# RE EVOLUTION AND DETECTION OF DOS AND DDOS ATTACK FOR ORGANIZED WSN: A REVIEW

Ramesh Kumar Shukla[1], Mr. Nitin Kumar[2]
[1]M.Tech (ECE), [2]Asst Prof. Dept of Electronics & Communication Engg., GITAM, Kablana

***Abstract: This paper demonstrates denial of service (DoS) attacks and DDoS attack in computer networks. The goal of these attacks is to prevent availability of network services from their legitimate users. This dissertation presents a structured view on possible attack and defense mechanisms, describes some new defense mechanisms, and provides new in-formation on selecting and evaluating defense mechanisms. Defending against DoS attacks and its distributed form is network and computer security. As scientific disciplines, network and computer security are relatively new. An indication of this is that even computer security terminology has not yet stabilized. Computer and network security were first studied in the early 1970s, and some of these earliest security papers are listed and available in survey. Denials of Service attacks are a timely and extremely important research topic. According to the CSI/FBI computer crime and security survey in the United States for the year 2004 ,DoS attacks are the second most widely detected outsider attack type in computer networks, immediately after virus infections. A computer crime and security survey in Australia for the year 2004 gives similar results. It is currently not possible to prevent DoS attacks and DDoS because many of these attacks are based on using ordinary protocols and services in an overwhelming manner. Specific security holes in the victim hosts or networks are thus not necessarily needed. For this reason we can only mitigate these attacks.***
***Keywords: DDOS, DOS,WSN, BBN, Node ID, AODV***

## I. INTRODUCTION

Denial of Service (DoS) attacks has proved to be a serious and permanent threat to users, organizations, and infrastructures of the Internet. 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.

### *1.1 DOS ATTACKS IN REAL-LIFE*

Real DoS incidents in the Internet between the years 1989 and 1995 were investigated. 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 GENERAL SECURITY TERMINOLOGY*

The subject of this dissertation is related to security in computer networks, that is network security. Generally the word security can be preceded by practically any asset to be protected, such as software security and computer security. Terms related to security do not unfortunately have any single definition and are seldom defined even roughly. One reason for this is that computer security is still in the early days of the discipline. Dieter Gollmann has described well the problem with security terminology Information security: A continuous process towards reasonable protection of information against unauthorized disclosure, transfer, modification, destruction, or control. Information security does not require information to be processed with computers or to be in electronic format.

#### *1.2.1 COMPUTER SECURITY:*

A continuous process towards a reasonably good prevention and detection of unauthorized actions by users of a computer system. Most existing computers are connected to networks, so network security is important.

#### *1.2.2 NETWORK SECURITY:*

A continuous process towards meeting reasonable objectives of providing confidentiality, integrity, availability, and access for legitimate users of network resources .The difference between computer security and network security has blurred as most computers (or hosts) are connected to networks, and practically any host can be accessed through a network in a similar way as sitting physically in front of it.

- Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. For systems, integrity is defined as the quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.
- Availability: The property of a system or a system resource being accessible and usable upon demand by an authorized entity, according to performance specifications for the system.
- Dependability: The ability to deliver service that can justifiably be trusted.Finally some widely used

  

definitions related to security will be defined.

- Vulnerability: A flaw in security procedures, software, internal system controls, or implementation of an (information) system that may affect the integrity, confidentiality, accountability, and/or availability of data or services.

*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.

## II. LITERATURE SURVEY

Routing in ad hoc networks is significantly different from routing in ordinary wired networks [16]. The wireless medium makes it possible to transmit a message to any node within the transmission range of a sender, and dynamic network topologies place heavy requirements on the convergence characteristics of routing protocols. As the name implies, ad hoc networks can be used to construct temporary networks without administrative intervention or any specific infrastructure devices. Correct behavior of all nodes is required, but as expressed in [2], cooperation is assumed but not enforced in mobile ad hoc networks. Even a single malicious node can thus harm routing in a whole ad hoc network. This makes ad hoc routing an attractive target for denial of service (DoS) attacks. The range attack described below is a new DoS and it distributed form attack against ad-hoc routing. It is based on changing periodically the transmission range of a wireless node. There is no need to compromise any node because an attacker only has to get close enough to the antenna of a node to be used for the range attack. The goal of this attack is to cause frequent topology changes.It is analyzed below how the range attack affects application level delays when end-users are downloading web pages from a server node

## III. SCOPE OF WORK

In this research is to help any network user in mitigating DoS attacks and DDoS in IP based network. This dissertation concentrates especially on the said 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.

## IV. 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.

*4.1 BACKGROUND*

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 batteries. 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 connection. Any of these vulnerabilities can be exploited in a DoS attack to prevent or delay legitimate access to services. The primary contribution here is to investigate resilience of three ad-hoc routing protocols against the attenuating range attack which is a new DoS attack against ad-hoc routing. The routing protocols are the Destination-Sequenced Distance-Vector (DSDV), the Ad hoc On-demand Distance-Vector (AODV), and the Dynamic Source Routing (DSR) protocols. The research methodology is based on using the ns-2 network simulator for analyzing the transmission delay in a small ad hoc network. One node of this ad hoc network is used by an enemy to carry out the range attack. It is argued in this paper that effectiveness of DoS defense mechanisms is situation dependent, that is, different defense mechanisms are useful for different applications. The simulation results indicate that DSDV provides the highest resilience against the range attack when applications require a very short transmission delay less or equal to 0.1 seconds. When applications tolerate a longer delay up to 2 seconds, AODV was found to provide the highest resilience against the range attack. Intrusion Detection Systems (IDS) can be used to detect DoS attacks. Reliable detection, however, is not always possible. A well-managed IDS is able to detect many real attack flows (true positives), but it will also miss detect some legitimate flows as attack flows (false positives).

## V. PROPOSED WORK

Proposed work states defense mechanisms against DoS attacks. 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 mit-igate 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.

*5.1 SUBJECTIVITY IN SECURITY*

Security is a controversial issue. When there have been no security incidents for a relatively long period of time, security is easily perceived to be too expensive, and it can be impossible to increase the level of security against new kinds of risks.

*5.2 DYNAMICALLY CHANGING RISKS*

The set of possible risks is not static. We cannot know all possible risks to prepare against, as new vulnerabilities can be encountered any day. Existing risks also change their severity. One day an issue can be classified as having a very low risk, but the next day it can be associated a high risk.

*5.3 PROPOSED TECHNIQUE*

Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously.

*5.4 NETWORK MODEL & ASSUMPTIO*

We approach this problem by selecting some nodes which are trustworthy and powerful in terms of battery power and range. These nodes which are referred to as Back Bone Nodes (BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the number of normal nodes are more than the number of DOS/DDOS nodes at any point of time.

*5.4.1 Allocation of IP address*

The IP address configuration in case of MANETs can broadly be classified into- i.Stateless approach ii. State full approach In the stateless approach an unconfigured host must obtain its own IP address by self assignment. This stateless approach adopts random address assignment and is followed by duplicate address detection mechanism to achieve address uniqueness. Stateless approaches do not keep any allocation.

## VI. COCLUSION 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.

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.

## REFERENCES

[1] Imad Aad, JeanPierre Hubaux and Edward W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," ," in Proceedings of the ACM MobiCom, Philadelphia, USA, Sept. 2004, pp. 202–215.

[2] 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 VOLUME 3 - NUMBER 4 , pp. 1-9

[3] Rizwan Khan and 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, NO. 11, October 2011 pp. 646-655

[4] Rachid Haboub and Mohammed Ouzzif, "secure and reliable routing in mobile adhoc networks," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012.

[5] Ankur Bawiskar and Dr. B.B. Meshram, "Survey of Attacks on Wireless Network," International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 1, March 2013.pp. 90-100

[6] Chitra Kiran N and Dr. G. Narendra Kumar, "Modelling Efficient Process Oriented Architecture for Secure Mobile Commerce Using Hybrid Routing Protocol in Mobile Adhoc Network," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 , pp.311-321.

[7] J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner, "State of the practice of intrusion detection technologies," Carnegie Mellon University, Software Engineering Institute, Tech. Rep. CMU/SEI-99-TR-028, Jan. 2000.

[8] D. Adkins, K. Lakshminarayanan, A. Perrig, and I. Stoica, "Towards a more functional and secure network infrastructure," University of California, Berkeley, Tech. Rep. UCB/CSD-03-1242, 2003.

[9] K. Agarwal and W. Wang, "An experimental study of cross-layer security protocols in public access wireless networks," in Proceedings of the IEEE GLOBECOM, St. Louis, USA, Nov. 2005.

[10] D. Ahmad, "The rising threat of vulnerabilities due to integer errors," IEEE Security & Privacy, vol. 1, no. 4, pp. 77–82, July/Aug. 2003.

  