltrating IP packets on the local router by installing a filter to detect them. The stumbling block to his solution is that if an attack jams the victim's local network with enough traffic, it also overwhelms the local router, overloading the filtering software and rendering it inoperable.
- Changing IPs: A Band-Aid solution to a DoS attack is to change the victim computer's IP address, thereby invalidating the old address. This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address. This option is practical because the current type of DoS attack is based on IP addresses. System administrators must make a series of changes— to domain name service entries, routing table entries, and so on - to lead traffic to the new IP address. Once the IP change—which takes some time—is completed, all Internet routers will have been informed, and edge routers will drop the attacking packets.
- Creating Client Bottlenecks: The objective behind this approach is to create bottleneck processes on the zombie computers, limiting their attacking ability.

B. Global Solutions

Clearly, as DoS attacks target the deficiencies of the Internet as a whole network, local solutions to the problem become futile. Global solutions are better from a technological standpoint.

- Improving the Security of the Entire Internet: Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to break into and plant daemon programs that would turn them into zombies.
- Using Globally Coordinated Filters: The strategy here is to prevent the accumulation of a critical mass of attacking packets in time. Once filters are installed throughout the Internet, a victim can send information that it has detected an attack, and the filters can stop attacking packets earlier along the attacking path, before they aggregate to lethal proportions. This method is effective even if

the attacker has already seized enough zombie computers to pose a threat.

- Tracing the Source IP Address: The goal of this approach is to trace the intruders' path back to the zombie computers and stop their attacks or, even better, to find the original attacker and take legal actions. If tracing is done promptly enough, it can help to abort the DoS attack. Catching the attacker would deter repeat attacks. However, two attacker techniques hinder tracing; IP spoofing that uses forged source IP addresses, and The hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified. Aim of this attack is to overload the server's bandwidth and other resources.

VII. TECHNIQUES FOR MITIGATING DOS ATTACKS IN MANET

A. *Using Protection Nodes*

The authors [24] have selected a node called protection node in a network. Once a DDoS attack has been detected, the doubtful traffic will be forwarded to the protection node. The victim will function as usual and it is expected that the attacker will stop the meaningless efforts after a certain length of attacking time. For the selection of protection node, they have implemented the hierarchical network architecture in which the nodes are divided into multiple levels based on their their importance. Lower level nodes are used to protect high level nodes. In particular, each lower level node is assigned as its protection node called destination protection node or Local Protection Node (LPN). They defend the target of DoS attacks. A neighbor of the same level will be selected as protection node for the lowest level nodes. In this scheme, when an attack route is made, the node that is the first hop from the source node will be assigned as a protection node called Remote Protection Node (RPN) which monitors the attack source node. If the source node is identified as a malicious one, RPN drops the packets from this node. They have adopted three-step-handshake approach for selection of LPN by message communication.

- The higher level node sends the LPN query packet (LPNREQ) to the nodes of its neighbor lower level. Once the request is received, neighbor node's fresh tags are unset. Then consequent LPNREQ packets from other nodes will not be accepted.
- The receivers send an acknowledgement packet (LPNACK) back to the sender. This PNACK message enables that the receiver notifies the sender that it is willing to serve as the LPN; and the sequence of the LPNACK messages helps the sender make a decision. The producer of the first received LPNACK packet is selected as the LPN.
- The protected node will send an LPN confirm (LPNCFM) message. The LPN node filters all the malicious packets in the traffic whose destination is the victim. Then Attack Notification Message (ANM) is sent to the victim immediately. Next, the victim sends an Attack Information Message (AIM) to RPN. Then RPN filters all the attacking packets at source side.

The advantage of this approach is cost of overhead of the system is low and the limitation is prioritizing nodes into different level may lead to starvation to low level nodes. Also basic properties of a MANET may disrupt.

B. *Using Rate Limits for RREQ*

The authors in [8] proposed a proactive scheme that can prevent a specific kind of DoS attack and identify the misbehaving node as well as it prevent DDoS. The proposed scheme is based on the application of two parameters: RREQ_ACCEPT_LIMIT and RREQ_BLACKLIST_LIMIT.

RREQ_ACCEPT_LIMIT represents the number of RREQs that can be accepted and processed per unit time by a node. The reason of this parameter usage is to specify a value that ensures uniform usage of a node's resources by its neighbors. RREQs more than this limit is dropped, but their timestamps are recorded. This information will help in monitoring the neighbor's activities. In their simulations, three RREQs can be accepted per unit time. The RREQ_BLACKLIST_LIMIT parameter is used to specify a value which determines whether a node is acting as malicious or not.

It tracks the number of RREQs forwarded by a neighboring node per unit time. If this count exceeds the value of RREQ_BLACKLIST_LIMIT, the corresponding neighboring node is trying to flood the network with possibly fake RREQs. On identifying a neighboring node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network.

The advantage of this scheme provides a better solution than existing approaches with no extra overhead and limitation is that RREQ_ACCEPT_LIMIT and RREQ_BLACKLIST_LIMIT can be overwritten by the attacker easily.

C. *Using Exponential Backoff Mechanism*

The focus of this paper[20] centers on reactive routing protocols which established routes between communicating nodes when needed using a route discovery process involving Route Requests and Route Replies, a process which can be easily misused for denial-of-service attacks. In this paper, they described one such attack, the Route Request Flooding Attack (RRFA) targeted at reactive routing protocols used in mobile Ad-Hoc networks. Then, they proposed the Route Request Flooding Defence (RRFD) mechanism that was designed to reduce the impact of RRFA that aims to do the following:

- Minimize the impact of breadth-RRFA and depth-RRFA on the entire network.
- Identify forged RREQs to a very high accuracy
- Allow the malicious node to maintain or establish valid data communications to reachable destinations.

RRFD consists of three components:

- In RREQ binary exponential backoff, each node will ensure that its neighbour follows a binary exponential backoff when sending RREQs in a RDC. If RREQs are sent faster than what is allowed, excess RREQs are dropped. This ensures that the generation of RREQs in a RDC follows a binary exponential backoff as stated in the AODV specifications.
- In RDC binary exponential backoff, each node will ensure that its neighbor follows a binary exponential backoff when initiating another RDC.
- In Fast Recovery, the number of RDCs that a node will need to wait before initiating another RDC will be reduced exponentially if it does not initiate another RDC for at least one RDC period.

The advantage of this scheme is this it can reduce the DoS attack to half and congestion problem as well and the limitation is reduces the throughput as waiting time is increased here.

D. *Using Reputation and Score Based Scheme*

The authors in [30] proposed a reputation-based incentive mechanism for detecting and preventing DoS attacks. They investigated DoS attacks committed by selfish and malicious nodes. Their scheme encouraged nodes to cooperate and exclude them from the network, only if they fail to do so. They have adopted a combination of detection and prevention measures in their proposal. When an attacker is a mobile, traceback mechanisms can be effective in determining the attack path or attack generating domain, but inefficient in identifying the attacking host. By giving incentives to cooperating nodes and some form of penalty to non-cooperating nodes may improve the performance and make sure security in MANETs. They proposed a reputation-based scheme for motivating nodes in ad-hoc networks to prevent both active and passive DoS attacks. They investigated the effect of both selfish and malicious nodes. They did not immediately exclude misbehaving nodes. Instead they first motivated them to cooperate before excluding them. A node which becomes indifferent and act malicious continuously can be excluded from the network. If nodes do not cooperate, their reputation gradually goes down and they are finally eliminated from the network. The advantage of this scheme is packet delivery ratio is increased and the routing and communication overhead is reduced. A Limitation of this scheme is the investigation of DDoS in MANET and integrated wireless networks.

In another approach the authors [26] implemented new architecture of Detection and control of DDoS attacks in MANET. That architecture consists of Monitor, Reputation System, Trust Manager/ Co-operation system, Path Manager. Monitor gathers information about the behavior of nodes in the network. From the observation, Monitoring systems detect misbehavior like Packet dropping, Modification, Fabrication, Timing misbehavior. Reputation System is responsible for monitoring evaluation, Detection &Reaction. Trust manager acts as a Co-operation system among the nodes performing the extensive task of Alarm Count and Trust Builder. It keeps track of the incoming and outgoing ALARM messages. Trust manager sends ALARM messages to warn others regarding malicious nodes. As a trust builder it performs the task to differentiate the consequences of packet is lost or drop naturally or whether is it due to likely collision in the network. Path Manager assigns reputation to path or route which successfully leads packets successfully from source to destination.

The Advantage of this approach improves overall network performance and functionality by prevention and detection and control of DoS and DDoS attack and limitation is building trust and updating trust-value increases routing overhead.

E. *Using Intrusion Detection System (IDS)*

In [39], The authors provided a survey of possible solutions for IDS against DDoS attacks. IDS is a system that supervises network for malicious activities or policy violations and generates reports based on gathered information. Since DDoS attack traffic may appear similar to legitimate traffic, a detection scheme has a high risk of interpreting legitimate traffic as attack traffic, which is called false positive. Particular attention is focused to IDS that minimizes false positives, with respect to different MANET mobility

models. IDS performance is mainly evaluated through two metrics: *detection scheme coverage* and *false positives*. Coverage represents a proportion of actual attacks that can be detected. Actually, it is a measure of IDS detection effectiveness. In the case of DoS attacks this is relatively easy to measure, as this type of attacks expose themselves with obvious degradation of target's services (e.g. high packet drop rate), though they can be easily detected. False positive is each event in the network that is, by mistake, reported as malicious. Usually, this metric is represented as value obtained by normalizing number of reported false positives versus the number of reported attacks. According to this, the perfect IDS will have the coverage of 100% and 0% false positives. In addition to these two metrics, the intrusion detection time should be as short as possible. The advantage of this approach is to minimize false positive.

In another approach [33], the authors focused on preventing denial-of-service (DoS) attacks. They have proposed an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. They have discussed some types of DDOS attacks like Sleep Deprivation and Rushing attack. These attacks are done due to malicious RREQ flooding (MRF). They have described Adaptive Intrusion Detection and Prevention (AIDP) which uses anomaly-based intrusion detection (ABID) to detect DoS attacks caused by MRF in MANETs. AIDP consists of two modules: training and a testing module. After establishing a network, the cluster head (CH) continuously gathers information and applies the AIDP training module for N time intervals (TI), resulting in an initial training profile (ITP). The ITP reflects the normal behaviour of the nodes in the network. In the testing phase the CH then applies the testing module after each TI. This test consists of several tasks, the first of which detects intrusion. If there is no intrusion then it updates the ITP in order to adapt the variation in the network behaviour as time progresses. If there is intrusion in the second task the CH identifies the intruding nodes. To optimise the probability of identifying intruders correctly with a low level of false positives, it maintains a test sliding window (TSW), in which detections of a node are required in P time intervals (TI). If this detection threshold is passed then the CH will Blacklist (BL) the node and isolate the node by informing all Cluster Nodes. The advantage of this method is reduced overhead, increased throughput.

In similar approach[34] the authors presented a method for determining intrusion or misbehave in MANET using intrusion detection system and protect the network from distributed denial of service (DDOS) and analyzed the result on the basis of actual TCP flow monitoring, routing load, packet delivery ratio and average end-to-end delay in normal , DDoS attack and IDS time. Their new defense mechanism consists of a flow monitoring table (FMT) of all the mobile node. It contains *time, sender_id, node coordinate axis and receiver_id id, transport_info, protocol_type, event_type*. They captured the information of all nodes till particular time. The normal and abnormal behaviour of the network is observed. If the network has *been* infected was identified, they found the attacker node and it will be blocked from the network. The advantage of this approach is their IDS has recovered the data 99.9%. A limitation of this approach is packet capturing, false route forwarding.

F. Limiting Continuous Packet Dropping

In [29], the authors proposed an approach for detection of malicious nodes and protection against DOS attack in AODV protocol. This approach maintains record of all nodes present in the network. Detection and prevention from denial of service attack in AODV routing protocol is implemented by their following algorithm.

- Set a threshold value for Packet Drops
- Observe the Sequence Numbers
- calculate the Packet Drops
- If Packet Drops > thresh hold value then
    - Raise Alarm
    - Delete the routes of the nodes on the basis of packet dropped by them
- Keep a log file to prove that identified nodes are responsible for maximum packet drops, hence removed. After detection of malicious node, it is isolated from network.

The advantage of this method is that leads to less conversation and less communication breakage in ad-hoc routing and limitation is it has limited applicability.

VIII. CONCLUSION

DoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is the primary victim. Loss of network resources causes economic loss, work delays, and loss of communication between network users. Solutions must be developed to prevent these DoS attacks. In this paper, we discussed denial of service attacks. We reviewed various security issues in MANET and discussed the effects of denial of service attacks on MANET or network performance. We also discussed various defense mechanisms that could be employed by networks and hosts. It is essential, that as the Internet and Internet usage expand, more comprehensive solutions and countermeasures to DoS attacks be developed, verified, and implemented

REFERENCES

[1] C.Siva Ram Murthy,B.S.Manoj, "Ad Hoc wireless networks Architectures and protocols" , Pearson Education, tenth impression, 2011.

[2] Subir Kumar Sarkar, T G Basavaraju, C Puttamadappa ,"Wireless Networks: Principles, Protocols, and Applications", Auerbach Publications Taylor & Francis Group,2008.

[3] Pietro Michiardi, Refik Molva , "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", December 2001.

[4] Elizabeth_M_Roger,Chai-Keong_Toh, " A review of current routing protocols for ad-hoc mobile wireless networks ",IEEE personal communication , April 1999.

[5] C. Perkins, E. Belding-Royer and S. Das, "Ad-Hoc On-Demand Distance Vector (AODV) Routing", RFC3561, july 2003.

[6] Peng Ning , Kun Sun, "How to misuse AODV:A case study of insider attacks against mobile ad-hoc routing protocols "Proceedings of the 2003 IEEE workshop on information assurance, U.S. ,june 2003.

[7] Christos Douligeris, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art" , Elsevier,13 October 2003.

[8] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody, "Security scheme for distributed dos in mobile ad hoc networks", ACM, Volume11,Issue1,September2004.

[9] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Denial of service attacks", Internet Protocol Journal, 7(4):13–25, December 2004.

[10] Hwee-Xian Tan, Winston K. G. Seah," Framework for statistical filtering against ddos attacks in MANETs", Proceedings of the Second International Conference on Embedded Software and Systems, 2005.

[11] S. Desilva and R.V. Boppana, "Mitigating malicious control packet floods in ad-hoc networks", Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC), pages 2112-2117, March 2005.

[12] Jarmo V. E. Molsa , "Increasing the dos attack resiliency in military ad-hoc networks" , Proceedings of the IEEE MILCOM 2005.

[13] P. Yi, Z. Dai, Y. Zhong and S. Zhang, "Resisting Flooding Attacks in Ad-Hoc Networks", Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'05), pages 657-662, April 2005.

[14] Yongjin Kim, Ahmed Helmy, "Attacker Traceback with Cross-layer Monitoring in Wireless Multi- hop Networks", SASN '06, October 30, 2006.

[15] Gary Breed Editorial Director, "Wireless Ad-Hoc Networks: Basic Concepts", Proceedings of High Frequency Electronics, March 2007.

[16] Mei Yang, "Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks", International Journal of Network Security, Vol.4, Mar. 2007.

[17] Yogesh Chaba, Yudhvir Singh, Preeti Aneja, "Performance analysis of disable ip broadcast technique for prevention of flooding-based DDoS attack in MANET", Journal Of Networks, VOL. 4, MAY 2009.

[18] Gaurav Kumar Gupt, Jitendra Singh, "Truth of DDOS attacks in MANET, Global Journal of Computer Science and Technology", December 2010.

[19] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[20] Zhi Ang EU and Winston Khoon Guan SEAH, "Mitigating Route Request Flooding Attacks in Mobile Ad-Hoc Networks" Proceeding of School of Computing, National University of Singapore euzhiang@comp.nus.edu.sg , Networking Department, Institute for Infocomm Research, A*STAR winston@i2r.a-star.edu.sg, November 2010.

[21] Pradip M. Jawandhiya , "A survey of mobile ad hoc network attacks", International Journal of Engineering Science and Technology, Vol. 2, 2010.

[22] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav , "Flooding attacks prevention in MANET ", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3 ,2011.

[23] Mohammad Wazid , Rajesh Kumar Singh, R. H. Goudar, "A survey of attacks happened at different layers of mobile ad-hoc network & some available detection techniques" , Proceedings published by International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[24] Minda Xiang, Yu Chen, Wei-Shinn Ku, Zhou Su, "Mitigating DDoS attacks using protection nodes in mobile ad hoc networks", IEEE Global Communications Conference, Dec. 2011.

[25] S.A.Arunmozhi, Y.Venkataramani, "DDoS attack and defense scheme in wireless ad hoc networks", International Journal of Network Security & Its Applications, Vol.3, May 2011.

[26] Rizwan Khan , A. K. Vatsa, "Detection and control of DDOS attacks over reputation and score based MANET", Journal of Emerging trends in Computing and Information Sciences, Vol.2, October 2011.

[27] Fei Wang, Hailong Wang, Xiaofeng Wang, Jinshu Su, "A new multistage approach to detect subtle DDoS attacks", Elsevier, 14 February 2011.

[28] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh3, "Attack Prevention Methods for DDoS Attacks In Manet"s, Asian Journal Of Computer Science And Information Technology, 2011.

[29] Kanchan, Sanjeev Rana, "Methodology for detecting and thwarting DoS in MANET", IJCA, 2011.

[30] Mieso K. Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", SYSTEMICS, Cybernetics And Informatics.

[31] Xin Jin, Yaoxue Zhang, Yi Pan, and Yuezhi Zhou, " A Novel Algorithm forTracing DoS Attackers in MANETs", EURASIP Journal on Wireless Communications and Networking,2006.

[32] Xianjun geng, Yun huang and Andrew b. Whinston, "DefendingWireless Infrastructure Against the Challenge of DDoS Attacks", 2002.

[33] Ramratan Ahirwal, Leeladhar Mahour, "Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network", International Journal on Computer Science and Engineering, 6 June 2012.

[34] Adnan Nadeem, Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs".

[35] Jarmo V. E. Molsa, "Effectiveness of rate-limiting in mitigating flooding dos attacks", International Association of Science and Technology for Development (IASTED),2004.

[36] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations" Request for Comments: 2501, January 1999.

[37] Yogesh Chaba, Yudhvir Singh, Prabha Rani, Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks", Recent Advances In Electronics, Hardware, Wireless And Optical Communications.

[38] Gal badishi, Amir Herzberg and idit keidar , " Keeping Denial Of Service Attackers In The Dark" , IEEE transaction and secure computing, vol-4,no-3, july-sep 2007.

[39] Mirjana Stojanovic,Valentina Timcenko, Slavica Boštjancic Rakas, Intrusion Detection Against Denial Of Service Attacks In Manet Environment, XXIX Simpozijum, 07, decembar 2011.

[40] Mitko Bogdanoski1, Aleksandar Risteski, "Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[41] Abdelhafid Abdelmalek, Zohra Slimane, Mohamed Feham and Abdelmalik Taleb-Ahmed, "A Security Framework for Buddy System based MANET Address Allocation Scheme", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[42] Preeti, Yogesh Chaba, Yudhvir Singh, "Review of detection and prevention policies for distributed denial of service attack in MANET", Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008)RIMT-IET, Mandi Gobindgarh. March 29, 2008.

[43] Mangesh M Ghonge , Pradeep M Jawandhiya , Dr. M S Ali ,"Countermeasures of network layer attacks in MANETs" IJCA Special Issue on Network Security and Cryptography, 2011.

[44] Xiaoxin Wu, David K.Y, "Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach", 3rd International conference on secure communications, pp. 310-319, September 2007.

[45] Kemal Bicakci , Bulent Tavli ," Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", Computer Standards & Interfaces 31 (2009) 931–941.