www.ijiarec.com

NOV 2013

International Journal of Intellectual Advancements and Research in Engineering Computations

A STRATEGY FOR DEFENDING PACKETS AGAINST RECOGNIZED INTERNAL JAMMERS IN WIRELESS SENSOR NETWORKS

*1K.Manojkumar, 2M.Vinoth Kumar, 3Dr.G.Tholkappia Arasu

ABSTRACT

Denial of Service attacks poses a serious threat to the intended service provided to the users. Detection of the jammers is quite easy in case of external locality since they possess a significant pattern of attack and route to attack the victim. Being an internal attacker, the node would have adequate knowledge over the present defensive mechanism and additional tools to masquerade their identity. The proposed method includes a detection technique for identifying the internal compromised node based on the location attributes and markings of the packets. The packets are transmitted towards the destination node using dedicated channels and timing without the disclosure of the keys for decrypting the message to every user node. This method involves the detection of a attack with the help of marked attributes in the packet. The hash function marks all the blocks of the message, with the link to the preceding and succeeding packet. All the packets are required to reassemble the whole meaningful message. The packets without those attributes would be regarded as the attack packet. On detection of the attack, a dynamic routing algorithm would determine the least used bandwidth for previous communication and allocates a dedicated channel between the source and destination.

Index terms: Denial of Service, Network Security, Detection, Message Splitting, Dynamic Routing Algorithm.

I INTRODUCTION

The modern era has now extremely advanced and well-developed and the basic reason for this development is actually the launch of the internet and its applications which have provided the individuals with the easiest routine in their daily lives. The internet has changed the face of the lives of people, turning them completely into the modern and latest lifestyle with its developments. Today, instead of the newspapers, the people use the internet to access the E-news which provides with not only the newspapers completely but also from the various news channels from all over the world. Even the live video news from the news channels can be accessed through the net, overpowering the other media, even including the television.

The internet is indeed the major advancement in the modern era, enabling the common people to sit at home and know the world. Network security starts from authenticating any user with a username and a password. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective measures are needed to prevent unauthorized access, this component fails to check potentially harmful content such as computer worms being transmitted over the network. An Intrusion Prevention System (IPS) helps to detect and inhibit the action of such malware. An Anomaly-Based Intrusion Detection System Eric et al (2004) monitors network traffic for suspicious content, unexpected traffic and other anomalies protect the network e.g. from denial of service attacks or an employee accessing files at odd times. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a high level analysis later.

II PROBLEM AND ANALYSIS

The investigative and defense process should begin immediately after an attack begins. The easiest way to survive an attack is to have planned for the attack. Having a separate emergency block of Internet Protocol (IP) addresses for critical servers with a separate route can be invaluable Alvaro et al (2004). A separate route perhaps a Digital Subscriber Line (DSL) is not that extravagant, and it can be used for load

Author for Correspondence:

*1K.Manojkumar, PG Scholar, Dept of Computer Science and Engg, K.S.R.College of Engineering, Tiruchengode, Tamilnadu, India. E-mail: rtrmano@gmail.com.

2M.Vinoth kumar, Assistant Professor, Dept of Computer Science and Engg , K.S.R.College of Engineering, Tiruchengode, Tamilnadu, India.

3Dr.G.Tholkappia Arasu, Principal, A.V.S Engineering College, Salem, Tamilnadu, India.

balancing or sharing under normal circumstances and switched to emergency mode in the event of an attack. Filtering is often ineffective, as the route to the filter will normally be swamped. So only a trickle of traffic will survive. However, by using an extremely resilient stateful packet filter that will inexpensively drop any unwanted packets, surviving a DoS attack becomes much easier. When such a high performance packet filtering server is attached to an ultra-high bandwidth connection (preferably an internet backbone), communication with the outside world will be unimpaired so long as not all of the available bandwidth is saturated, and performance behind the packet filter will remain normal as long as the packet filter drops all DoS packets. It should be noted however, that in this case the victim of the DoS attack still would need to pay for the excessive bandwidth. The price of service unavailability thus needs to be weighed against the price of truly exorbitant bandwidth/traffic.

Intrusion-Prevention Systems are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior based DoS attacks. An Application Specific Integrated Circuit (ASIC) based IPS can detect and block attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way. A Rate-Based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is traffic anomaly. It must let the legitimate traffic flow while blocking the attack traffic.

III SOLUTION AND MECHANISM

The investigative and defense process should begin immediately after an attack begins. The easiest way to survive an attack is to have planned for the attack. Having a separate emergency block of Internet Protocol (IP) addresses for critical servers with a separate route can be invaluable Alvaro et al (2004). A separate route perhaps a Digital Subscriber Line (DSL) is not that extravagant, and it can be used for load

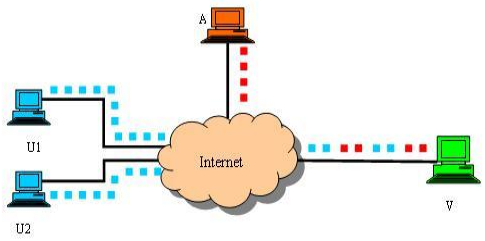
balancing or sharing under normal circumstances and switched to emergency mode in the event of an attack.

Filtering is often ineffective, as the route to the filter will normally be swamped. So only a trickle of traffic will survive. However, by using an extremely resilient stateful packet filter that will inexpensively drop any unwanted packets, surviving a DoS attack becomes much easier. When such a high performance packet filtering server is attached to an ultra-high bandwidth connection (preferably an internet backbone), communication with the outside world will be unimpaired so long as not all of the available bandwidth is saturated, and performance behind the packet filter will remain normal as long as the packet filter drops all DoS packets. It should be noted however, that in this case the victim of the DoS attack still would need to pay for the excessive bandwidth. The price of service unavailability thus needs to be weighed against the price of truly exorbitant bandwidth/traffic.

Intrusion-Prevention Systems are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior based DoS attacks. An Application Specific Integrated Circuit (ASIC) based IPS can detect and block attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way. A Rate-Based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is traffic anomaly. It must let the legitimate traffic flow while blocking the attack traffic.

DENIAL OF SERVICE

In general terms, Denial of Service attacks as shown in Figure 1.1 are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.



U1, U2- Legitimate User, A- Attacker, V- victim

Figure 1 Denial of Service Attack

Symptoms of denial of service attacks include unusually slow network performance (opening files or accessing web sites), unavailability of a particular web site and inability to access any web site. Such attacks can be perpetrated in a number of ways Bao-Tung Wang and Henning Schulzrinne (2004). The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time, causing resource starvation and preventing any useful work from occurring.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

DISTRIBUTED DENIAL OF SERVICE

A Distributed Denial of Service occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The five major components of a Distributed Denial of Service attack are

Client - an application that can be used to initiate attacks by sending commands to other components, also called the attacker or intruder.

Daemon - a process running on an agent, responsible for receiving and carrying out commands issued by a client, also called bcast (broadcast program).

Handler - a host running a client also called master.

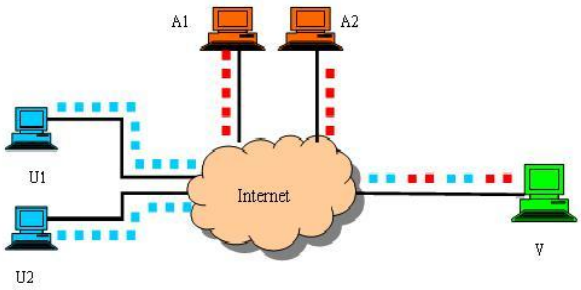
Agent - a host running a daemon, also called zombie.

Victim - the target (a host or network) of a distributed attack.

Distributed Denial of Service attacks involves breaking into hundreds or thousands of machines all over the Internet (Stephen 2004). The attacker then installs Distributed Denial of Service software on them, allowing them to control all these burgled machines to launch coordinated attack on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stacks resources, breaking network connectivity to the victims.

These systems are compromised by attackers using a variety of methods. Malware can carry Distributed Denial of Service attack mechanisms as shown in Figure 1.2; one of the better-known examples of this was "MyDoom". Its Denial of Service mechanism was triggered on a specific date and time. This type of Distributed Denial of Service involved hard coding the target IP address prior to the release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent (or the trojan may contain one). Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web.



U1, U2- Legitimate User, A1, A2 - Attacker, V- victim

Figure.2 Distributed Denial of Service Attack

Stacheldraht is a classic example of a Distributed Denial of Service tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the Distributed Denial of Service attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.

Botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users. More sophisticated attackers use Distributed Denial of Service tools for the purposes of extortion — even against their business rivals. Jammers are a serious threat to the confidentiality and integrity of a network being wired or of wireless nature. In wireless networks, a considerable amount of

effort is reduced to the jammer to present him into the services. Detection and preventive strategies are presented with innovative options to keep the jammer away. The report concentrates on the more severe case of internal jammers, with enough knowledge on the structure of the network. This method mentioned has defined a new approach to mark the packets with certain identity of lesser computations required rather than complex and space consuming Packet Marking Techniques. The marking technique would strive to maintain the order and identity of the original message irrespective of the sequence of reception at the other end. Since the sequential order is alone marked, efficiency is gained in proper and faster reassembly of the message construction. Retransmit protocols would effectively request for the missing order in case of jamming. Organizing the list of frequencies used for previous communications enables the better usage of resources allocated for reassignment of a secure channel between the intended source and destination nodes.

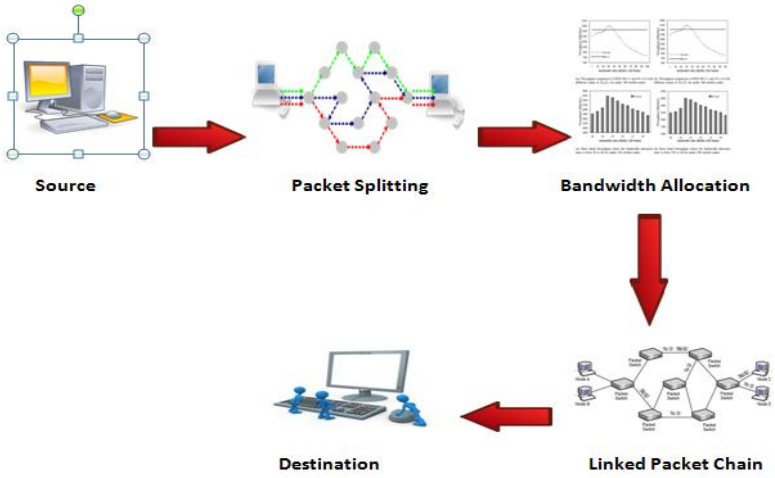


Fig 3: System architecture

PACKET SPLITTING

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'. By itself, small packets will not evade any IDS that reassemble packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet reassemblers but not the target computer.

Fragmentation

The Internet Protocol (IP) show datagram fragmentation, breaking it into smaller pieces, so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The Identification field, and Fragment offset field along with Don't Fragment and More Fragment flags in the IP protocol header are used for fragmentation and reassembly of IP datagrams.

In a case where a router receives a protocol data unit (PDU) larger than the next hop's MTU, it has two options if the transport is IPv4. Drop the PDU and send an Internet Control Message Protocol (ICMP) message which indicates the condition Packet too Big, or to fragment the IP packet and send it over the link with a smaller MTU. IPv6 hosts are required to determine the optimal Path MTU before sending packets; however, it is guaranteed that any IPv6 packet smaller than or equal to 1280 bytes must be deliverable without the need to use IPv6 fragmentation.

If a receiving host receives a fragmented IP packet, it has to reassemble the datagram and pass it to the higher protocol layer. Reassembly is intended to happen in the receiving host but in practice it may be done by an intermediate router, for example, network address translation may need to re-assemble fragments in order to translate data streams, e.g. the FTP control protocol.

IP fragmentation can cause excessive retransmissions when fragments encounter packet loss and reliable protocols such as TCP must retransmit all of the fragments in order to recover from the loss of a single fragment. Thus, senders typically use two approaches to decide the size of IP datagrams to send over the network. The first is for the sending host to

send an IP datagram of size equal to the MTU of the first hop of the source destination pair. The second is to run the path MTU discovery algorithm, to determine the path MTU between two IP hosts, so that IP fragmentation can be avoided.

BANDWIDTH ALLOCATION

Protocol Substitution (aka protocol proxy)

Any chatty protocol (a protocol that involves lots of back-and-forth messaging between peers, or clients and servers) typically doesn't behave well when extended across wide-area links. Where outright protocol substitution isn't feasible, many WAN bandwidth optimization devices terminate protocol connections for things such as CIFS (Common Internet File System) locally, then substitute another more streamlined protocol to encapsulate key traffic elements across wide-area links. In action, a 30 MB file transfer may take as long as seven minutes across a WAN link using CIFS, but that delay can be reduced to under a minute using Riverbed's wide-area file services (WAFS) instead.

Traffic shaping and management

WAN optimization devices can apply all kinds of traffic shaping and management techniques to speed time- or latency-sensitive packets on their way while relegating time- or latency-insensitive packets to available bandwidth that might otherwise go unused over time. When traffic shaping is applied to a set of packets (which is usually called a flow or a stream) it imposes additional delays on some packets so that they conform to a predefined set of constraints called a traffic contract or a traffic profile. This lets WAN devices control the volume of traffic sent across a link over a specific period (known as bandwidth throttling) or the maximum rate at which traffic may transit the link (known as rate limiting). Sometimes, more complex regimes may also be applied, such as the generic cell rate algorithm used to shape traffic on ATM networks.

Traffic prioritization and grooming

Some traffic needs to go faster than others or, at least, be subject to minimal or predefined ceilings on latency. Prioritization essentially pushes such traffic to the head of all the queues under its control and helps speed such packets on their way. This is a natural consequence of quality of service (QoS) regimes or of service-level agreement (SLA) guarantees for latency, throughput, response time and so forth. WAN optimization devices play key roles in helping to define, monitor and manage QoS and other priority schemes.

Traffic grooming ensures not only that bandwidth is subject to priority but that unwanted or potentially dangerous protocols are either blocked from accessing a WAN link or limited to exceedingly small bandwidth allocations. Think about various peer-to-peer protocols that don't have legitimate business uses or various kinds of streaming multimedia protocols for watching movies or videos that have no normal place at work. Traffic grooming can prevent such protocols from consuming precious bandwidth. Many experts believe that minuscule allocations for such protocols are desirable because they permit such traffic to move and thus can trace traffic back to senders or receivers of the same.

SECURITY

Link State Packet (LSP) is a packet of information generated by a network router in a link state routing protocol that lists the router's neighbors. Link state packet can also be further defined as special datagrams that determine the names of and the cost or distance to any neighboring routers and associated networks. They are used to efficiently determine what the new neighbor is, if a link failure occurs, and the cost of changing a link if the need arises. LSPs are queued for transmission, and must time out at about the same time. They must be acknowledged, and can be distributed throughout the network, but cannot use the routing database.

Linked State Packets chain

When Information needed for exchange is collected, a router then builds a packet containing all the data. The packet starts with the identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbor, the delay to that neighbor is given. Building a link state packet is usually easy; the complex part is determining when to build them. One way to reduce this problem is to build them periodically, that is, at regular intervals, or when some significant event occurs, such as a line or neighbor going down or coming back up again, or changing its properties appreciatively.

A major procedure called flooding which is used for distributing link state algorithms throughout the routing domain can be implemented with link state packets. However, ordinary flooding may result in problems, because it generates exponential behavior. Smart flooding, on the other hand, recognizes link state packets appropriately.

IV CONCLUSION

The message sent from the source to destination is divided into a set of optimal number of packets for faster and efficient communication. The security implemented in those separated packets. Each packet is marked with the attributes with the ideology of establishing an association in between them and thus security. Packets without the identity marks are discarded at the moment they arrive at the destination considering them as the attack of a jammer. Different mechanisms have been analyzed and the optimal strategy is implemented in the phase. The bandwidth allocation is implied to enable connectivity between the source and destination. Allocated bandwidth is secured and defined to be constant, additional mechanisms are analyzed to meet the congestion control strategies and other problem of peak time traffic. Wastage of

network's resources is eliminated to the maximum extent in this phase. Thus security of the packets is conserved by a packet marking technique and a secure channel of communication.

FUTURE WORK

The positive and degradation effects of the jammers are analyzed after discussing the types of jammers, the models of attacks and the efficiency of today's world. This paper supports the installation of such high efficient and reliable jammer networks to enhance the security level of the important applications and domestic usage. The jammers need to be eradicated to improve the efficiency and security of the wireless network. The compatibility and usability enhanced the jammers intrusion. Controls and additional conditions on the framework of the wireless networks could possibly mitigate the jamming attacks. Since every attack is unique, a general strategy cannot be designed to solve all modes of attacks. Hence a solution which is the ultimate and fruitful for major attacks needs to be framed and implemented.

REFERENCES

[1] Alejandro Proano and Loukas Lazos. "Packet-Hiding Methods for Preventing Selective Jamming Attacks," *IEEE Transactions on dependable and secure computing*, Vol. 9, No. 1, January/February 2012.

[2] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. "Reactive jamming in wireless networks: How realistic is the threat?," *In Proceedings of WiSec*, 2011

[3] Y. Liu, P. Ning, H. Dai, and A. Liu. "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," In *Proceedings of INFOCOM*, San Diego, 2010.

[4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P.Harteland P. Havinga. "Energy-efficient link-layer jamming attacks against WSN MAC Protocols," ACM Transactions on Sensors Networks, 5(1):1–38, 2009.

[5] L. Lazos, S. Liu, and M. Krunz. "Mitigating control-Channel Jamming attacks in multi-channel adhoc Networks," In Proceedings of the 2ndACM conference on wireless network security, pages 169–180, 2009

[6] M. Strasser, C. Popper, and S. Capkun. "Efficient uncoordinated fhss anti-jamming communication," *In Proceedings of MobiHoc*, pages 207–218, 2009.

[7] P. Tague, M. Li, and R. Poovendran. "Mitigation of control channel jamming under node capture attacks," *IEEE Transactions on Mobile Computing*, 8(9):1221–1234, 2009.

[8] M. Strasser, C. Popper, S. Capkun, and M. Cagalj. "Jamming-resistant key establishment using uncoordinated frequency hopping," *In Proceedings of IEEE Symposium on Security and Privacy*, 2008.

[9] W. Xu, W. Trappe, and Y. Zhang. "Anti-jamming timing channels for wireless networks," *In Proceedings of WiSec*, pages 203–213, 2008.

[10] M. Cagalj, S. Capkun, and J.-P. Hubaux. "Wormhole-based antijamming techniques in sensor networks," *IEEE Transactions on Mobile Computing*, 6(1):100–114, 2007.