ISSN:2348-2079

MAR-2014

International Journal of Intellectual Advancements and Research in Engineering Computations

TWO WAY CHAINED PACKETS MARKING TECHNIQUE FOR SECURE COMMUNICATION IN WIRELESS SENSOR NETWORKS

[*1]Dr.C.Chandrasekar, [*2] V.Prabhakaran,M.Phil.,

ABSTRACT

Wireless Sensor Networks, at the outset, used in military applications for sensitive data recordings and transfer which obviously limits the participation of mankind. Today wireless Sensor Networks has entered and proved its efficiency in almost every application. Yet there are some metrics to holdback the security of the same, due to the very own attractive features of flexibility and open nature. Jamming of the medium to deny the service of a legitimate user is one among the many vulnerabilities of a wireless Sensor Network. This paper intends to provide a scheme for detecting the attack by a bidirectional link between the packets and recognizing any off the chain packets at the boundary routers. Prevention of any mishap packets from entering into the network improves the security of the network. A novel approach of marking the neighborhood packets forms a chain of legitimate message will preserve the originality at the other end and any packets to be found without the link information will be eliminated at the perimeter. This approach intends to provide a secure environment which withstands detection and mitigation as the principle.

Index terms: Jamming, Bi-directional, Packets, Legitimate, Information.

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. Any piece of information regarding anything in our daily lives, may it be a cosmetic technique for the ladies or the men health problems, the cooking recipes for trying the new dishes or the home decoration tips, the information on the latest appliance or product you are going to buy or the search for the new house, there it is already on the internet. The interconnected computer networks use the standardized Internet Protocol Suite-Transmission Control Protocol or Internet Protocol to serve billions of users worldwide. The Internet has become a large market for companies; some of the biggest companies, today, have grown by taking advantage of the efficient nature of low-cost

Author for Correspondence:

[*1]Dr.C.Chandrasekar, Asst. Professor, Department of Computer Applications, Sree Narayana Guru College, Coimbatore, Tamilnadu, India.

[*2]Mr.V.Prabhakaran,M.Phil., Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamilnadu, India. Email- prabhakaranmvp@gmail.com.

advertising and commerce through the Internet, also known as e-commerce. It is the fastest way to spread information to a vast number of people simultaneously. The low cost and nearly instantaneous sharing of ideas, knowledge, and skills has made collaborative work dramatically easier. Not only can a group cheaply communicate and share ideas, but the wide reach of the Internet allows such groups to be easily formed in the first place. Messages can be exchanged even more quickly and conveniently via e-mail. Extensions to these systems may allow files to be exchanged, "whiteboard" drawings to be shared or voice and video contact between team members to be established. The Internet allows computer users to remotely access other computers and information stores easily, wherever they may be across the world. They may do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This is encouraging new ways of working from home, collaboration and information sharing in many industries. Network security Cotroneo et al (2002) consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

Network security starts from authenticating any user with a username and a password. Once authenticated, a stateful 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.Attacks can be based on system software or data. System software based attacks include Automated or user-initiated network-aware attacks (viruses, worms, trojan horses, peer-to-peer) which targets files and data often causing loss of machine control, productivity and time. The malicious system misuse which targets shared resources and protected data. Unmonitored software installation – unknown, untested or unstable programs installed along with intended items that interfere with supporting applications leading to unreliable systems and loss of productivity. Data Integrity, Confidentiality and Availability based attack target. Compromise, theft and / or disclosure of information due to outsider cyber attack or malicious or accidental insider actions. Data loss from any resource with electronic data storage.

II PROBLEM AND ANALYSIS

Denial of Service Attacks

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

Background

DoS attacks are emerging in various forms and becoming more sophisticated. The scope of these attacks spreads over a wide range of Internet protocols to prevent users from gaining access to a spectrum of Internet services. Generally, the various attack types share a common nature in the sense that they rely on the deterministic behavior of most Internet protocols and the lack of authentication over the Internet. To launch a powerful DoS attack, an

attacker has to secure enough resources to achieve the desired damage to the victim. A single attacker could mobilize thousands of compromised computers (also known as zombies or slaves) from unsuspected users. Compromising computers is done in recruitment phase that precedes the actual DoS attack. The systematic way of attack recruitment phase includes gaining remote unauthorized access to a large number of computers. It is also possible to perform attack recruitment via spreading of viruses and Trojan horses. In order to perform a distributed denial-of-service attack, the attacker needs to recruit the multiple agent (slave) machines. This process is usually performed automatically through scanning of remote machines, looking for security holes that would enable subversion. Vulnerable machines are then exploited by using the discovered vulnerability to gain access to the machine, and they are infected with the attack code. The exploits/infection phase is also automated, and the infected machines can be used for further recruitment of new agents . Agent machines perform the attack against the victim. The attackers usually hide the identity of the agent machines during the attack through spoofing of the source address field in packets. The agent machines can thus be reused for future attacks.

The alarming increase in the number of DoS attacks against e-commerce companies and other organizations, the emergence of newly sophisticated attacks, and the growing fear of potential powerful coordinated attacks have led to a significant amount of research in recent years aiming at countering these attacks on all fronts. However, by considering the different ways by which attacks can be conducted, it can be seen that winning the battle against attackers is not easy at all. In fact, the research done so far in this field provides partial solutions to the problem, or in some cases, solutions to specific instances of DoS attacks rather than providing a comprehensive solution. A typical countermeasure would be reactive, effective, generic, locally deployable, and dynamic. Based on their primary objectives, DoS countermeasures are classified into three major categories, namely, prevention, mitigation, and traceback.

III MECHANISM AND SOLUTION

Preventing DoS attacks aims at avoiding the occurrence of these attacks in the first place. Since DoS attack mechanisms vary, attack prevention techniques vary as well. In fact, there are few and not very effective schemes for preventing various types of DoS attack. Most of these schemes are especially useful for preventing attacks that employ source address spoofing. Other schemes, however, apply to attacks that do not necessarily rely on source address spoofing. For example, lightweight authentication is used for preventing QoS-based attacks, while TCP's time-out randomization is used for preventing low-rate TCP attacks. Prevention schemes are usually proactive in nature, generally require global deployment in order to be effective, and they are usually static in nature. Further DoS prevention is classified based on the location of their deployment as (i) Source-based, (ii) network-based, and (iii) victim-based.

Mitigation:

Mitigation of DoS attacks is a reactive countermeasure that is usually initiated by the victim after detecting an attack. The main challenge in DoS mitigation is to accurately identify attack packets and filter them without causing collateral damage to legitimate traffic destined to the victim. There have been two major approaches to perform DoS mitigation, namely, the rate limiting-based and path-based. Rate limiting-based schemes deal with DoS attacks either as a congestion control problem or as a resource management problem. In both cases, the main idea is to characterize attack traffic and limit it. This approach is reactive, does not require wide scale deployment in most cases, generic in the sense that it applies to flooding attacks of any protocol type. However, it is not effective since it does not avoid collateral damage. Statistical-based schemes are based on the fact that attack traffic is more likely to hold a combination of attributes that were rarely seen by the victim. Therefore, incoming packets that hold attributes that do not match the attributes of an up-to-date traffic profile maintained at the victim are filtered directly. This approach is not effective as it introduces high false positive rates. Path-based schemes perform attack traffic filtering based on the identification of the paths traversed by attack packets, the length of the paths followed by attack packets or even by controlling the paths followed by legitimate packets. In another way, a server farm together with a load balancer is used to enhance a web server's capacity. With this increased capacity, the web

server is able to handle more web requests and is less likely to be disabled by a bandwidth attack.

IP Traceback

IP traceback Minho Sung and Jun Xu (2003), is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for Denial Of Service attacks or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP Traceback Stefan Savage et al (2001) is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward Denial of Service attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

Attack Traceback addresses the problem of collecting information about individual packet forwarding agents and collating this data to obtain an approximate Internet router-level graph (attack tree rooted at the victim); whereby tracing the routing path that any packet has taken, provides sufficient basis for attack attribution (attack tree leaves). The Attack traceback is necessary for cleansing zombie attackers, while also being of critical forensic value to law enforcement. The major sources of attacks are due to the increase in the accessing of the network resources by an outside unauthorized user. These users are from different geographical regions and different countries. This makes the traceback process difficult in the real time situation. The information transmitted from one router consists of the source address and the destination address along with the information contained.

Scheme Description

The attacks have to be sensed at once to immediately prevent the network from damage. Resource of any means could be the target of an attcker. The attack originates from the different positioned attacker in order to evade detection mechanisms. The proposed scheme includes the marking of the packets which will strive to preserve the identity of the user. The scheme is implemented at the packet level segregations, with a function to mark the previous and current packet links to the current packet.

A message may be divided into a number of packets, depending on the network protocols. Each packet will hold a considerable part of the message, along with the definitions of the Source and Destined node. The IP header will hold these information of the source and destination node. While the paper proposes to include the linking information of the packets which precedes and succeeds the current packet. By the same, the entire message can be splitted into a number of packets, holding the information of which position it belongs to. The packets may be transmitted into the network in any order, due to network congestions, high traffic etc. Yet the proposed scheme will enable the system to identify the chain of packets.

The attacker may be anonymous or masquerade his/her identity in the place of Source address in the IP header. Inspite, the system proposed demands a linking of message packets which would be not known to the user being external to the network. The packets without the link with other packets may be considered as the attack packets. The security mechanism will surely report the messages with no links established. 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.

A separate Log of information will increment a trust value for each source and destination domains for a considerable time to limit the security mechanisms of legitimate users. After a specific time, the legitimate users would gain an enhanced level of trust by the

system and thus, they will be liberated to further usage.

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.

REFERENCE

[1]. Li Ke Wanlei, Zhou Ping Li, Jing Hai and Jianwen Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics", IEEE - International Conference on Network and System Security, NSS '09, pp. 9-17, 2009.

[2]. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Elec- tron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[3]. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Net-work Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[4]. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[5]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[6]. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[7]. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8]. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9]. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10]. G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[11]. D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[13]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14]. K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[15]. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[16]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[17]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[18]. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[19]. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[20]. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.

[21]. A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.