International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

ENHANCEMENT IN SECURITY ISSUES DUE TO DDOS & DOS IN MOBILE WSN

Ankit Garg[1], Mr. Devkant Tyagi[2]
[1]M.Tech(Computer Science), [2]Assistant Professor M.Tech(CS)
Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India

ABSTRACT: With the recent advances in modern communication systems, wireless networks are expected to provide communication with confidentiality, data integrity, and availability of service to the user. Confidentiality of data can simply be explained as prevention of the un trusted third party from accessing the secure data. Data integrity ensures that replay attacks are prevented and the data is not modified and availability ensures that legitimate users can access services, data and network resources when requested. As wireless sensor networks continue to grow due to the fact that they are potentially low cost and effective (providing solutions to a number of real world challenges), the need for effective security mechanisms also grow. Most of the WSN's routing protocols are easy and straightforward because of this reason they are vulnerable to attacks. The Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to wireless sensor networks. So we start by considering such characteristics of the network and giving their impact on the security of the network. By preventing a single device from sending traffic or by preventing the communication between the network, DoS attacks target availability of services to the users. In this paper we present a survey of attacks on WSN, discuss about the various DoS attacks, and the impact of DoS on the performance of the system. The simulation results show that the impact of DoS attacks on performance of WSN can be more severe, if carried out on coordinator or router, instead of just targeting the end devices. Evaluation of Wireless Sensor Networks (WSN) for performance evaluation is a popular research area and a wealth of literature exists in this area. Denial-of-Service (DoS) attacks are recognized as one of the most serious threats due to the resources constrained property in WSN. Here this research includes the LEACH and CBCR for evaluating the performance or QoS of WSN in term of dead node in time domain. Further all finding will be shown in term of energy dissipation and number of dead node occurrence in WSN in number of round basis. We proposed mixed algorithm based on CBCR and LEACH to analysis the energy dissipation and dead node occurrence in WSN.

Keywords: DoS, DDoS, CBCR, LEACH, WSN, Internet Protocol.

I. INTRODUCTION

1.1 An Overview of Denial of Service Attacks

Denial of Service (DoS) attacks has proved to be a serious and permanent threat to users, organizations, and infrastructures. The primary goal of these attacks is to prevent access to a particular resource like a web server. A large number of defenses against DoS attacks have been proposed in the literature, but none of them gives reliable protection. There will always be vulnerable hosts in the Internet to be used as sources of attack traffic. It is simply not feasible to expect all existing hosts in the Internet to be protected well enough (in July 2005 it was estimated that there were approximately 350 000 000 hosts in the Internet). In addition, it is very difficult to reliably recognize and filter only attack traffic without causing any collateral damage to legitimate traffic. A DoS attack can be carried out either as a flooding or a logic attack. A flooding DoS attack is based on brute force. Real-looking but unnecessary data is sent as much as possible to a victim. As a result, network bandwidth is wasted, disk space is filled with unnecessary data (such as spam e-mail, junk files, and intentional error messages), fixed size data structures inside host software are filled with bogus information, or processing power is spent for unuseful purposes. To amplify the effects, DoS attacks can be run in a coordinated fashion from several sources at the same time (Distributed DoS, DDoS). A logic DoS attack is based on an intelligent exploitation of vulnerabilities in the target. For example, a skillfully constructed fragmented Internet Protocol (IP) data-gram may crash a system due to a serious fault in the operating system (OS) software. Another example of a logic attack is to exploit missing authentication requirements by injecting bogus routing information to prevent traffic from reaching a victim's network. There are two major reasons that make DoS attacks attractive for attackers. The first reason is that there are effective automatic tools available for attacking any victim, so expertise is not necessarily required. The second reason is that it is usually impossible to locate an attacker without extensive human interaction or without new features in most routers of the Internet. DoS attacks make use of vulnerabilities in end-hosts, routers, and other systems connected to a computer network. The size of a population having the same vulnerability can be large. In July 2003 a vulnerability was found from the whole population of Cisco routers and switches running any version of the Cisco IOS software and con-figured to process Internet Protocol version 4 (IPv4) packets. This vulnerability made it possible to block an interface, which resulted in a DoS condition without any alarms being triggered. Another example of a large population is the Microsoft Windows Metafile (WMF) vulnerability which was found in December 2005 from all versions of Windows 98, 98SE, ME, 2000, and XP. This vulnerability made it possible to install any malicious software on these hosts, for example, to send DoS attack traffic. User interaction was, however, required to exploit this vulnerability.

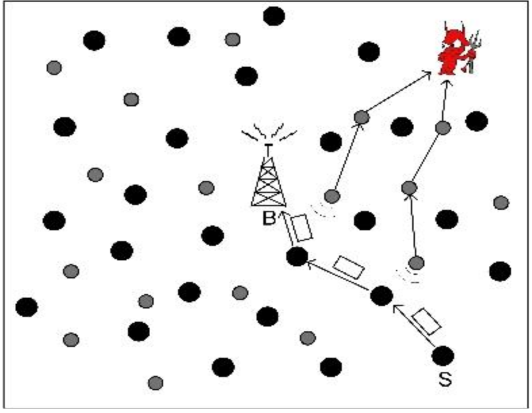

Fig 1.1: DOS attack in WSN

1.1.1 DoS Attacks in Real-Life

Real DoS incidents in the Internet between the years 1989 and 1995 were investigated in. The three most typical effects were the following: 51% of these incidents filled a disk, 33% of the incidents degraded network service, and 26% of the incidents deleted some critical files. A single incident was able to cause several types of damages at the same time (the sum of percentages is more than 100%).

1.2 Terminology

This section gives definitions for the most important terms used throughout this dissertation.

1.2.1 Denial of Service Terminology

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. Examples of resources in this definition are network bandwidth, processing capacity, disk space, memory, and static memory structures. An attack (which does not have to be successful) is defined in the ANSI's Telecom Glossary 2000 to be an attempt to violate security. This will be used as the basis for defining a DoS attack.

Denial of service attack: An intentional attempt to prevent or degrade availability of any resources. It is not always possible to say exactly what in practice a DoS attack is. For example, spam e-mails constitute approximately 70% of incoming e-mails, but spam is generally not considered to be DoS, even though a large amount of spam induces delay for end users. Added delay as such, however, is one characteristic of DoS attacks. The term intrusion is used to denote a successful attack.

Intrusion: Successful unauthorized usage or misuse of a network or computer system. As expressed in this thesis, it is not possible to prevent DoS attacks reliably. In-stead, we talk about mitigating these attacks. According to the Webster's dictionary, the verb mitigate means the following.

To mitigate: To lessen in force or intensity, or to make less severe. DoS attacks are one manifestation of computer crime, other manifestations including malicious software, spam, spyware, fraud, and phishing, abuse of networks, unauthorized access, and theft of proprietary information. The definition for computer crime in the ANSI's Telecom Glossary 2000 is the following.

Computer crime: A violation of law committed with the aid of, or directly involving, a data processing system or network. DoS attacks can be classified based on the number of sources included in an attack. In a basic DoS attack the attacker uses a single source host to send attack traffic to a victim. A distributed DoS (DDoS) attack involves more than one sources of attack traffic:

Distributed denial of service attack: An attempt to prevent or degrade availability of any resources by using multiple source hosts at the same time to send attack traffic. Typically the participants in a DDoS attack form a hierarchical DDoS network where an attacker controls a few masters (or handlers), which in turn control a much higher number of agents (or daemons or zombies or bots) to carry out a real attack against a victim. These are defined as follows.

Agent (or daemon or zombie or bot): A compromised host used to send attack traffic in a DoS attack.

Master (or handler): A compromised host used to control the operation of a large set of agents

DDoS network: A hierarchically structured set of masters and agentsto make it easier to control a DDoS attack by an attacker. DoS attacks may be either destructive or derivative.

Destructive DoS attack: Prevents the availability of a resource completely.

Degradative (non-destructive) DoS attack: Reduces the performance of a resource. A destructive DoS attack can, for example, crash a system or fill disk partitions. In these cases human intervention is typically needed for recovery. A degradative DoS attack will typically cause only temporary problems, and a system will recover automatically as soon as an attack terminates. An example of a degradative DoS attack is a flooding attack overloading a network link or a host central processing unit (CPU). A prolonged high-bandwidth flooding attack, however, may have unexpected results, such as system crashes.

A DoS attack can be seen to have two different directions.

Inward DoS attack: From the victim point of view a DoS attack con-sists of incoming attack packets.

Outward DoS attack: From the attack source point of view a DoS attack consists of outgoing packets. DoS attacks consist of two major phases. Both of these phases make use of deficiencies in the design or implementation of applications, protocols, and the Internet architecture.

Deployment phase: Installation of a malicious program on a set of compromised hosts to be used later as a source for DoS attack traffic.

Attack phase: Coordinated transmission of attack traffic against avictim.

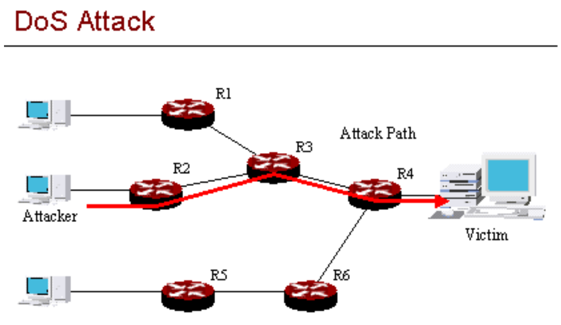

Fig 1.2: DOS attack through different routers

1.3 Research Problem

Mitigating DoS attacks is difficult especially due to the following problems.Very little has been done to compare, contrast, and categorize the different ideas related to DoS attacks and defenses. As a result it is difficult to understand what a computer network user needs to do and why to mitigate the threat from DoS attacks. There are no effective defense mechanisms against many important DoS attack types.

There is no guidance on how to select defense mechanisms. Existing defense mechanisms have been evaluated according to very limited criteria. Often relevant risks have been ignored evaluations have been carried out under ideal conditions. No research publications exist for giving a systematic list of issues related to defense evaluation.

II. LITERATURE SURVEY

A. Literature Survey

Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay proposed a detailed study of the source code of the popular DDoS attack bots, Agobot, SDBot, RBot and Spybot to provide an in-depth understanding of the attacks in order to facilitate the design of more effective and efficient detection and mitigation techniques. In recent years, we have seen the arrival of Distributed Denial-of-Service (DDoS) open-source bot-based attack tools facilitating easy code enhancement, and so resulting in attack tools becoming more powerful. Developing new techniques for detecting and responding to the latest DDoS attacks often entails using attack traces to determine attack signatures and to test the techniques. However, obtaining actual attack traces is difficult, because the high-profile organizations that are typically attacked will not release monitored data as it may contain sensitive information.

Manasdeep proposed Distributed Denial-of-Service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users by using multiple hosts attempting to connect simultaneously to the victim machine. It generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Attackers typically target sites of high-profile web servers such as banks, credit card payment gateways, and even root name servers.

Vern Paxson proposed a number of possible defenses against reflector attacks, finding that most prove impractical, and then assess the degree to which different forms of reflector traffic will have characteristic signatures that the victim can use to identify and filter out the attack traffic. Our analysis indicates that three types of reflectors pose particularly significant threats: DNS and Gnutella servers, and TCP-based servers (particularly Web servers) running on TCP implementations that suffer from predictable initial sequence numbers. We argue in conclusion in support of “reverse ITRACE” [Ba00] and for the utility of packet traceback techniques that work even for low volume flows, such as SPIE.

NathalieWeiler proposed a honeypot for such attacks. The goal is to convincingly simulate the success of the compromise of a system to a potential DDoS attacker. Thereby, we can implement the lessons learned by the honeypot in our other systems to harden them against such attacks. On the other hand, we protect the rest of our network infrastructure form the impact of such an attack. Distributed Denial-of-Service attacks are still a big threat to the Internet. Several proposals for coping with the attacks have been made in the recent past, but neither of them are successful on themselves

Frank Kargl Joern Maier Michael Weber proposed different forms of attacks and give an overview over the most common DDoS tools. Furthermore we present a solution based on Class Based Routing mechanisms in the Linux kernel that will prevent the most severe impacts of DDoS on clusters of web servers with a prepended load balancing server. The goal is to keep the web servers under attack responding to the normal client requests. Some performance tests and a comparison to other approaches conclude our paper. Recently many prominent web sites face so called Distributed Denial of Service Attacks (DDoS). While former security threats could be faced by a tight security policy and active measures like using Firewalls, vendor patches etc. these DDoS are new in such way that there is no completely satisfying protection yet.

Abusayeed Saifullah proposed a novel technique for protecting an internet server from distributed denial-of-service attacks. The defense mechanism is based on a distributed algorithm that performs weight-fair throttling at the upstream routers. The throttling is weight-fair because the traffics destined for the server are controlled (increased or decreased) by the leaky-buckets at the routers based on the number of users connected, directly or through other routers, to each router. To the best of our knowledge, this is the first weightfair technique for saving an internet server from denial-of-service attacks. The system is guaranteed to work even if some of the routers are compromised. Furthermore, in the beginning of the algorithm, the server’s capacity is underestimated by the routers so as to protect the server from any sudden initial attack.

Shibiao Lin Tzi-cker Chiueh proposed taxonomies of the known and potential DDoS attack techniques and tools. Along with this, we discuss the issues and defend challenges in fighting with these attacks. Based on the new understanding of the problem, we propose classes of solutions to detect, survive and react to the DDoS attacks. Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. Researchers have come up with more and more specific solutions to the DDoS problem. However, existing DDoS attack tools keep being improved and new attack techniques are developed. It is desirable to construct comprehensive DDoS solutions to current and future DDoS attack variants rather than to react with specific countermeasures. In order to assist in this, we conduct a thorough survey on the problem of DDoS.

Sugih Jamin proposed An attacker inundates its victim with otherwise legitimate service requests or traffic such that victim's resources are overloaded and overwhelmed to the point that the victim can perform no useful work. A newly emerging, particularly virulent strain of DoS attack enabled by the wide deployment of the Internet. Attacker commandeers systems (zombies) distributed across the Internet to send correlated service requests or traffic to the victim to overload the victim.

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey proposed the idea that Distributed Denial of Service (DDoS) is an increasingly common Internet phenomenon and is capable of silencing Internet speech, usually for a brief interval but occasionally for longer. We explore the specific phenomenon of DDoS attacks on independent media and human rights organizations, seeking to understand the nature and frequency of these attacks, their efficacy, and the responses available to sites under attack. Our report offers advice to independent media and human rights sites likely to be targeted by DDoS but comes to the uncomfortable conclusion that there is no easy solution to these attacks for many of these sites, particularly for attacks that exhaust network bandwidth.

III. PROBLEM FORMULATION

A. Existing work

In this research is to help any network user in mitigating DoS attacks and DDoS in IP-based networks. This dissertation concentrates especially on the following areas:One should understand existing attack mechanisms and available defense mechanisms, and have a rough idea about the benefits (best-case performance) of each defense mechanism. One should acknowledge possible situation dependency of defense mechanisms, and be able to choose the most suitable defense when more than one defense mechanisms are available against a specific attack type. One should evaluate defense mechanisms in a comprehensive way, including both benefits and disadvantages (worst-case performance), as an attacker can exploit any weakness in a defense mechanism. Knowledge of all of these issues is necessary in successful mitigation of DoS and DDOS attacks. Without knowing how a specific defense mechanism works under different possible conditions and what the real benefits and weaknesses are, it is not possible to assure the suitability of a defense mechanism against a certain type of a DoS and DDOS attack.

3.1 Research Methodology

Research methodologies used in this dissertation are primarily based on simulating different attack scenarios, but measurements, mathematical modeling based on game theory, and requirement specification are also used in the publications. The used re-search methodologies are explained in detail later in this dissertation when describing each contribution.

This dissertation studies DoS attacks in computer networks using the Internet Proto-col (IP), namely the Internet and mobile ad hoc networks. DoS attacks in the physical world are not studied here.Majority of the publications in this dissertation concentrate on the fixed (wired) Internet, but most of the presented attack and defense mechanisms are applicable to wireless networks, too. Publications P3 and P4 concentrate only on specific attacks and defenses in wireless mobile ad hoc networks.The emphasis of this research is on DoS attacks in general, and DDoS attacks are treated as a subset of DoS attacks. DDoS attacks are based on the same mechanisms as basic DoS attacks, but there is one exception during the deployment phase. A DDoS tool needs to be installed on many vulnerable hosts. The installation of DoS software on a single vulnerable host is, however, a common prerequisite for most DoS attacks. Thus attack and defense mechanisms described in this dissertation are applicable to both DoS and DDoS attacks.

3.2 Defense Mechanisms Against Denial Of Service Attacks

In risk management one must understand the most important risks and decide how to mitigate them. Risks can be either accepted as such, mitigated by using one or more defense mechanisms, or transferred to third parties (such as with insurances). The primary goal is to ensure business continuity and, at the same time, keep the associated costs at a reasonable level.Effective risk management, however, is not possible without a good knowledge in existing attack mechanisms and available defense mechanisms. A widely exploited attack mechanism can be associated a high risk requiring effective mitigation. Completely different actions should be taken in a risk management process when no defense mechanisms exist against a specific attack, and when effective defense mechanisms can be easily deployed.

3.3 Mitigating Denial of Service Attacks

A comprehensive and structured description about existing DoS attack and defense mechanisms is given here. This section is divided in five parts. The first part describes the role of worms and viruses in creating programmable sets of source hosts for DoS attacks. The second part gives a structured view on existing generic DoS attack mechanisms. The third part describes how to handle DoS attacks in general at a victim site. The fourth part gives a structured list of many existing defense mechanisms against major attack types. The final part in this section discusses the importance of risk management in the process of actually selecting defense mechanisms.

3.4 Attack Mechanisms

Once DoS software has been deployed, an attacker is able to proceed to the final attack phase. An actual attack will consist of a flooding or a logic attack against a single victim.

3.4.1 Coordination of DDoS Agents

In case of a DDoS attack an attacker must first coordinate all DDoS agents to attack in unison for effectiveness reasons. This coordination requires attack commands to be transmitted to every agent through a control channel. There are several choices for transmitting this control channel information, usually in an encrypted form. In it is stated that IRC channels are the most widely used control channel mechanism but web-based channels are used in an increasing fashion by many botnets.

3.4.2 Detection of DoS Attacks

Intrusion Detection Systems (IDSs) are tools for detecting intrusive network or hostactivity, and announcing alerts. These systems can be divided in two major classes. Network Intrusion Detection Systems (NIDSs) are passive nodes which have access to all traffic in a network link. Host Intrusion Detection Systems (HIDSs) are applications which analyze log files and other security related information and try to detect intrusive use of a single host. NIDSs and HIDSs do not have equal advantages and disadvantages, so an important site needs to employ a combination of them.

There are two distinct analysis methods to decide, whether an intrusion has been found or not. Signature-based misuse detection tries to locate known patterns from the incoming sensor data, much like the existing antivirus software does. The major problem with misuse detection is the requirement for exact signatures (fingerprints) of attacks, which makes these kinds of systems reactive and places strict requirements on the speed of signature updating. This means inability to detect new or even slightly modified attacks. Anomaly detection is based on observing significant deviations from typical or expected behavior of systems or users.

The major problem with anomaly detection is the difficulty in defining what is typical or expected behavior and what is not. Anomaly detection systems can detect some new or modified attacks.

3.4.3 Effectiveness of DoS and DDOS Attack Detection

IDSs have proved to be necessary tools for detecting attacks. IDS can provide log files and traces of network traffic which can be used to get further information about the involved hosts and the amount of damages. Later this information can be used as a proof of an attack in lawsuits. IDSs are used in an increasing fashion to show the presence of attacks against corporate and even home networks. Detection of DoS attacks is not simple because these attacks exploit features of ordinary protocol behavior. By choosing an attack method suitably an attacker has the possibility of escaping the detection by IDS.

3.4.4 Reaction against Detected DoS and DDOS Attacks

As was shown in the previous subsection, detection of DoS and it distributed form attacks is not a simple task. An experienced attacker can hide DoS activity. This has implications on the reaction phase. Automatic reaction mechanisms are fast, but the problem with false positives must be tackled somehow. Typically human intervention is required at some moment of time.A prerequisite for the mitigation of DoS and DDOS attacks is a detailed knowledge of the details of an ongoing attack (the characterization sub phase).

If the exact signature of attack traffic is not known, such as in the case of a flooding DoS attack, mitigation mechanisms can easily cause damage for legitimate users. A widely used way to react against DoS attacks has been a labor-intensive manual procedure by network administrators, which means manual input debugging to locate routers on the path of the attack traffic step by step towards the attack source, and manual installation of packet filtering or rate-limiting rules in these routers handling attack traffic. An automatic mechanism is needed for a quick early reaction. The implementation of a reaction mechanism can reside either in an end-host or a network security device. When comparing the two implementation locations, network security devices are better places for reacting against inward flooding and many logic DoS attacks because the attack must be mitigated as near the actual source as possible.

IV. METHODOLOGY

4.1 Technique and methodology

Denial of Service (DoS) attacks are a more serious threat in mobile ad hoc networks than in wired networks due to the complexity, resource constraints, dynamic net-work topology, open network architecture, and shared transmission media. The higher the complexity of a system, the more possibilities there are to be exploited for attack purposes. Resource constraints restrict the ability to handle and withstand attacks due to limited processing power, transmission bandwidth, and lifetime of bat-teries. Dynamic network topology places a burden on routing protocols when trying to achieve short reaction and convergence times. Open network architecture and shared transmission media make it possible to join a network without a physical con-nection. Any of these vulnerabilities can be exploited in a DoS attack to prevent or delay legitimate access to services.

4.2 Simulation work in Ad Hoc Network

The Matlab network simulator was used to investigate the application level performance during range attacks. Two modifications were made to the basic ns 3.5simulator: nodes were allowed to have different transmission ranges, and the infinite loop problem of the DSDV was patched. The structure of the simulated ad hoc network is shown in the figure 2.10. This network consists of six nodes, numbered from 0 to 5. The x- and y-coordinates for a node are indicated in parenthesis below each node. The IEEE 802.11 MAC layer is used in the network. All messages are transmitted with the bandwidth of 1 Mbps.

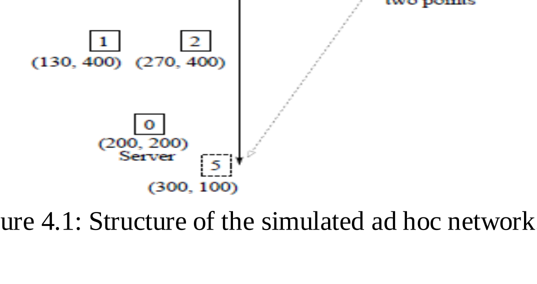

Figure 4.1: Structure of the simulated ad hoc network.

Nodes 0 to 4 are static. The node 5 is moving vertically along the y-axis back and forth between the points (300,700) and (300,100). At the beginning of a simulation it starts moving downwards with the speed of 3 m/s. At the time of 400 seconds it starts moving upwards. The node 5 initiates a movement every 400 seconds. The node 3 is used for the range attack. The default transmission range for all nodes is 250 meters. In the attenuation range attack the range of the node 3 is reduced periodically to 40 meters. In the amplifying attack this range is periodically increased to 550 meters.

Client nodes are downloading web pages from the server node 0 with an exponentially distributed inter-page time, the average value being 30 seconds. These pages are downloaded automatically over the TCP protocol. Each web page contains 2920 bytes, which results in two full-size TCP segments. It is expected that persistent TCP connections are used, so the three-way handshake is not required for initiating a download. It should be noticed that the downloaded information does not necessarily have to be a web page because an application is only expected to use TCP for its transmission purposes.

The transmission delay for a download is the complete time to transmit and acknowledge a single web page. This delay is thus the time from the transmission of the first TCP segment to the reception of the acknowledgement of the second TCP segment at the server node 0.

4.2 The Setup of the Simulator

The topology of the simulated network is shown in the figure 4.2 The legitimate FTP traffic is sent between the FTP client and the FTP server which are attached to the Client router and the Server router, respectively. The RLS router in the middle implements the rate limiting and the related one-way packet loss as an ns-2 error model, which uniformly discards a specific fraction (R) of packets being sent to the Server router. The underlying TCP for FTP applications is of type Reno (TCP/Reno) with a packet size of 1460 bytes. The links between the Client router and the Server router have a bandwidth of 2 Mbps and a delay of 10 ms. The Attack traffic router is connected to the RLS router through a 500 kbps link with a delay of 20 ms.

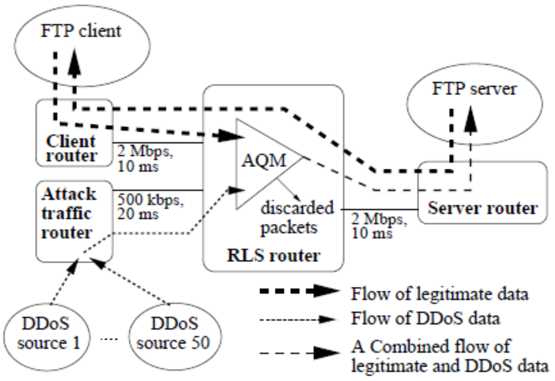

Figure 4.2: The topology of the simulated network. The dotted lines indicate the flow of data. The AQM in the RLS router dis-cards a specific fraction of packets being sent to the FTP server. No packets are discarded by RLS in the reverse direction.

A Distributed DoS (DDoS) attack is simulated in the network with a group of 50 DDoS sources. Each DDoS source sends a large file with the FTP protocol to the FTP server. Attack traffic is thus sent over the TCP protocol (TCP/Reno). These DDoS sources are able to create at most 500 kbps of background traffic due the link bandwidth at the Attack traffic router.The flow of data packets is shown with dotted lines in the figure 4.6 (the flow of TCP acknowledgements from the FTP server to DDoS sources is not shown in this figure).

The FTP client either downloads a large file from the FTP server or uploads a large file to the FTP server. Both legitimate and DDoS FTP packets being forwarded to the Server router are discarded with probability R at the RLS router by an AQM mechanism. The reverse direction for FTP traffic does not encounter any packet loss by the RLS.

4.3 The Effect of One-Way Packet Loss on TCP Throughput

The simulations consisted of the transmission of a very large file for 100 000 sec-onds. This simulation time was chosen because it provided reasonably smooth result curves. The amount of data transmitted during this time was calculated from the final TCP acknowledgement received by the sender. The figure below shows the simulation results for file upload and download tests when no background DDoS traffic was present. Simulation results in the figure 4.8 show the results of the file transfer tests during a DDoS attack.

The x-axis of these figures shows the packet discard probability R. The y-axis shows the average throughput during the whole 100 000 second simulation as bits per second (bps). The solid thick line indicates the throughput of file downloading, and the dotted thick line indicates the throughput of file uploading. The thin dotted line indicates the theoretical TCP throughput according to equation (4.1) (MSS=1460 bytes, RT T =40 ms, and C=0.45). Even though the theoretical curve is shown for the whole x-axis range, it is valid only with relatively small values of R.These simulation results indicate that for file upload the one-way packet discard probability R must be below 0.1 for TCP to have a reasonable average throughput. File download, however, is able to withstand a packet discard probability up to 0.5 before the average throughput starts to decline seriously.

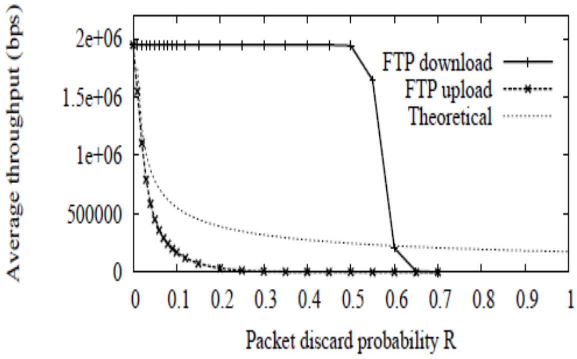

Figure 4.3: The average TCP throughput in the simulator. No background traffic was present.

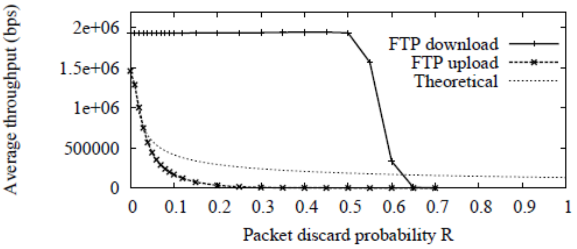

Figure 4.4: The average TCP throughput in the simulator. A flooding DDoS attack was in the background.

The effect of the background DDoS attack is visible only in the throughput of file upload. When uploading a file the bandwidth of the network link from the RLS router to the Server router is shared with the DDoS attack traffic. Two competing types of traffic will share the bandwidth of this link, and less bandwidth is available for legitimate file uploading during a DDoS attack. File downloading is being sent in the reverse direction on this network link, and the DDoS attack does not consume the bandwidth of the link in this direction. Changing the TCP-based DDoS attack traffic to UDP-based (50 Pareto On/Off traffic sources) did not have any visible effect on these results.

The local connection from the RLS router to the FTP server is assumed to provide the full bandwidth for both directions at the same time (for example, by separate wires).

4.4 Proposed Work

Proposed work states defense mechanisms against DoS attacks in wsn under considering of LEACH and CBCR protocol. One very relevant question that has not yet been discussed is whether it is possible to define exactly what defense mechanisms an organization or a user should implement to mitigate these attacks. This is mainly the responsibility of risk management as has been emphasized before in this dissertation. There are, however, many practical problems in risk management in achieving an optimal level of security.Other relevant questions not yet discussed here are related to the reliability of results from simulations and mathematical modeling.

4.5 Detection Algorithm for DOS and its distributed form in WSN

Step 1: Source Node (SN) sends a Request to Restricted IP (RRIP) to the Back Bone Node (BBN).

Step 2: On receiving the Restricted IP (RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously and awaits for reply (RREP)

Step 3: On receiving the RREP, each node forwarding the RREP to the sender matches the RREP nodes with the node entries present in the Malicious Node and Blacklist table maintained at each node in the network. If the nodes in the RREP does not match with the entries in the two tables then the RREP is forwarded towards the sender node S.

Removal process: Step 1: If the RREP is received only to the Destination & not to the Restricted IP (RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole/DDOS detection, by sending a request to the BBN to enter into promiscuous mode

Step 3: The BBN now starts the monitoring of the nodes in the RREP path and sends a PMODE_ON message to the sender node to notify that the promiscuous mode is ON for the BBN.

Step 4: On receiving the PMODE_ON message from BBN the sender node S sends a dummy packet through the same route reply(RREP) for the destination D.

Step 5 The BBN Instruct all neighbors of Nrrep (of the node sending route reply message to S) to vote for the next node to which Nrrep is forwarding packets originating from S and destined to D.

Step 6: On receiving node ids from neighbors of Nrrep, BBN elects the next node to which Nrrep is forwarding the packets based on reported reference counts.

Step 7: If dummy packet is sent to the next node in the path which is the same node as the elected node then we replace the elected node as the Nrrep node and we verify the next node for the new Nrrep node with the help of neighbors of new Nrrep.

Step 8 If the elected node is a null node, Nrrep is itself dropping all the packets. We cross verify the malicious behavior of the elected node with the simultaneous dropping of dummy packet by the same node in the network.

Step 9: On detection of the malicious node, its node ID is broadcasted to the remaining nodes in the network including the sender node. The other nodes in the network then append this malicious node entry in the Malicious Node table which is maintained at each node in the network and its count is set to 1.

4.7 CLUSTER BASED ROUTING PROTOCOL (CBRP) In WSN

The energy consumption is one of main challenges in Wireless Sensor Network (WSN).Also packet loss that occur due tomobility of the sensor nodes as well as effective bandwidth utilization are at the concern in wireless sensor network applications. So CBRP is proposed for the same.

A. Need for CBRP

To overcome the issues of DoS and DDoS in WSN, cluster based routing protocol is proposed. It is on-demand and hierarchical routing protocol. Due to the nature of mobile nodes in the networks it is non-trivial problem to find path from source to the destination and perform the communication between nodes for a long period of time. Proactive routing protocols are not appropriate for mobile ad hoc networks, as they continuously use a large portion of the network capacity to keep the routing information. So the reactive protocols are used for WSN. The basic idea of on-demand routing protocols, is that a source node sends a route request and makes routing decision based on received route reply, which may be sent by destination or intermediate node. On-demand routing has several advantages, such as simplicity, correctness and flexibility.

In cluster-based routing, the network is dynamically organized into partitions called clusters with the objective of maintaining a relatively stable effective topology. [5] In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. Cluster based routing protocol (CBRP) define new algorithm for cluster head election that can better handle heterogeneous energy circumstances than existing clustering algorithms. Which elect the cluster head only based on a node's own residual energy.

B. Cluster Based Routing Algorithm

1. Clustering routing algorithm is used to find out intra cluster and inter cluster link in wireless sensor network clusters are acted as a router, which maintain and distribute of the routing information.

2. After node is selected as cluster head, it will broadcast information that he is the cluster head to the rest of the nodes in the same cluster. The remaining nodes decide to join the cluster according to the size of the received signal.

3. On the other hand, when the sensor node does not receive data request message from the cluster head it will try to establish new membership with new cluster to avoid packet loss.

4. When the sensor node receives data request message from cluster head but it has no data to send, the node will not occupy any time slot. Thus, the timeslot will be assigned to another member who has data to send.

5. This adaptive protocol can avoid wastage of timeslot, hence ensure efficient bandwidth utilization. Each cluster head keep some free timeslot to enable other incoming nodes from other cluster to join its cluster.

6. Overall implementation of CBRP consists of two phases:

a) Setup phase - It includes cluster head election, advertisement, decision and schedule creation.

b) Steady phase -Sending data to cluster head takes place.

V. RESULT

Result and discussion under simulation Simulations

All simulations used in this dissertation are terminating simulations with a finite time horizon. The duration of a simulation is thus predetermined by the total simulation time which is clearly stated in all simulation-based publications. We introduce the DOS and DDOS attack in WSN and calculate the energy level and number of dead node in time domain analysis over the successive iteration.

5.1 Simulation Parameters

Parameter	Value
Network Size	[100 100];
Number Of Sensor Nodes	100
Sensor Node Deployment	Uniform Random
Percentage Of Cluster Head	5
Data_Packet_Size	=128
Energy_Th	10e-3
Eelec	=50e-9
Efs	=10e-12
Eda	=5e-9
Mobility Model	Random Way Point Model
Data_Packet_Size	=128
Broadcast_Packet_Size	=24
Transimission_Range	=20
Zoom	=10
Communication Radius	D0=87.71

5.2 Simulation Output

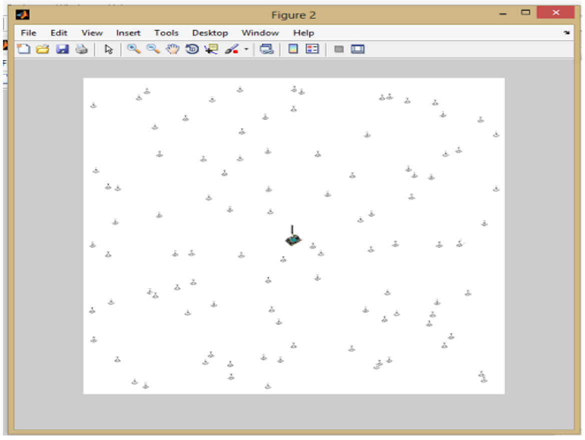

Figure 5.1: 100 Nodes Created in WSN Arena

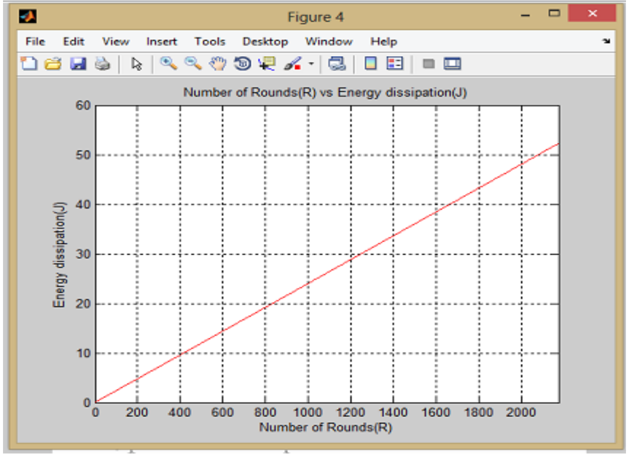

Figure 5.2: Number of Rounds Vs Energy Dissipation

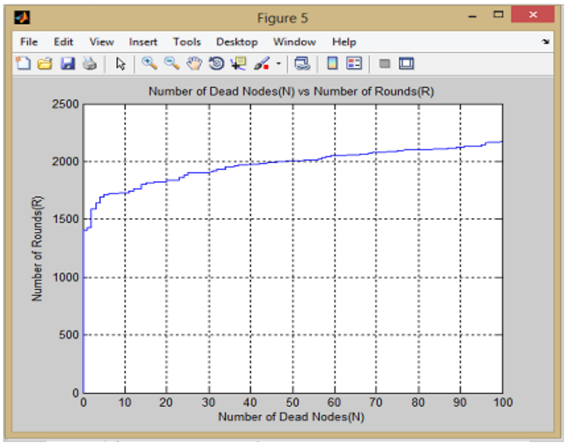

Figure 5.3: Number of Dead Nodes Vs Number of Rounds

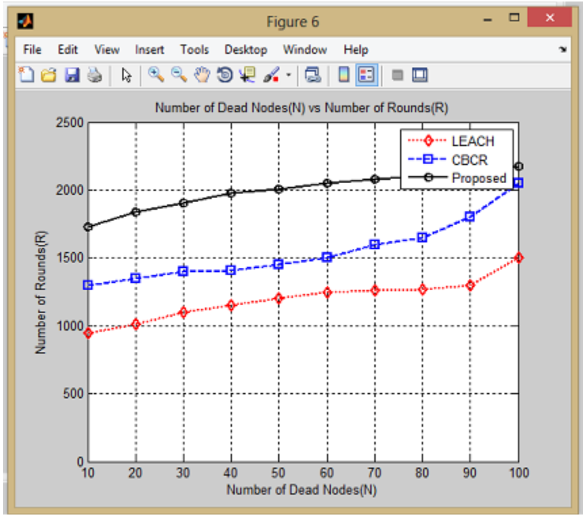

Figure 5.4: Number of Dead Nodes Vs Number of Rounds (LEACH, CBCR and Proposed)

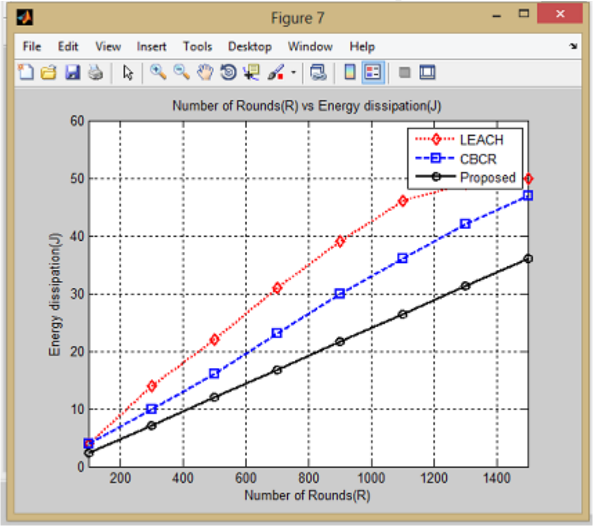

Figure 5.5: Number of Rounds Vs Energy Dissipation (LEACH, CBCR and Proposed)

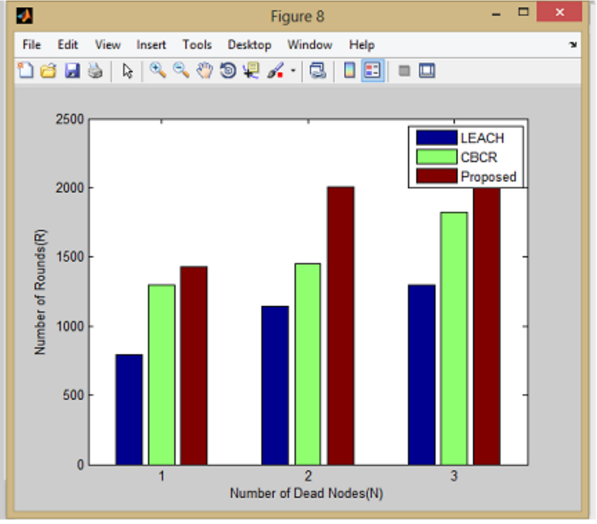

Figure 5.6: Number of Dead Nodes Vs Number of Rounds (LEACH, CBCR and Proposed)

5.3 Comparison of different attack mechanisms

This dissertation described therange attack as a new attack mechanism against ad hoc networks. In the dissertation it was not investigated whether this new attack would be the worst possible attack mechanism in any realistic situation. It would be interesting to compare the effectiveness of the range attack with other attack mechanisms, such as destroying a wireless node or blocking an antenna permanently. The range attack is more difficult to detect than the loss of a node, but a lost node may force an ad hoc network to be partitioned permanently, depending on the mobility and topology of the network. An enemy's decision on choosing an attack mechanism depends, for example, on how much one can degrade the network performance, how much effort is needed to carry out an attack, and how long an attack can be continued without being detected and mitigated.

VI. CONCLUSION AND FUTURE WORK

Conclusions and Future Work

DoS attacks and distributed DoS are a part of an overall risk management strategy for an organization. Each organization must identify the most important DoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DoS attacks should not thus be underestimated, but not overestimated, either. In the future the problem from DoS attacks will most probably increase because the number of hosts connected in the Internet increases, access lines get faster, soft-ware products get more complex, and security continues to be difficult for an ordinary home user and even many organizations. The more there are hosts in the Internet, the more of them can potentially be used for DoS purposes. The intensity of DoS attacks can also increase, as a higher number of hosts can produce more traffic over faster Internet access lines. As software gets more complex, more vulnerability will reside in them to be used for compromising hosts. The fast pace of new revisions does not make the situation easier. Finally, it will continue to be difficult to evaluate security risks in existing computer systems, especially by ordinary people.

REFERENCES

[1] Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay “A Survey of Bots Used for Distributed Denial of Service Attacks” Department of Computing, Imperial College London, 180 Queen’s Gate, SW7 2AZ, London, United Kingdom. {vlt, mss, nd}@doc.ic.ac.uk WWW home page: http://www.doc.ic.ac.uk.

[2] Manasdeep “Distributed Denial-of-Service Testing and Methodology” Network Intelligence (India) Pvt. Ltd. 204 Ecospace,Old Nagardas Road, Near Andheri Subway, Andheri.

[3] Vern Paxson “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks” To appear in Computer Communication Review 31(3), July 2001.

[4] NathalieWeiler “Honeypots for Distributed Denial of Service Attacks” Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02) 1080-1383/02 $17.00 © 2002 IEEE.

[5] Frank Kargl Joern Maier Michael Weber “Protecting Web Servers from Distributed Denial of Service Attacks” Copyright is held by the author/owner. WWW10, May 1-5, 2001, Hong Kong. ACM 1-58113-348-0/01/0005. 514

[6] Abusayeed Saifullah “Defending against Distributed Denial-of Service Attacks with Weight-Fair Router Throttles” Department of Computer Science and Engineering Washington University in St. Louis saifullaha@cse.wustl.edu

[7] Shibiao Lin Tzi-cker Chiueh “A Survey on Solutions to Distributed Denial of Service Attacks” Department of Computer Science Stony Brook University, Stony Brook, NY-11794.

[8] Sugih Jamin “Detection and Blocking of Distributed Denial of Service Attack” EECS Department University of Michigan jamin@eecs.umich.edu.

[9] Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey “Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites” The Berkman Center for Internet & Society at Harvard University December 2010