IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 05-08
www.iosrjournals.org

Providing The Security Against The DDOS Attack In Mobile Ad Hoc Networks

Amrita A.Shirode[1], Prof. Vinod S. Wadne[2]
Department Of Computer Engineering Jspm's Icoer,Wagholi Pune, India

Abstract: *The extensive applications of Mobile ad hoc networks are in civilian and military. In the MANETs nodes are joining to any point and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. In our paper, we are trying to solve the problem regarding attacks by black-hole in the group of nodes. We are dealing with the identifications of multiple black holes and a remedy to generate another route avoiding black-hole attacked nodes. We are also trying to deliver security to avoid DDOS attack.*

Keywords: *Security, algorithms, distributed denial of attack, intrusion detection system.*

I. Introduction

MANET is collection of nodes or the terminals having the wireless communication. It communicates one another having no assistance of any centralize system. In this system the nodes connected each other by wireless link and sending the packet data to one another. Because of the absence of centralize system the routing is held by nodes themselves. The nodes have mobility and routing nature capability, thus they consist of many weaknesses regarding security. To resolve security problems we require Intrusion detection system. This can classified as Signature based intrusion detection and anomaly based intrusion detection. Signature based consists of previously defined signatures stored in data base of IDS. If there is any trouble in network IDS matches it with the previously saved signature and if it is matched than IDS found the attack. If there is attack and their signature is not found in database then IDS cannot be capable to detect the attack. So the database should update periodically is compulsory. So to overcome this problem anomaly based IDS are conceived. In this firstly the IDS made the normal profile of network. It put the normal profile as base profile compares with examined network profiles. The advantage of this technique is it can able to notice attacks without having previous knowledge of attacks. Intrusion attacks are easy in network as compared to wired networks. The serious attacks are considered in networks is DDoS attacks. DDoS attacks are on large scales, coordinate the attack by availability of service at victim systems or networks resources. DDoS attacks are defined by directing number of packets to destination node through co-ordination of intermediate nodes which are spread all over the networks. At the attacked node the large traffic of data consumes bandwidth and is not allowing important packet reached to the destination.

II. Related Work

In the network the AODV protocol, the attacked node in IDS pretends as fresh enough network routes to destination demanded by all nodes and engage traffic. The source is broadcasting the RREQ for destination, the attacked node replies with RREP and with next node details. This message is perceived as, if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that destination is after black hole node. The next node and perceives the other RREP packets with next node coming from other nodes.

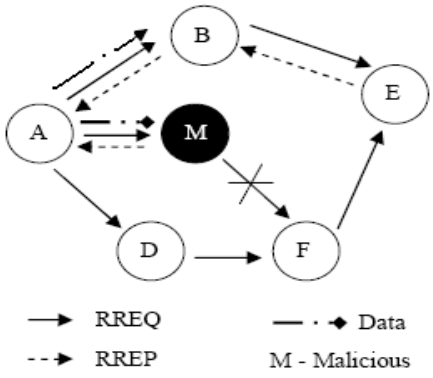


Figure 1. Propagation of RREQ and RREP from A to E

The source starts to deliver out its packets to attacked node and after small time interval to the other node, trusting that these packets will reach to the destination either by one link.

III. Attacks On Manet

In the rest of this paper, we review the basics of AODV protocol and attacks. We are also describing methods which have proposed for detection or prevention of these attacks and proposed a new mechanism that effectively prevents the attacks and finally, we conclude the paper.

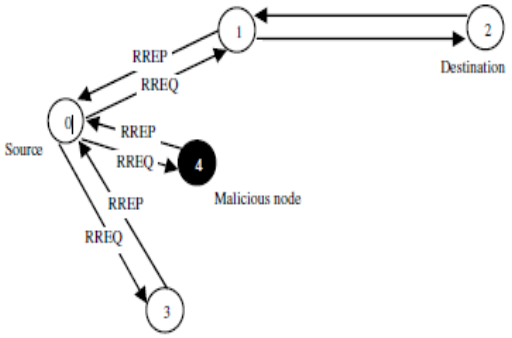
1. Black Hole Attack

1.1. Black Hole

The black hole attacks have two properties: 1. Nodes exploit routing protocol, like AODV, to broadcast itself as having safe route to the destination, even route is false, with the intention of interrupting packets. Second, node utilizes the interrupted packets. We describe following facts for protocol representation.

1.2. Cooperative Black Hole Attack

According AODV, when source S needs to communicate with destination D, the source S is broadcasting route request (RREQ) packet. Neighboring node updates its routing table and enters the new entry for the source. It checks the availability of destination or the fresh route towards destination node. If no availability is there, intermediate nodes update the RREQ by increasing the hop count. It results in floods in network with RREQ to destination D till it reaches destination or intermediate node which fresh route to destination, as described by example in Figure 2. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.



2. Wormhole Attack

Wormhole attack is the challenging attack in ad hoc routing. I this type of attack malicious nodes make the tunnel having high connectivity referred as a wormhole tunnel. The wormhole tunnel may be wired or wireless form or an optical link. As attacked nodes launch wormhole link it starts gathering the data. It forwards to one another. Then it is communicate the packet over wormhole tunnels to other locations. The real data are transmitted to other destination in network. Malicious node pretends that they are neighbors in the network. By this, it utilizes the whole communication channel through them. Wormhole attacks affect both proactive and on demand routing protocols. In wormhole attack, honest nodes in network do not forecast the original network creation. This roots severe harm in network that is founded on localization scheme and it can lead honest nodes to take wrong decision. It's problematic to notice such unsafe attacks and no one can forecast what the wormhole nodes activities. The wormhole attacks are unseen at advanced layer and therefore, two end points of the wormhole are not visible in the route in which detection becomes much more complex. Wormhole node consequence in denial of service as it makes discard of all packets instead of forwarding. In this kind of attack, attacked node gathers packets at one end and channels them to other end of network. This process is getting repeated. The most hazardous thing in wormhole attack is that attacker is invisible at higher layers of network. The wormhole attacker drops the packets or selectively forwards packets so that it cannot be detected. The wormhole attacker can launch its attack even in the network with better security in terms of authenticity and confidentiality. The wormhole locates the attacker in the central part of the network and thus, the attacker uses this location in several ways. The result of wormhole attack is that it discards the data packets instead of forwarding these data packets and thus resulting in a denial of service attack or particularly discarding the data packets. These are some of the possible dangerous attacks in MANET. Therefore, we present a proficient technique for the detection of the wormhole attack.

3. Denial of Service

The attack called Denial of service (DoS) has developed most important threat to ad hoc networks. Initial attacks were procedural games among attackers. As an example, attacker wants to control the IRC channel via DoS attacks in contradiction of the owner. Attacker recognize in the underground communal via taking down standard web sites. As it is easy-to-use attack tools, it can easily download from Internet, so the normal users may become attackers also. Sometime attackers coordinately stated their observations via initiation attacks against administrations whose rules they disagreed with. Such attacks performed illegal actions. Enterprises might usage attacks to hit off their contenders in market. The attacker vulnerable online industries with DoS attack. It requested payments for guard. DoS attack which is known to Internet conquer objective by exhausting resources, that is anything connected to network and performance, like link bandwidth, TCP buffers, service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. It's problematic for attacker to overload the objective's resources from single PC; recent attacks were thrown via huge number of attacking hosts over Internet. Such attacks called distributed denial of service (DDoS) attacks. In such attacks, because of the aggregation of attacked traffic can tremendous likened to victims, the attacks can be forced the victims to significantly reduce its performance or stops delivering any service. Associated with conventional DoS attack could be addressed by securing systems or prohibiting illegal remote local access, DDoS attacks are complex and hard to avoid.

4. Distributed Denial of Service

Distributed Denial of Service (DDoS) is progressively Internet phenomenon and is accomplished of silencing speech, frequently for a interval but rarely longer. DDoS attack in contradiction of independent media and human rights sites have common in past years, even outdoor of elections, and military operations. With latest highly DDoS attacks on Wikileaks, and "Operation Payback" attack by "Anonymous" sites apparent to oppose Wikileaks, we suppose these attacks become more public. Media and human rights sites suffered from types of attacks, containing filtering, intrusions, and defacements along to DDoS attacks, and such attacks interact with one another in composite ways. Independent media and human rights sites suffer from both application DDoS attacks, which exhaust local server resources and can usually be mitigated by a skilled system administrator; and network DDoS attacks, which exhaust network bandwidth and can usually only be mitigated with the help of a hosting provider at considerable expense. Push-back is a tool for protecting against Distributed Denial-of-Service (DDoS) attacks. Distributed Denial-of-Service (DDoS) attacks are treated a congestion control problem. Because such a congestion caused by malicious hosts. They are not obeying outdated end to end congestion control, the problem must handled by routers. The functionality added to router for detection drop data packets that belong to attack. The routers are notified to drop such packets in order that the router's resources be used to route legitimate traffic hence term push-back. Client puzzles have been advocated as a promising countermeasure to DoS attacks in the recent years. In order to identify the attackers, the victim server issues a puzzle to the client that sent the traffic. When the client is able to solve the puzzle, it is assumed to be authentic and the traffic from it is allowed into the server. If the victim suspects that the puzzles are solved by most of the clients, it increases the complexity of the puzzles. This puzzle solving technique allows the traversal of the attack traffic throughout the intermediate routers before reaching the destination. In order to attain the advantages of both push-back and puzzle solving techniques, a hybrid scheme called Router based push-back technique, which involves both the techniques to solve the problem of DDoS attacks is proposed. In this proposal, the puzzle solving mechanism is pushed back to the core routers rather than having at the victim. The router based client puzzle mechanism checks the host system whether it is legitimate or not by providing a puzzle to be solved by the suspected host.

IV. IDS Intrusion Detection Case

We will measure throughput provide to genuine users and to attacker when consuming algorithms.

Distributed denial of service attack scenario

1. Normal Case

The network having number of senders and the receivers. The transport layered mechanisms as TCP and UDP with the protocol AODV routing. Afterward the settings all parameters are going to calculate the results.

2. Attack Case

Attack module creates one node called attacker node. It sets some parameters like scan port , scan time , infection rate , and infection parameter , attacker node send probing packet to all other neighbour node whose belongs to in radio range, if any node as week node with nearby or in the radio ange on attacker node agree with communication through attacker node. The searching packet accept by attacked node and pollute through contagion. This infected nodes launch DDOS (distributed denial of service) attacks. It infects to other nodes that cases overall network has infected.

3. IDS Case

In intrusion detection system we will consider one node as IDS node. This node lookout all range of nodes. If there is any unusual behaviour detected to network, system will firstly check the indications of attacks. It finds attacker nodes , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

V. Conclusion

We are going to discussed distributed denial of service attack on Internet. We defined distributed attacks are directed, we also reviewed known distributed denial of services. We discussed various defenses mechanism that could employed by network and host. We examine performance of various queuing algorithms in alleviating the distributed denial of service attacks and in providing desired service to the users. It found the majority of algorithms that we are going to considered bandwidth to genuine user during attacks. Even in denial of service attacks, the defined algorithm can guarantee bandwidth for the certain class of the input flow, The algorithm was effective in the as long as limited bandwidth to genuine users. Since implementation of a Class Based Queuing algorithm required additional effort, there is a tradeoff between its performance and the implementation overhead. In summary, our simulation results indicated that implementing queuing algorithms in network routers may provide the desired solution in protecting users in cases of distributed denial of service attacks.

References

[1]. C. Adams and J. Gilchrist, "RFC 2612: The CAST-256 encryption algorithm," June 1999, http://www.cis.ohiostate.edu/htbin/rfc/rfc2612.html.
[2]. J. Barlow and W. Thrower, "TFN2K – an analysis," Feb. 2000, http://packetstorm.securify.com/distributed/TFN2k_ Analysis.htm.
[3]. S. Bellovin, "Security problems in the TCP/IP protocol suite," Comput. Commun. Rev., vol. 19, no. 2, pp. 32-48, Apr. 1989.
[4]. S. Bellovin, "Distributed denial of service attacks," Feb. 2000, http://www.research.att.com/~smb/talks.
[5]. S. Bellovin, Ed., "The ICMP traceback message," Network Working Group Internet Draft, Mar. 2000, http://www. research.att.com/~smb/papers/draft-bellovin-itrace-00.txt.
[6]. CERT Coordination Center, Cert Advisories: "CA-2000-01 denial-of-service developments," http://www.cert.org/advisories/ CA-2000-01.html; "CA-99-17 denial-of-service tools," http://www.cert.org/advisories/CA-99-17-denial-of-servicetools.html; "CA-98-13-tcp-denial-of-service: vulnerability in certain TCP/IP implementations," http://www.cert.org/advisories/ CA-98-13-tcp-denial-of-service.html.
[7]. CERT Coordination Center, "Results of the distributed systems intruder tools workshop," Nov. 1999, http://www.cert.org/reports/dsit_workshop.pdf.
[8]. Cisco Systems, Inc., "Defining strategies to protect against TCP SYN denial of service attacks," July 1999, http://www.cisco.com/warp/public/707/4.html.
[9]. Daemon9, Infinity, and Route, "IP-spoofing demystified: trust-relationship exploitation," Phrack Mag., June 1996, http://www.fc.net/phrack/files/p48/p48-14.html.
[10]. D. Dittrich, "The DoS project's 'Trinoo' distributed denial of service attack tool," Oct. 1999; "The 'Stacheldraht' distributed denial of service attack tool," Dec. 1999; "The 'Tribe Flood Network' distributed denial of service attack tool," Oct. 1999, http://www.washington.edu/People/dad.
[11]. D. Dittrich, S. Dietrich, and N. Long, "An analysis of the 'Shaft' distributed denial of device tool," Mar. 2000, http://netsec.gsfc.nasa.gov/~spock/shaft_analysis.txt.
[12]. [12] P. Ferguson and D. Senie, "RFC 2267: Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing," Jan. 1998, http://info.internet.isi.edu/innotes/rfc/files/rfc2267.txt.
[13]. S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," IEEE/ACM Trans. Networking, vol. 1 no. 4, pp. 397-413, Aug. 1993.
[14]. S. Floyd and V. Jacobson, "Link-sharing and resource management models for packet networks," IEEE/ACM Trans. Networking, vol. 3 no. 4, pp. 365-386, Aug. 1995.