Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Algorithms for Defending MANETs against the DDoS Attacks

A.Anna lakshmi
Assistant Professor
Department of CSE
KSR College of Engineering
Tamil Nadu

Dr.K.R.Valluvan
Prof. & Head
Department of ECE,
Velalar College of Engineering
Tamil Nadu

Abstract - Mobile Ad hoc Network is the kind of wireless networks that utilize multi-hop radio relaying [1] and it is an infrastructure less Network due to its capability of operating without the support of any fixed infrastructure. Security plays a vital role in mobile ad hoc network (MANET) due to its applications like battlefield or disaster-recovery networks [2]. Current wireless research points out that the wireless MANET has more security problems than traditional wired and wireless networks. MANET is severely affected by Distributed Denial of Service (DDoS) attacks which becomes a problem for users of computer systems connected to the Internet. MANETs are more vulnerable compared to wired networks due the lack of a trusted centralized authority and limited resources. This paper discusses various attacks on MANET and defense mechanisms for DDOS attacks in MANET as reported in the literature.

Keywords:

I. INTRODUCTION

Denial of Service (DoS) attack uses one computer to flood a server with packets. Aim of this attack is to overload the server's bandwidth and other resources. A distributed denial of service attack is a severe form of DOS which uses multiple machines to prevent the legitimate use of a service. It is an active attack [3] and powerful technique[4] to attack Internet resources. It adds to the many-to-one dimension [4] to the DoS problem. Making the prevention and mitigation schemes for them are more complicated. But the impact is proportionally severe. DDoS is composed as shown in Fig.1. First attacker build a network of vulnerable nodes [6] which are used to initiate the attack. The vulnerable nodes called zombies are then installed with attack tools, which allow them to carry out attacks under the control of the attacker.The zombies are divided into masters and slaves[5].The attacker motivates the masters to start the attack, the masters then motivate the slaves. The slaves flood the victim.

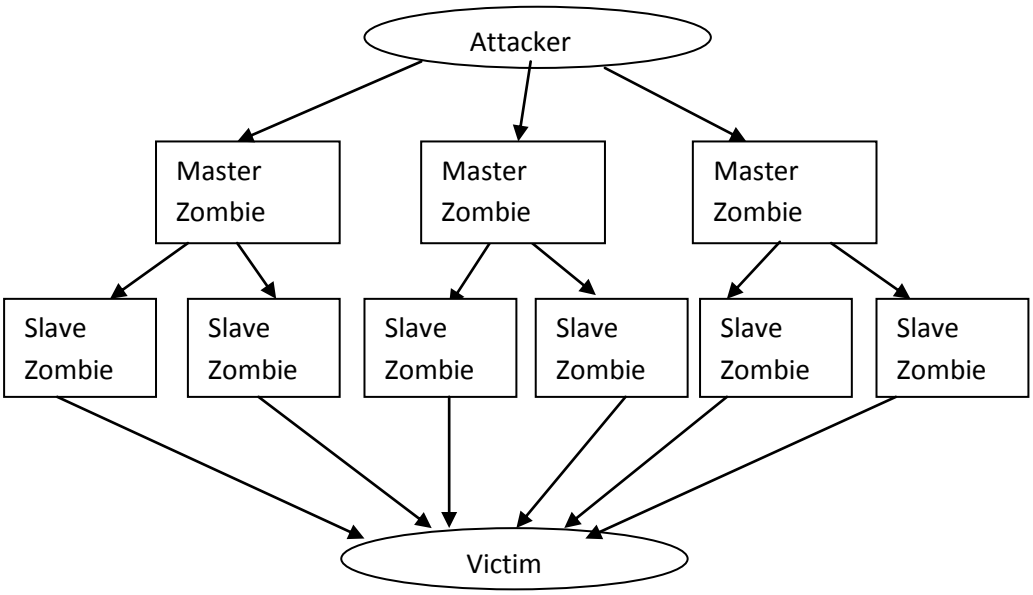

Fig. 1.Block diagram of DDOS attack

In this paper, various defense mechanisms for detection and prevention of DDoS attacks are discussed. The rest of the paper is prepared as follows. Section 2 discusses the different types of security attacks on MANET. In section 3, various defense mechanisms for DDoS attacks on MANET are explained. Section 4 describes the conclusion.

II. DIFFERENT TYPES OF ATTACKS IN MANET

MANET is affected by various attacks[7] as shown in Table 2.

TABLE II
VARIOUS TYPES OF ATTACKS IN MANETS

Security Attacks (External Vs Internal)					
Passive attacks	**Active attacks**				
-Eavesdropping attacks -Traffic analysis & Monitoring	**MAC Layer Attack**	**Network Layer Attack**	**Transport Layer Attack**	**Application Layer Attack**	**Other Attacks**
	Jamming	-Wormhole -Black hole -Information -disclosure -IP spoofing -Modification	-Session Hijacking -SYN flooding	-Repudiation -Data Corruption	-DOS -DDOS - Impersonation -Flooding -Gray hole -Packet dropping -Jellyfish

According to [7], a passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Passive and active attacks are categorized as mentioned above.

III. DEFENSE MECHANISMS

In [6], the authors compared the statistical filtering defense mechanism for DDOS attack on wired and wireless network. They have discussed about framework of statistical filtering. Their assumption is like if there are N filters and N legitimate nodes, then $N_{filter} \leq N_{legitimate}$ nodes. Each filter can work like other legitimate nodes to forward the packets to neighbors. For effective filtering, this filters are equipped with more processing and storage capabilities. Before deploying statistical filtering, normal traffic profiles can be observed during a pre-specified learning window size, W_{learn}. After the observing period, there may be a possibility for happening of attack. Hence they have established online updation of normal traffic profile at specific interval. They have utilized hierarchical based filtering structure in which nodes are grouped into a cluster. There is a cluster head for each cluster to monitor filtering and routing within the cluster. For regular intervals, cluster-head will be rotated for the purpose of load sharing. So no node will spend all of its energy on routing and filtering. Each and every new cluster-head has been authenticated by the previous cluster-head by using private / public key sharing within the cluster. In addition to the Static filter (that uses same filtering policy for all the times), Adaptive filter (filtering policy can be modified based on the traffic characteristics of attack packets) they have introduced another filter called Adaptive filter with feedback. This class of filters can get feedback from the victim nodes in the MANET about the type of attack packets that are being received as well as the congestion level of the network (based on the average end-to-end delay of legitimate packets), and thus is able to improve its adaptive filtering policy. This information is obtained at the application layer, which discards attack packets and propagate this information down to the lower level layers like transport and network layer. The advantage of this method is packet delivery ratio is increased and average end-to-end delay is decreased. A limitation of this method is cluster-based routing protocol filtering mechanism.

In [11], the authors proposed a new defense mechanism which has a flow monitoring table (FMT) at each node. FMT contains *flow id, source id, destination id and packet sending rate*. Data transfer rate is calculated for each flow at the intermediate nodes. With each flow, the updated FMT is sent to the destination. After monitoring the MAC(Media Access Control)layer, the destination sends the Explicit Congestion Notification (ECN) bit to alert the sender nodes about the congestion. After seeing these packets with ECN marking, the sender nodes reduce their sending rate. If the channel becomes congested continuously due to some sender nodes do not reduce their sending rate, it can be found by the destination using the updated FMT. It checks current sending rate with the previous sending rate of a flow. When both the rates are same, the corresponding sender of the flow is considered as an attacker. Once the DDoS attackers are found, all the packets from those nodes will be rejected. An advantage of this scheme is to improve the performance of Adhoc network, high bandwidth, high packet delivery ratio, reduced packet drop for legitimate users.

In [9], the authors 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. 1) 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. 2) 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. 3) the protected node will send an LPNconfirm (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.

In [12], the authors analyzed cluster based intrusion detection method. In this method, the cluster head is selected based on the clique and cluster head computation methods to watch the whole process in the cluster. The hierarchical state routing (HSR) protocol is a distributed multi-level hierarchical routing protocol that does clustering at different levels with efficient membership management at every level of clustering. Clustering increases efficient resource allocation and management. HSR works by classifying different levels of cluster. Clustering algorithm is used for selecting leaders at each level. The first level of physical clustering is done among the nodes which are reachable in a single wireless hop. Members of the first level of this cluster are called as leaf nodes. The next higher level of physical clustering is done among the nodes that are elected as leaders of each of these first-level clusters. Cluster leader is responsible for monitoring security management, intrusion detection computations and data reduction.

In [13], [20], the authors developed a new protocol framework for attacker called CATCH, It is a mechanism towards mobile multi-hop networks (MANET, wireless mesh and sensor networks), which has been concentrated on MAC and network cross-layer approach. CATCH traceback protocol consists of the following four parts: (1) abnormality detection, (2) abnormality characterization, (3) abnormality searching and (4) countermeasures. All the nodes in the network monitors abnormality. Each node monitors the activity of network and MAC layer. If abnormality is detected, the information is captured and logged. Based on the observation of increased packets at network layer, increased collisions at MAC layer, increased frames at MAC layer, increased busy time at MAC layer abnormality is detected. After abnormality detection, it is characterized as time series. After that, Searching of abnormality is implemented by the methods of Traffic pattern matching and Kolmogorov – Smirnov (KS) -fitness test. They have discussed the counter measures like packet filtering and rate limiting. The advantage of this method is computation and memory overhead is low.

In [8], the authors introduced a new Intrusion Detection System (IDS) against DDOS attacks. They have simulated the results through three different criteria like NORMAL case, DDoS attack case and IDS intrusion detection case. In IDS Case, they have selected one node as IDS node which monitors all the mobile nodes within the radio range. If any abnormality is detected in the network behavior, IDS checks the misbehavior with the symptoms of the attack and detects the attack in the attacker node which will be blocked from the network. The advantage of this scheme is throughput and packet delivery fraction is high. End to End delay is reduced.

In [14], [18], the authors proposed a new mechanism for Reduction of Quality (ROQ) attack which is a new mode of DDOS attack. They have classified this attack into 4 types. 1) Pulsing attack 2) Round Robin attack 3) Self-Whisper attack 4) Flooding attack. To counter these attacks, They have introduced a defense scheme that includes the detection and response phases. Detection phase uses three status values that can be obtained from the MAC layer: frequency of receiving RTS/CTS packets, frequency of sensing a busy channel, and the number of RTS/DATA retransmissions. When the number of RTS/CTS packets received exceeds a certain threshold RTS/CTS_{thresh} which represents that too many nodes compete for the channel within the radio range. When the channel is identified as a busy state, a node will persist in the backoff stage and stop the CW(Contention Window) count. In Common, if the number of retransmissions for RTS packets is greater than 7 and that for DATA packets is greater than 4, the packets will be dropped. Thus if the number of retransmissions exceeds a threshold RETthresh, it represents channel congestion. During the response phase, each packet will be marked with an Explicit Congestion Notification (ECN) bit by the nodes, to notify the sender nodes and keep a list of these nodes. When the sender nodes seeing these packets with ECN marking, will then reduce their sending rate. Still the channel continues to be congested because some of the sender nodes do not reduce their sending rate. These nodes will be considered as malicious nodes. Packet from these nodes will be dropped. The advantage of this method is increase in delay and decrease in good put has been observed.

The authors in [10] proposed a proactive scheme that can prevent a specific kind of DoS attack and identify the misbehaving node as well as it prevents 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.

In [15], the authors 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. Advantage of this approach improves overall network performance and functionality by prevention and detection and control of DoS and DDoS attack.

In [16], the authors introduced a new multistage approach to detect subtle DDoS attacks. They proposed a novel multistage DDoS detection framework that consists of a NTS (Network Traffic State) prediction, fine-grained singularity detection and a malicious address extraction engine. They present a model of DDoS attacks based on the following several hypothesis.

•, All the hosts send packets through a monitor point at an identical rate during the normal time.

• All the hosts which access the victim server regularly send packets at an identical rate during the normal time

• All the compromised hosts increase their access rate to the victim by the same ratio during DDoS attacks

• In a DDoS attack, compromised hosts send a significant proportion of traffic to the victim. Meanwhile, all the regular traffic, including the traffic of legitimate hosts accessing the victim, the traffic of compromised hosts accessing other servers in the network, hold their line all the time.

In multistage DDoS detection framework, they have predicted Network Traffic State at a monitor point and compared the predicted state with the real NTS observed. The result of the first stage activates more fine-grained detection in the second stage. Singularity detection in the second stage contributes to reduce false positives by a quantitative analysis on the degree of anomaly caused by DDoS attacks. Simultaneously, it can find the starting time of DDOS attack. After obtaining the approximate start time of attacks, they distinguished malicious IP addresses for attack reactions. It is relatively easy to achieve by comparing the features right after start time to that of before. The advantage of this scheme is improving the accuracy of DDoS detections**.**

The authors in [21] discussed one kind of DDoS attack called black hole attack in MANET on most vulnerability protocol called Ad-hoc On Demand Vector (AODV). AODV is a reactive routing protocol which produce routes and maintain them only if it is needed. So it may be called as on demand routing protocols. They usually use distance-vector routing algorithms and uses traditional routing tables. It This means that for each destination exist one entry in routing table and uses sequence number, that this number ensure the freshness of routes and guarantee the loop-free routing. This protocol is based on two phases: 1) route discovery 2) route maintenance. These phases don't do any job until the network needs to establish a route between source and destination. If the node has no route entry for the destination, the RREQ message (Route Request message) will be broadcasted. In this time, if the next node is the destination, or has a valid route to the destination, a RREP message (Route Reply message) will be generated and sent back to the source. If some malicious nodes send RREP to source, then it is difficult to identify that it is an attacker node due to mobility of adhoc network. All nodes monitor their own neighborhood when a node in an active route gets lost. A route error message (RERR message) is generated to notify the other nodes. This protocol uses another message called HELLO to inform the neighbors that the link is still alive.

In [23], 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.

1. Set a threshold value for Packet Drops
2. Observe the Sequence Numbers
3. calculate the Packet Drops
4. If Packet Drops > thresh hold value then
   A. Raise Alarm
   B. Delete the routes of the nodes on the basis of packet dropped by them

5. 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 adhoc routing.

In [24], The authors provided a survey of possible solutions for Intrusion Detection System (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 [25], the authors proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification. Since nodes are selfish, they may not perform the verification in order to avoid paying the overhead. A bad packet that escapes verification along the whole network path will bring a penalty to all its forwarders. A network game can be formulated in which nodes along a network path, in optimizing their own benefits, are encouraged to act collectively to filter out bad packets. In their approach, the packets from legitimate sources should be digitally signed by their respective senders. The signed SIG with the certificate is used to verify that the packet is from the claimed legitimate source. If the SIG carried in the packet does not match the SIG that a forwarder generates from the received packet, the packet is classified as a bad packet and therefore dropped. The advantage of this approach is that filters bad packets. A limitation of this method is the design of protocols to accurately estimate the severity of attack.

In [26], The authors 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 [27], the authors introduced a new algorithm called zone sampling-based traceback (ZSBT) to trace the DoS attackers in MANETs. While a node forwards a packet, the node writes its zone ID into the packet with a probability. After receiving these packets, the victim can reconstruct the path between the attacker and itself. The ZSBT algorithm consists of three processes: initialization process, zone sampling process, and path reconstruction process. In the initialization process, each node constructs a chain and allow the victim be the head. The chain is used to reconstruct the attack path by sorting the zone ID information in the packets. When a node receives a packet, if the node is the victim, the ZSBT algorithm executes the path reconstruction process. Otherwise, the ZSBT algorithm executes the zone sampling process In the path reconstruction process, the victim reconstructs the zone path from the attacker to itself using the zone information in each packet. In the Zone Sampling process, the node writes its zone ID into the node with a probability p and then forwards the packet. There are two static fields, zone ID, and distance in each packet are reserved. zone ID is used to record the zone ID of the node on the path. Distance denotes the distance from current node to the victim and its initial value is set as zero. The advantage of this method is communication overhead is low. A limitation of this method is focus on locating the exact DDoS attackers.

In [28], the authors proposed a conceptual model which incorporates both cooperative technological solutions and economic incentive mechanisms built on usage-based fees. The Cooperative technological solutions are device security improvement, User level traffic control, Coordinated filters, Tracing back. First User level traffic control and Coordinated filters have been implemented simultaneously to achieve better defence. User-level traffic control is embodied in a set of traffic control rules specifically for a given network device. Even if user-level traffic control fails, DDoS attack is defeated by identifying the attacking traffics and stopping them by using coordinated filters. The purpose of coordination among filters is to stop the traffic as early as possible along the attacking paths to prevent the damage from aggregated traffic. If suppose the coordinated filters cannot effectively stop the attack, there still exists another technological solution to trace back to the zombie devices to shut down the attack from the source. The characteristics of that four coordinated technological solutions are improving the security of all relevant devices. The advantage of this approach is cost effectiveness has been addressed.

In [29], the authors implemented an efficient on-the-fly search technique, Small World-based Attacker Traceback (SWAT), to trace back DoS and DDoS attackers in MANETs. They have provided high-level overview of SWAT architecture and compare it with existing IP traceback schemes. They utilized the concept of Contacts, and use Traffic Pattern Matching (TPM) and Traffic Volume Matching(TVM) techniques. They also proposed multi-

directional search, in-network processing and query suppression to reduce communication overhead in energy constrained MANETs and increase traceback robustness against spoofing and collusion. DoS/DDoS attack is first identified by intrusion detection system at each node. Once the attack is identified, the victim initiates attacker traceback, which is composed of attack traffic analysis and efficient searching. Basically, attack traffic is characterized at the victim to be used as attack signature. Then searching process in launched with the attack signature to find relay nodes and final attacker. To characterize attack traffic from ordinary traffic, they used traffic pattern and traffic volume. Traffic pattern and traffic volume represent abnormal characteristics of attack traffic. When attack starts, traffic shows abnormal pattern/volume increase and the abnormality is observed consistently on the route from attacker to victim. Characterizing attack traffic with traffic pattern/volume in SWAT is light-weight when compared to existing IP traceback in terms of information gathering/storage since it requires only the packet count information in a given time window. Once the attack traffic signature is characterized by traffic pattern/volume, victim node initiates efficient search process. By finding nodes in the neighbour, which observe similar attack traffic signature, they can find nodes that relayed the attack traffic. The process is continued recursively from the neighbour nodes up to the attacker(s). To efficiently search nodes that observed similar traffic signature on the attack route, they extended small world-based contact. Contact nodes are a set of nodes outside the vicinity (radius), which are used as short-cut to build small world and provide wide view on entire network to the victim. Victim node sends query with attack signature to its vicinity nodes (nodes within radius) and contact nodes. To send to contacts, the victim node chooses borders to which it sends queries. The borders in turn choose the contacts at r hops away to which the borders forward the query. Each contact performs in-network processing to check whether there are vicinity nodes that observed attack traffic. If there is no node that observed attack traffic, it suppresses query. Otherwise, it sends next level query to the contact of contact. In doing so, we can perform directional search for DoS attacker traceback and multidirectional search for DDoS attacker traceback, where the search process has directionality towards attacker(s). The advantage of this scheme is Directional and multi-directional search significantly reduces communication overhead.

In [30], 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.

In [31], 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 [32], the authors introduced and analyzed a novel capability-based security mechanism called CapMan(Capability-based Defense against Multi-Path Denial of Service Attacks). This mechanism is particularly against multi path communication in MANET. It consists of two main components: the capability distribution and the capability enforcement. The capability distribution protocol empowers the responder of a traffic flow to issue and distribute a capability to all the nodes along the routing path. After the responder received a connection request from an initiator, it sends a capability packet to the initiator as a notification of the acceptance of an end-to-end flow and the discovery of a new routing path. The capability is not only used as a ticket by the initiator to send data packets, but also saved by all intermediate nodes to restrict the number of packets they will forward for the flow. In addition, the capability enforcement mechanism implements the capability constraint on a per-hop basis across multiple routing paths. They assume multi-path routing between end nodes and that the routing paths do change dynamically. To account for that, all nodes periodically exchange bandwidth consumption reports. This enables each node to maintain a global view of the per flow throughput and capability between any pair of initiator and responder. Thus, their approach can effectively identify and mitigate sophisticated DoS attacks that target multi-path routing protocols, even if both the initiator and the responder are colluding malicious insiders. The advantage of this method is capable of protecting both the network and the end nodes from sophisticated DoS attacks.

In [33], the authors proposed a novel cooperative system which consists of a client detector and a server detector for producing warning of a DDoS attack. The client detector uses a Bloom filter-based detection scheme is placed on the client side to generate accurate detection results and it consumes minimal storage and computational resources. Its main task is to monitor the TCP control packets entering and leaving a domain. The detection scheme is developed from a modified hash table. They have designed the new hash table based on the Bloom filter method. States of each TCP three-way handshake are recorded in the hash table and the abnormal asymmetric three-way handshake can be clearly seen inside the client detector. The client detector thus can issue a DDoS attack after analyzing suspicious alarms. They proposed using a modified Bloom filter in order to construct a hash table that can record three-way TCP control packets at a limited storage cost. The modified structure of the novel hash table makes it possible to capture abnormal handshakes even where the volume of traffic is large.The server detector can actively assist the warning process by sending requests to innocent hosts. With the assistance of client detectors, a server detector can detect a forthcoming DDoS attack at an early stage. The Advantage of this approach is that can both passively and actively detect DDoS attacks. A limitation of this approach is to design the hash function to reduce the occurrence of hash collision, which should also reduce potential false negatives and false positives.

In [34], the authors introduced a dynamic DoS attack . The dynamic DoS attack is characterized in exploiting the node mobility, dynamic power control, and compromised nodes to spread new DoS attacks dynamically. And they have discussed static and dynamic DoS attacks. The DoS attacks launched on link layer and network layer is called as static DoS attack. Eg. Black hole and Jelly fish attack. Malicious nodes may be able to move around the entire network, to adjust transmission power dynamically, or even to propagate DoS attacks by compromising their cooperative neighbors. Therefore, the DoS attacks may become dynamic in terms of the expansion of attack coverage and the propagation of attack impact.

In [35], the authors conducted qualitative analysis and simulations to investigate the feasibility and evaluate the attack path detection performance of existing IP Traceback techniques like Source Path Isolation Engine, Probabilistic Packet Marking, and ICMP Traceback on wireless ad-hoc networks, using proactive (DSDV) or reactive (AODV) routing protocol. To trace the true source of the attackers, several IP Traceback mechanisms have been proposed to maintain accountability. In SPIE, every intermediate router maintains the digests of processed packets. After a particular time interval, the processed packets specifics are transferred to a central server for longer-term storage and analysis. In this scheme, only one attack packet is required to reconstruct the attack path. In PPM, packets are marked by intermediate routers probabilistically to contain fragments of the path information. When the victim has collected sufficient number of marked packets, it would be able to reconstruct the attack path. In ITrace, each intermediate router generates a new ICMP packet, called the ITrace message at a low probability for each packet it processed. The message contains information about this router and the packet, and is sent to the same destination of the packet. Upon reception of sufficient number of ITrace messages, the victim would be able to reconstruct the attack path.

In [36], the authors introduced a new method to improve the topology stability of the MANET on stable topology. Due to free mobility of nodes, an attack path in MANET might dynamically change on the routing path. Since the topology is keep on changing, the detected attack path is no longer valid and need to traceback again, or the in-processing traceback procedure cannot be completed within the prospective time. For this reason, a stable environment for traceback has been created on stable topology to bring higher traceback efficiency. They used the Identity Replacement based AODV(IR-AODV) protocol to enhance the stability of MANET topology so that the host could have sufficient time to traceback. Research indicates that it greatly improve the traceback success ratio. The advantage of this approach is to improve the topology stability of MANET and also traceback efficiency is improved.

The authors in [38] proposed a traceable overlay network with relative stable topology support for traceback based on identity replacement mechanism. They have proposed an Identity Replacement (IR) mechanism to give a more stable topology support for traceback. Since MANET has a dynamic topology, it is impossible to keep the physical topology being static for a long time. So they have created a virtual overlay network above the network layer to a relative stable logical topology. Each node has a unique physical id on network layer like n1, n2 and so on. And it has a node name as logical id on overlay layer like W, X, Y, Z. The node id is supposed to be fixed, while the node name can be changed according to the network context. And there is a temporary mapping between them. At first there is a routing path from n1to n4 on physical network layer: n1→n2→n3→n4. And on the virtual overlay layer, there is a corresponding logical path: W→X→Y→Z. They assumed the node n2 moves away and n5 just moves into this path. After a route recovery process, the physical path will migrate to: n1→n5→n3→n4. In order to maintain the stability of the overlay layer topology, they proposed an Identity Replacement mechanism. In order to remain the overlay layer topology stable, the node n5 will change its name (logical id) to "X" according to the current network context, while its physical node id will not be changed. Thus depending on this mechanism, the topology of the overlay network could be remained as stable as they can. Then they have performed traceback on this overlay network with a relative more stable topology support. The advantage of this method is traceback performance is improved.

In [39], the authors presented a quantitative model to characterize the DDoS flooding attack and its traffic statistics. They also proposed an analytical model for looking for specific patterns of the attack traffic, aiming to achieve: (1) Decide if there is an anomaly in the traffic and whether the anomaly is the DDoS attack (2) Decide the time when the attack is launched. Network forensics is the process of capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. The flooding attack considered in their work performs at the network layer. It aims to paralyze the entire network, rather than any particular node, by

injecting overwhelming attack traffic (e.g. RREQ broadcasting) into the MANET. Because all or most of key resources of mobile nodes are meaninglessly consumed on processing and transmitting the attack traffic, legitimate users' traffic is denied. As a result, a network-wide congestion, instead of the congestion surrounding a individual node as in conventional Internet DDoS attacks, is created. The advantage of this method is to detect DDoS attacks more effectively by traffic pattern identification proposed in
their work.

In [17], [37], the authors proposed a technique that can prevent a specific kind of DoS attack i.e. smurf attack. The proposed scheme can prevent Distributed DoS (DDoS) attack. They have discussed two types of DDoS attacks such as Malicious Packet Dropping based DDoS attack and Flooding Based DDoS attack. In packet dropping attack, some nodes are made as malicious by the attacker, and the malicious nodes drops some or all data packets sent to it for further forwarding even when no congestion occurs. They have implemented two detection techniques like Unconditional Packet Dropping technique and Malicious Flooding on SpecificTtarget. Unconditional Packet Dropping technique is used to detect packet dropping attack. Here they monitored the statistics Forward Percentage (FP) over a adequately long time period T. FP verifies the ratio of forwarded packets over the packets that are transmitted. In flooding attack, the attacker begins a lot of Route Request packets (RREQ Flooding Attack) for a node. so that the node has to be congested. For this attack, they proposed a technique called Malicious Flooding on SpecificTtarget which is to detect flood attack which monitors the total number of flood over a period of time. They have proposed a new Prevention Technique called Disabling IPBroadcasts. A broadcast is a data packet that is intended for multiple hosts. There are two types of broadcasts supported by Cisco routers: directed and flooded. A directed broadcast is a packet sent to a specific network or series of networks, whereas a flooded broadcast is a packet sent to every network. They have discussed flooded broadcast due to DDoS attack. A cruel type of DDoS attack is the Smurf attack, which is made possible mostly because of badly configured network devices that respond to Internet Control Message Protocol (ICMP) echoes sent to broadcast addresses. The attacker sends a large amount of ICMP traffic to a broadcast address and uses a victim's IP address as the source IP. So the replies from all the devices that respond to the broadcast address will flood the victim. So it is clear that IP broadcast cause the flood on the victim node. By disabling IP Broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. However, to defend against this attack, all neighboring networks need to disable IP broadcasts. The advantage of this method is that prevents flood attack.

IV. CONCLUSION

Security is the most important feature for deployment in mobile Adhoc network. Distributed Denial of Service attacks are more complex and serious problem, and as a result, several approaches have been proposed to counter them. This paper discussed the various methods available in the literature with regard to various defense mechanisms for DoS and DDoS attacks on MANET.

REFERENCES

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

[2] Jiazi YI, Polytech Nantes *A Survey on the Applications of MANET*, Feb 2008.

[3] Rajni Sharma, Alisha saini, *A study of various security attacks and their countermeasures in manet*, International journal of advanced research in Computer Science and Software Engineering", Volume-1, Issue-1, December-2011.

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

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

[6] 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

[7] Pradip M. Jawandhiya: *A Survey of Mobile Ad Hoc Network Attacks*, International Journal of Engineering Science and Technology, Vol. 2, 2010.

[8] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, *A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network*, International Journal of Computer Applications, Volume 41, March 2012

[9] 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.

[10] 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.

[11] 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.

[12] Shanmuga vadivu G, Umamaheswari A, *An Efficient Leader Election Mechanism For Intrusion Detection in MANET*, Journal of Computer Applications, Volume-5, February 10, 2012.

[13] Yongjin Kim a, Ahmed Helmy b, *CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks*, Elsevier, 2009.

[14] Wei Ren, Dit-Yan Yeung, Hai Jin1, and Mei Yang, *Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks*, International Journal of Network Security, Vol.4, Mar. 2007.

[15] 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.
[16] Fei Wang, Hailong Wang, Xiaofeng Wang, Jinshu Su, *A new multistage approach to detect subtle DDoS attacks*, Elsevier, 14 February 2011.
[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] Wei Ren, Hai Jin, Tenghong Liu, *Congestion Targeted Reduction of Quality of Service DDoS Attacking and Defense Scheme in Mobile Ad Hoc Networks*,Proceedings of the Seventh IEEE International Symposium on Multimedia, 2005
[19] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh3, *Attack Prevention Methods for DDoS Attacks In Manets*, Asian Journal Of Computer Science And Information Technology, 2011.
[20] Yongjin Kim, Ahmed Helmy, *Attacker Traceback with Cross-layer Monitoring in Wireless Multi- hop Networks*, SASN '06, October 30, 2006.
[21] Shideh Saraeian, Fazllolah Adibniya, Mohammad GhasemZadeh and.SeyedAzim Abtahi, *Performance Evaluation of AODV Protocol under DDoS Attacks in MANET*, World Academy of Science, Engineering and Technology, 2008.
[22] Gaurav Kumar Gupt, Jitendra Singh, *Truth of DDOS attacks in MANET*, Global Journal of Computer Science and Technology, December 2010.
[23] Kanchan, Sanjeev Rana, *Methodology for Detecting and Thwarting DoS in MANET*, IJCA,2011.
[24] Mirjana Stojanovic,Valentina Timcenko, Slavica Boštjancic Rakas, *Intrusion Detection Against Denial Of Service Attacks In Manet Environment*, XXIX Simpozijum, 07, decembar 2011.
[25] Xiaoxin Wu, David K. Y. Yau, *Mitigating Denial-of-Service Attacks in MANET By Incentive-based Packet Filtering: A Game-theoretic Approach.*
[26] 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.
[27] Xin Jin, Yaoxue Zhang, Yi Pan, and Yuezhi Zhou, *ZSBT: A Novel Algorithm forTracing DoS Attackers in MANETs*, EURASIP Journal onWireless Communications and Networking,2006.
[28] Xianjun geng, Yun huang and Andrew b. Whinston, *DefendingWireless Infrastructure Against the Challenge of DDoS Attacks*,2002.
[29] Yongjin Kim, Ahmed Helmy, *SWAT: Small World-based Attacker Traceback in Ad-hoc Networks*, Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005.
[30] 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.
[31] Adnan Nadeem, Michael Howarth, *Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs*.
[32] Quan Jia, Kun Sun, Angelos Stavrou, *CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET*.
[33] Bin Xiao, Wei Chen, Yanxiang He, *A novel approach to detecting DDoS attacks at an early stage*, J Supercomput, 2006.
[34] Fei Xing Wenye Wang, *Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks*.
[35] Vrizlynn L. L. Thing, Henry C. J. Lee, *IP Traceback for Wireless Ad-hoc Networks*, IEEE,2004.
[36] Lili Zhang, Yinan Jing, Xueping Wang, Xiu Ca, *Attack Source Traceback based on Stable Topology in MANET*, 2011 IEEE.
[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] Yinan Jing, Xueping Wang, Lili Zhang, Gendu Zhang, *Stable Topology Support for Tracing DDoS Attackers in MANET*, 2011 IEEE.
[39] Yinghua Guo, Matthew Simon, *Network forensics in MANET: traffic analysis of source spoofed DoSattacks*, Fourth International Conference on Network and System Security, 2010.
[40] 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, March 29, 2008.

