WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Intelligent Approach To Detect Probe Attack

Avanthika Sai K[1], Soumya K[2]*

Student, JAIN (Deemed-to be University)
Professor, JAIN (Deemed-to be University)

ABSTRACT :

This paper presents an intelligent approach for detecting probe attacks in Wireless Access Networks (WANs), with a focus on identifying external threats. Conventional methods for detecting Distributed Denial-of-Service (DDoS) attacks and MAC spoofing in WANs face limitations, underscoring the need for advanced detection strategies. The proposed method leverages a trained feedforward neural network to analyze key parameters such as frame subtype, data rate, delta-time, and sequence number, enabling the differentiation between authentic and malicious frames. Real-world WLAN traffic is utilized, prioritizing the swift identification of intrusions within the communication process. The study underscores the effectiveness of Artificial Neural Networks (ANNs) in managing the complexity and unpredictability inherent in WLAN traffic, while simultaneously reducing monitoring overhead and delivering precise detection outcomes. Furthermore, by investing in understanding emerging technologies, exploring neural network applications, enhancing cybersecurity skills, contributing to research and development, advocating for secure network practices, and promoting ethical AI use, individuals can actively contribute to advancing network security and mitigating cyber threats in modern networks.Keywords: Wireless Access Networks, probe attacks, Distributed Denial-of-Service (DDoS), MAC spoofing, feedforward neural network, cybersecurity, emerging technologies, research and development, secure network practices, ethical AI use.

Introduction :

Voice over the Internet Protocol (VoIP) Voice over Internet Protocol (VoIP) is a group of methods for transmitting audio over the internet. Data packets are used to transport voice as digital signals. The Protocol for Session Initiation SIP is a VoIP and multimedia IETF standard. SIP is an application protocol for establishing, updating, and terminating VoIP connections. SIP's flexibility and simplicity make it an easy protocol to extend. distributed denial-of-service attacks There are a lot of requests coming from a lot of different hosts in a DDoS attack. Because of this, genuine customers will be unable to access their desired services. Availability, rather than data consistency, is a fundamental problem in VoIP and practically other network domains. Authentic MAC addresses may be used to circumvent AP access lists. Because of this, attackers can launch a Denial-of-Service (DoS) assault on legitimate stations. An intelligent strategy to detect WLAN probe request assaults is discussed in the analysis (Gerhards-Padilla, et al., 2010).

Open Research Question :

Request and answer messages for beacon, probe, and other WLAN communications are not encrypted, allowing sniffers to see the contents. Since network membership is not required at this stage, anybody with a valid Media Access Control (MAC) address may request a probe. An attacker either actively or passively examines the network before an attack to get access to essential network data. This is only the beginning of MAC address spoofing. Their Wireless Intrusion Prevention System (WIDS) tackled these early stages of an attack before moving on to more sophisticated techniques. Analysis of current research and the development of IEEE 802.11 select committees is required to construct an effective WIDS that can detect MAC spoofing and probe request attacks on IEEE 802.11 networks. This research uses a wireless home network to keep tabs on traffic in real-time. Real-world WLAN traffic is used in this research instead of data from a database or traffic generated by a testbed. Our goal is to find an intrusion as soon as feasible in the communications process. Initial tests revealed that WLAN traffic patterns are typically unpredictable and reliant on the user's usage, system software, and applications. Other reasons for missed frames include congestion, packet jitter or lost packets, and network traffic prioritization services such as Service Quality Prioritization (SQP) (QoS). Data complexity and unpredictability made Artificial Neural Networks (ANNs) ideal for this job (ANN). Due to WLAN traffic and the parallel processing feature of ANNs, the monitoring STA's performance is onegatively impacted by these factors. Only four characteristics are used to identify an assault in this study. This dramatically decreases the monitoring vehicle's overhead while still delivering the anticipated findings. This study offers an intelligent method for detecting WLAN probe request assaults. A controlled feedforward neural network of four input neurons, two hidden layers, and an outputs neuron is used to analyze WLAN data gathered on a home wireless connection (Jeyanthi, 2014).

Related Work :

Intrusion detection is used when an unauthorized person attempts to get access or has already accessed or breached the network. It is no secret that many scientists have been working on this problem to find a solution. Bicakci et al. (2009) provide a comprehensive assessment of popular non-intelligent ways for detecting and avoiding DOS assaults, while Bansal et al. (2008) assess several widely used non-cryptographic techniques of MAC spoof identification in WLANs. To identify and prevent PRF attacks, they point to the use of encryption, sequence number analysis, reducing retry limits, including Network Adapter Card (NIC) profiling, which includes the use of Signal Strength Indicators (SSI) with Radio Frequency (RF) fingertip printing (Arivudainambi, et al., 2018).

The most dependable solution may be based on cryptography. In order to increase management frame security, Bansal et al. (2008) suggest using a shared key. In order to implement this approach, the wireless card must be updated. Hardware upgrades are impractical since so many wireless cards will need to be replaced. Nevertheless, it is a costly endeavor that might need protocol maintenance and perhaps serve as a denial-of- service attack vector in and of itself.

False frames may be used to identify other attacks, such as those using probe requests. MAC spoofing may be detected using the structure and behaviour of the sequence number field, according to Malekzadeh et al. (2007a). Madory D (2006) uses a temporal lag between frames and a sliding window of received signal intensities as part of the detection algorithm to identify spoofs. Use a window of sequence numbers and statistics on traffic arrivals to detect spoofing and unusual traffic in wireless networks (FRR - Forge Resistance Relationship Method). It may be hard to tell the difference between an attacker and a victim if both parties are broadcasting simultaneously.

As a result of adopting this method, the network is forced to do more work than it would otherwise. To identify identity-based attacks against wireless communication, Bansal et al. (2008) recommend that signal printouts be used instead of other methods. A single AP for all STAs defeats the purpose of having several APs. RSSI metrics alone are unable of distinguishing between a genuine STA and an adversary." "WIDS employs a wide range of statistical and rule-based methods, many of which are time-consuming, do not keep up with changes in the climate, and eventually become out-of-date when they are implemented.

Academics have recognized three sorts of frames: management, control, and data. It is the responsibility of management structures to ensure that all employees have access to efficient communication. Control frames provide for more efficient transmission of data. In the Open System Interconnect, network layer packets are contained in data frames, which are encased in data frames. Each frame's MAC structure comprises the Mac header, the frame content, and also the Frame Check Sequence, among some other things (FCS). All of the data frame's control and location information is included in the MAC header. Quality of service control messages is also included. Frame-specific data is stored in the frame's body, such as information on the frame's type and subtype. Security methods in FCS include a CRC (Cyclic Redundancy Check).

It is easy to manually or subjected to statistical the frames in a WLAN test bed to discover probing attacks and other irregularities, thanks to its highly regulated topology. The ability to record and analyse frames in a chaotic, real-time environment is critical for a successful WIDS. According to the researchers, they used an unsupervised feed-forward neural network (NN) design with four input neurons and 20 hidden cells in each of the two hidden layers, in addition to an additional single linear output neuron in each of the two hidden layers, to distinguish legitimate and rogue frames from each other (Nazih, et al., 2020).

Access points (APs) maintain a list of authorized MAC addresses in order to prevent unauthorized access. Ifconfig, and SMAC2 (Windows) may indeed be used to disguise MAC addresses to make the STA seem to be authentic. To ask a question and get an answer, you do not have to be a part of a network. As a consequence, all an attacker needs to launch a Probe Request is a legitimate MAC address. Probing is often the first step in any assault on a computer network before going on to the next level (Guo, & Perreau, 2010).

According to the report, many of these solutions are based on non-existent data sets and identifying invasive behaviour depending on examining known vulnerabilities. Aside from the complexity of these solutions, it has been noticed that some of them have been simulated & tested without taking into account the actual implementation and computer resources they may demand. Therefore, these methods do not apply to academic research since they are either too complicated or costly to apply (Ayyamuthukumar, & Karthik, 2015).

Research Approach :

When considering how much data and computational power is required for practical implementation, the research considered building a WIDS with a few variables. It was determined that four independent variables: MAC frame ID, frame subtype, signal characteristics and delta time values, were the best fit for the study. There is nothing you can do about these variables. If this is the case, some believe attackers employ sequence number software to create patterns matching the user's STA so that they may get access. Because they cannot predict the STA's behavior, the accuracy and usefulness of this technique are in doubt. There's no way to know whether the STA's NIC card will boot up, be reset, transfer data, or sit idle until it does one of those things. An attacker may modify the signal intensity, move closer to the user's STA or just cause a signal fluctuation as a result of environmental conditions, which may be exploited. Thus, it is more of a theoretical problem rather than a practical one. It's possible, according to some, that probe request frames are generated by a misconfigured STA or by a real user who makes repeated efforts to log in to the AP. STAs and users may be fixed by network administrators in this situation. This method works even if the real user is offline. STA and probe request spoofing are both possibilities that might be indicated by any one of these variables. The other three variables may be required to support this if doubt exists (L. S. 2021).

5. Advancing Network Security Through Personal Investment and Advocacy

The utilization of a Wireless Access Network's frequency selective band for identifying outside attackers represents a significant advancement in network security. As an individual invested in technology and cybersecurity, this innovative approach piques my interest and prompts considerations for personal investment in several areas:

1. **Understanding Emerging Technologies:** Investing time and effort into understanding the intricacies of technologies such as Wireless Access Networks and neural networks is crucial. By staying informed about the latest advancements in the field, I can better comprehend the potential applications and implications of such technologies for network security.
2. **Exploring Neural Network Applications:** The use of a trained feedforward neural network for detecting probe request assaults highlights the increasing role of artificial intelligence in cybersecurity. Exploring the workings of neural networks and their applications in threat detection can provide valuable insights into enhancing network security measures.
3. **Enhancing Cybersecurity Skills:** As the threat landscape evolves, investing in continuous learning and skill development in cybersecurity is essential. This includes gaining proficiency in analyzing network traffic, understanding attack vectors, and implementing robust security measures to safeguard networks against potential threats.
4. **Contributing to Research and Development:** Supporting research efforts aimed at improving network security methodologies, such as monitoring total bandwidth and implementing coordinated monitoring techniques, can have a positive impact on enhancing the effectiveness of security measures. Contributing to research initiatives or collaborating with experts in the field can foster innovation and drive progress in cybersecurity.
5. **Promoting Secure Network Practices:** Investing in initiatives aimed at promoting awareness and adoption of secure network practices among individuals and organizations can help mitigate cybersecurity risks. Educating users about the importance of implementing strong passwords, updating software regularly, and adhering to security best practices can contribute to building a more resilient cybersecurity posture.
6. **Advocating for Ethical AI Use:** Given the reliance on artificial intelligence, particularly neural networks, in cybersecurity applications, advocating for the ethical use of AI technologies is paramount. Investing efforts in promoting responsible AI development and usage can help mitigate potential risks associated with AI-driven security solutions.

In summary, personal investment in understanding emerging technologies, exploring neural network applications, enhancing cybersecurity skills, contributing to research and development, promoting secure network practices, and advocating for ethical AI use can play a crucial role in advancing network security and safeguarding against cyber threats in an increasingly connected world.

Conclusion :

The development of an intelligent approach to detect probe attacks in Wireless Access Networks (WANs) represents a significant advancement in network security. Traditional methods for detecting Distributed Denial-of-Service (DDoS) attacks and MAC spoofing have limitations, emphasizing the need for more sophisticated detection strategies. The proposed method employs a trained feedforward neural network, which effectively analyzes various parameters to distinguish between authentic and malicious frames in real-world WLAN traffic.

By investing in understanding emerging technologies, exploring neural network applications, enhancing cybersecurity skills, contributing to research and development, promoting secure network practices, and advocating for ethical AI use, individuals can actively contribute to advancing network security. These investments and advocacy efforts are crucial in mitigating cyber threats and ensuring the resilience of modern networks.

In conclusion, the combination of innovative detection methods and proactive engagement in cybersecurity practices can significantly enhance network security and protect against evolving cyber threats in an increasingly interconnected world.

REFERENCES :

1. Gerhards-Padilla, E., Aschenbruck, N. and Martini, P., 2010. TOGBAD-an an approach to detect routing attacks in tactical environments. Security and Communication Networks, 4(8), pp.793-806.
2. Jeyanthi, N., Thandeeswaran, R. and Vinithra, J., 2014. Rqa based approach to detect and prevent DDoS attacks in VoIP networks. Cybernetics and Information Technologies, 14(1), pp.11-24.
3. Arivudainambi, D., K.A, V. K., & Sibi Chakkaravarthy, S. (2018). LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks. *Neural Computing and Applications*, *31*(5), 1491–1501. https://doi.org/10.1007/s00521-018-3383-7
4. Ayyamuthukumar, D., & Karthik, S. (2015). Correlation Based Approach with a Sliding Window Model to Detect and Mitigate Ddos Attacks. *Journal of Computer Science*, *11*(2), 438–442. https:// doi.org/10.3844/jcssp.2015.438.442
5. Et. Al., L. S. (2021). A Secure Methodology to Detect and Prevent Ddos and Sql Injection Attacks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 341–346. https:// doi.org/10.17762/turcomat.v12i2.722
6. Guo, Y., & Perreau, S. (2010a). Detect DDoS flooding attacks in mobile ad hoc networks.
7. *International Journal of Security and Networks*, *5*(4), 259. https://doi.org/10.1504/ijsn.2010.037666
8. Guo, Y., & Perreau, S. (2010b). Detect DDoS flooding attacks in mobile ad hoc networks.
9. *International Journal of Security and Networks*, *5*(4), 259. https://doi.org/10.1504/ijsn.2010.037666
10. A Hybrid Modified Grasshopper Optimization Algorithm and Genetic Algorithm to Detect and Prevent DDoS Attacks. (2021). *International Journal of Engineering*, *34*(4). https://doi.org/10.5829/ ije.2021.34.04a.07
11. Nazih, W., Elkilani, W. S., Dhahri, H., & Abdelkader, T. (2020). Survey of Countering DoS/DDoS Attacks on SIP Based VoIP Networks. *Electronics*, *9*(11), 1827. https://doi.org/10.3390/ electronics9111827

12. Nazih, W., Hifny, Y., Elkilani, W. S., Dhahri, H., & Abdelkader, T. (2020). Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks. *Sensors*, *20*(20), 5875. https://doi.org/ 10.3390/s20205875