IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Design of a Novel Technique for Denial of Service Attack Detection in Wireless Network

Sanjeev Kumar[1*], Nishant Agnihotri[2]

[1] Department of Computer Science, Indus International University, Una India
[2] Department of Computer Science, Indus International University, Una India

Corresponding Author: kumar8039@gmail.com, Tel.: +91-88945-52267

Available online at: www.ijcseonline.org

Accepted: 19/May/2018, Published: 31/May/2018

***Abstract*—**There are the numbers of techniques available in the literature for the detection of denial of service attack but the effective and efficient detection of this attack in the wireless domain remains open challenges. Recently the detection of distributed denial of services attacks is the major problem in the wireless domain. In this paper, a novel technique has been designed for the detection of distributed denial of service attack in wireless networks. When sending a large scale of data to different nodes, distributed denial-of-service DDoS attacks intend the victims; consequently there is a need to implement a number of DDOS protection techniques all jointly and integrate on multiple techniques, primarily on the areas required uninterrupted service. The data and its value are unprecedented and hence cannot be ignored. This system is based on a mechanism which ensures that the fallacious information did not get injected in any kind of actual data flowing over the network. This paper has focused toward an approach which is detection of DDoS attack over a network. This mechanism works on trust generation mechanism where trust certificate is issued on the basis of training data asset comparison with the actual behavior of any node working over a network. This trust mechanism results into the detection of malicious contents and finding the intruders resulting into the attack over a network.

Keywords— *DDoS attack, Ids attack, ad-hoc network attack.*

I. INTRODUCTION

This paper focuses on the detection of attacks in Wireless networks (802.11b). As the Wireless LAN (WLAN) has some inherent flaws, it is prone to different attacks. The widespread deployment of WLANs makes detection of attacks on these networks essential. This work uses an agent-based system called Cougar Intrusion Detection System (CIDS) developed at the ISSRL lab for wireless LAN, which was the earlier tool that uses intelligent techniques like fuzzy Decision System to detect different attacks in the network. To test the efficiency of the system, three of the most common attacks that occur on a WLAN are implemented and these are detected using the modified CIDS. Two of these attacks are launched in a real environment and the remaining on is performed using a Network simulator, NS2. Some of these attacks are launched. In an ad-hoc network and the others are tested in an infrastructure network. Accordingly, data are collected pre processed and fuzzy rules are generated for different attack detection. The results indicate that in all the three cases CIDS was able to detect the attacks with good detection rate. The problem of intrusion detection has been studied for several years with early papers on the subject appearing in the late 1970s and early 1980s. While the definition of an intrusion varies slightly from paper to paper, definitions such as the following are widely accepted: "any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. An intrusion detection system then is a system which attempts to detect and in some cases react to intrusions, whether on one system, the group of systems, or computer network.

II. LITERATURE SURVEY

DDoS Attack which is called Distributed Denial of Service attack is an attempt when an online system becomes unavailable and out of use because of multiple and overwhelming request at a time from multiple sources. These types of attacks are an effort to make an online resource unavailable to its deliberate users. [1].

Presently very few approaches are there which completely destroy the DDoS attack from the network is to creating lock or with high security for each and every nodes on the Internet against the misuse that is surely impractical. In present, major huge spots handle the attack in very cynical approaches to it. And this is creating obstacle for the attacker. Therefore, the

prohibition of DDoS is kept open challenges and there is urgency and great demand to create defensive approach for detecting the attacks and the reactive systems by failing excess of the traffic.

DDoS attack is provoked by the victims, source and the networks between them which mean the three major factors of the network system. This makes it an esasy approach to encounter the attack at the destination as to the sources cause the destination bring about a huge bulk of traffic than source [2].

Still there exists requirement tobe applied on various techniques subsequently and cooperatively on the almost all wireless networks in order to keep security for all the nodes in the network and are injected by the attackers. There present various approaches announces by adding digital signatures and the encryption features, but there is always proportionate complexes, more overhead, and more delay in the network, the impediment, and detection mechanism is required to access the quality of services. In this paper Intelligent Agent-Based Defense (IABD) Architecture for DDoS Attacks was specified, which completely assigns an early warning whenever the pre-attack activities are disclose, adopting trust mechanisms[3].

Znaidi et al. [4] have propounded a procedures how to perceive wormhole attack in wireless networks and safe, assured it. This procedures taking into account confined and neighborhood information and without the requirements of the other frameworks such as location information, clock synchronization or dedicated hardware. Moreover, the algorithm is not relying on the wireless communication models. The drawbacks of this procedure are that a wormhole link could be perceived only when the real separation between any two wormhole nodes is greater than four-hop because of the computed coefficients.

Xu et al. [5] emphasized over distributed wormhole detection algorithm (DWDA) can be design on the basis of network disorder detection and commence by the existence of a wormhole. A hop-counting perspective was used as an analysis mechanism for the wormhole attack observation and after that reconstructs local maps in all meeting point, in the algorithm. It can give the imprecise position of a wormhole which is helpful to the testers for scheming further protection perspectives, which is beneficial. Deformity caused by wormholes a "diameter" features is used eventually to observe it.

Win et al. [6] expressed different types of wormhole attack detection techniques had inscribed for wireless networks. They label proposal employ in the DaW security model that can be synthesize a protection and diagnose perspective for wormhole attack with the use of false positive, false negative and accuracy of alarm presentation framework. The production of the label was dignified by the use of ns-2 simulations and initiate that the suggested routing protocol was accomplish much superior in terms to achieve cheap delay.It can found to be more fixed and has to be differentiated with LF research

Hu et al. [7] a daring attack have furnish to secure opposite of a wormhole attack in a wireless network, and plan a new procedure for securing and perceiving wormhole. Packet leashes techniques were suggested to recognize wormhole attacks us these leashes are (i) geographic leashes (ii) temporal leashes. As a result an authentication protocol called TIK plot with the use of temporal leashes.

Ronghui et al. [8] have established a easy and efficient perspective discover and notice wormhole attack. This algorithm also gives an evaluation of the position of the wormhole in wireless networks. Location discovery in wireless networks using hop counting technique on which this label is based upon.

S.Vijayaraniet. et.al.[9] Network IDS system is a device or software application that assemble the data and information from the various nodes in the network and it accumulate the attacked packets for malicious activity which are moving and violating the policy in the network. There would be a sensors based on the parameter and they assemble the data of the prior attack and their sensor monitor would prevent the further traffic of the various nodes on the network.

Mr.Khaire et.al.[10] has discussed about having resolving the ability against key-recovery attacks. While doing so, an adversarial model borrowed from the related field of adversarial learning are adapted to the anomaly detection context.According to two adversarial settings and depending on the feedback given by KIDS to probing queries we have presented key-recovery attacks. We are also providing high level security to it by providing the re-signature technology.

Anju Bala et.al [11] proposed an attempt that has been made to detect and classify the wireless sensor network and to detect widely used security mechanisms to handle those attacks. Challenges of wireless sensor networks are also discussed. This survey will inspire the candidates to come forward with smart and more robust security mechanisms to make researchers in the future and secure their network.

NiyatiShah et.al. [12] There are special skills in both active routing and reactive routing. Better PDR (packet delivery ratio) and correct identity are likely in the active detection method, but periodically suffer from high routing overhead due to transmission packets. The reactive identification

method eliminates the routing overhead problem in an incident-driven manner, but some packets suffer loss at the beginning of the routing process.

Atul Patel et.al. [13] New structure can be growAnd how a global data collection module will help IDS agents to identify incidents of infiltration. First of all, when a system starts requesting a request, it will be checked in the Global Data Collection module if it does not find that it will be placed in the blacklist and a detailed artist of the message has been created, thus all neighbouring nodes can know infiltration. Point, and take appropriate action.

Mohammad SazzadulHoque et.al. [14] Using a number of agents and victims described a method and the approach to detect incompatible network intrusion involves both quantitative and obvious characteristics of the network data to obtain classification rules. Using GP method, it monitors a parameter of traffic in the network

III. PROPOSED DETECTION TECHNIQUES

Mobile agents have been used for creation of the scenario where detection of attack can be considered on the bases of DOS. This detecting technique is capable to detect throughput rate of data and attack on bandwidth.

ALGORITHMS FOCUSSED

All the agents are working in the form of nodes which are responsible for analyzing the flow of data from all the ports of sample network on specific time interval.
Following are the steps involved in the detection technique

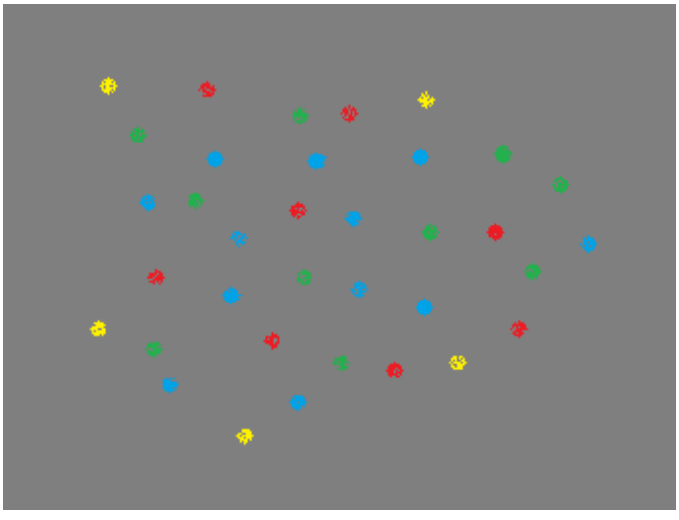

Figure 1: Nodes over network

In Figure 1 Blue node represents the random nodes.
Red Node represents the intruders.
Yellow node represents the administrator nodes.
Green node represents the trusted node.

Traffic and DoS Detection mechanism:

Steps:

1. Collection of the data by the administrator node on specific time interval i.e. D(ADM)-I/O/T
2. Training data set will be attached with the detection system for learning the behaviours of Ports D(TRN)-IOP
3. Data analyzer will keep analyzing the behaviour of the input data with the training data
4. Complete analysis of the variation in the behaviour of the agents (D(TRn)IOP == D(ADM)-I/O/T), -1,0,+1 will be monitored and will be reported to admin agent.
5. Trust mechanism will issue a trust certificate to each node on the basis of the previous reports.
6. Trust certificates C(T)ADM will be analyzed for any variations in the demand of the particular node at each time interval.
7. Variation in load will be analyzed by the analyzer and this will issue an agents trust report on the basis of throughput metrics i.e. TM(D(ADM)/O/T, D(ADM)-I/T) on the variation of bandwidth.
8. Variation in report will results in the information about attack.

Algorithm DET(IO)
1. For all ports collect data D(ADM)-I/O/T. 2. Compare V1,V2 i.e. (D(ADM)-I/O/T),(D(TRn)-IOT) 3. If v1==v2 call DET(IO) 4. Else call Trust(IO) 5. End

Algorithm: To start detection system

Algorithm Trust(IO)
1. For i=1 to i=10

2. If var(V1,V2)>=5
   Issue (TM(low), call Band(Var)
3. If Ver((V1,V2)<=5
   Issue TM(Hig), call DET(IO)
4. Else call Trust (IO)
5. End

Algorithm: To ensure trust mechanism

Algorithm Band (Var)

1. For all TM(low), i=1to 50
bandwidth = Bandwidth +20
2.Comp(V1, V2), TM(Low)
3.If Comp(V1,V2),1
Issue Low trust Certificate.
4.If If Comp(V1,V2),0
Issue Clean agent
5.Else issue dead agent.
6.Repeat 1 to 5
7.exit

Algorithm: To detect the intruder and identifying the attack

IV. RESULTS

The output of the detection technique is based upon the network simulator 2. This technique has been used with the Denial of service attack using the detection mechanism which is unauthorized flow of data on a particular network.

For evaluating the performance of the proposed technique following metrics have been used:

- Bandwidth Metric — this particular metric is solely responsible for inspection of the interruption in the bandwidth of the network caused by any unauthorized interception.

- Throughput Metric — throughput metric is used to monitor the real results of accurate data received on the other end whereas it has no connection with the jitter.

The performance of the proposed system has been analyzed on the basis of variation in the bandwidth from 550kbps to 850kbps, Figure [2] shows the comparison on varying parameters.

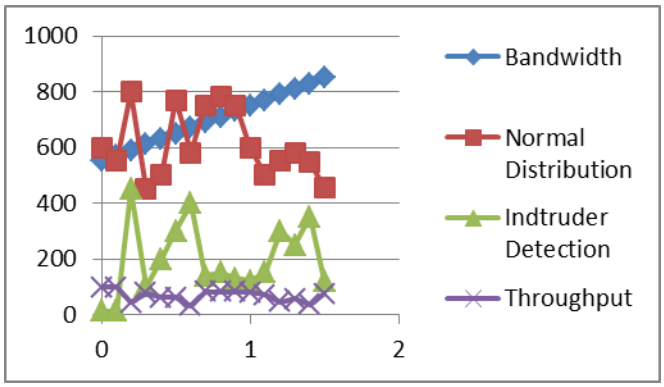

Figure 2: Comparison Graph of Bandwidth vs Frequency vs Intruder Detection

V. CONCLUSION

A detection technique has been designed based on the mobile agents for detecting Distributed Denial of Service (DDoS) Attacks in wireless LAN. The various performance parameters such as throughput, packet delivery, the false positive rate were taken for measuring the performance of the proposed technique. The proposed technique was compared with the normal attacks scenario and seen that proposed technique is an effective measure for the detection of intruders in wireless networks. The main advantage of the proposed technique is that it provides an early each agent executes a. If an agent finds that the received report from any other agent does not match with the expected results, it can be considered as a compromised agent node.

Detection algorithm and based on the detection results, it exchanges its report with other agents. Based on the collaborative report, a final alert is sent to the base station. Further, a trust mechanism in which each agent checks the trust of other agents, to identify the compromised agent nodes has been designed warning when pre-attack activities are detected. The agents proposed in the architecture are autonomous, mobile and cooperative entities.

REFERENCES

[1]. Kaufman Charlie, Perlman Radia, Speciner Mike. Network Security: Private Communication in a Public World, 2nd ed., USA, Prentice Hall PTR, 2002.

[2]. J. Levington M. Unlocking the secret of wireless security. In Oen, p. 23 United Kingdom, Wilmington Business Publishing, Sept. 2002.

[3]. Fluher, S. Mantin, I. Shamir,A. Weaknesses in the key scheduling algorithm of RC4 [online], referred 12.4.2003,URL://citeceer.nj.nec.com/fluhrer01.html.

[4]. W. Znaidi, M. Minier, and J.P. Babau, "Detecting wormhole attacks in wireless networks using local neighbourhood information." In Proceedings of IEEE 19th

International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 2008

[5]. Y. Xu, G. Chen, J. Ford and F. Makedon, "Distributed wormhole attack detection in wireless sensor networks." In Proceedings of the First Annual IFIP Working Group International Conference on Critical Infrastructure Protection, 2007.

[6]. K.S. Win, "Analysis of detecting wormhole attack in wireless networks", In World Academy °f Science, Engineering and Technology, pp. 422-428, 2008.

[7]. Y. C. Hu, Y. Chun, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks." In IEEE Twenty-Second Annual Joint Conference of the Computer and Communications, Vol. 3, pp. 1976-1986, 2003.

[8]. H. Ronghui, M. Guoqing, W. Chunlei and F. Lan, "Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes", World Academy of Science, Engineering and Technology, Vol. 3 pp. 31-44, 2009.

[9]. S.Vijayarani1 Ms. Maria sylviaa intrusion detection system – a study (IJSPTM) vol 4, no 1, february 2015

[10]. Mr.Khaire S. H.1 Prof.Hemant Gupta2 Prof.Mayank Bhatt3 *IJSRD Vol. 5, Issue 12, 2018 | ISSN (online): 2321-0613*

[11]. Anju Bala security attacks and challenges of wireless sensor network | volume 3 | issue 1 | issn : 2456- 3307| © 2018 ijsrcseit

[12]. *Niyati Shah, SharadaValiveti*Intrusion Detection Systems for the Availability Attacks in Ad-Hoc Networks ISSN 2277-1956/V1N3-1850-1857 *www.ijecse.org*

[13]. Atul Patel, RuchiKansara, Dr. PareshVirparia A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network *(IJACSA) pp 68*

[14]. Mohammad Sazzadul Hoque1, Md. Abdul Mukit2 and Md. Abu Naser Bikas3 AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM (IJNSA), Vol.4, No.2, March 2012

[15]. K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET", Wireless personal communications, Vol. 73, Issue 1, pp. 95-126, 2013. http://www.indjst.org

Authors Profile

Sanjeev Kumar is a M.Tech. Student of Department of CSE at Indus International University. His field of interest is Network Security and Scalability of Cloud.

Nishant Agnihotri is an Assistant Professor in the department of CSE of Indus International University. His area of specialization is Computer Networks and Big Data analytics. He is pursuing his doctorate in the field of Big data analytics and security.