DETECTION OF DOS ATTACKS TOWARDS WI-FI

Dona Antony
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala
donaantony20019@gmail.com

C S Pooja
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala
poojaparvathy09@gmail.co m

Akshara S Kumar
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala
aksharaskumar4 @gmai l.com

Prof. Manesh T
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala
manesht.cs@adishankara.ac.in

Prof. Rosemary Deljo
Adi Shankara Institute of Engineering and Technology,Kalady,Kerala
rosemaryv.cs@adishankara.ac.in

ABSTRACT

WLANs are widely employable in several networking applications because of their mobility, flexibility and availability. With the advent of Internet of Things(IoT) , wi-fi enabled devices have become ubiquitous everywhere especially to set up smart environments such as smart homes ,smart cities , agriculture ,smart healthcare ,etc. Unfortunately, WLANS are susceptible to a wide array of wireless security attacks – say Man In The Middle attacks where an attacker inserts a rogue access point into a vulnerable network. With the WPA3 device gaining popularity ,this opens another way for the attackers to cause potential harm. In a resource-constrained environment , we need an adequate, effective and lightweight mechanism to ensure defence against such deauthentication and disassociation attacks.

KEYWORDS

Wi-fi, DoS attacks, intrusion detection

INTRODUCTION

The Wi-Fi alliance enforced the use of 802.11 standard or Protected Management Frames (PMF) that are capable of offering protection against spoofed deauthentication or disassociation based MitM or DoS attacks. PMF being vendor -specific and thus optional, many existing IoT devices (in smart environments) do not comply with the PMF standard. Though WFA has made it mandatory to use PMF in WPA3 protocols or devices, inside attackers can still do the deauthentication or disassociation attacks. This is the cause that we intend to address.The relevance of this issue comes from the fact that new WPA3 devices are gaining wide popularity these days.

Most of the existing mechanisms practise cryptographic authentication of communication channels, beacons or devices to detect any such intrusion. However, such mechanisms are ineffective unless all devices connected in a LAN support them. Another complication is that implementation of these mechanisms are based on the use of modified standards and this would require several firmware modifications and complex software integration to existing devices. In context of a heterogeneous environment, these methods won’t suffice. And the fact that management and maintenance of existing defence mechanisms takes substantial technical knowledge it yet another concern.We believe that the lightweight, signature based solution we propose for the same will address this issue efficiently.

TECHNOLOGIES USED

We capture wi-fi frames in both a normal scenario and attack scenario. And then , compare the parameters in both the cases and thus analyse how the parameters vary . We perform a signature – based intrusion detection .We rely on the following indicators : (i) Number of deauthentication or disassociation frames (threshold) (ii) time span or duration (iii) number of duplicates (same source MAC to same destination MAC) (iv) Reason code for deauthentication (v) Data frames after deauthentication (vi) timespan or duration of frames

SCAPY

This is a Python library used for packet management.It enables the creation,forging and decoding of network packets and also for injecting packets into the network.

RASPBERRY PI

Raspberry Pi can be plugged into the laptop and an SSH session can be used to access this.
It makes the system more user friendly so that even people with absolutely no technical knowledge can use it without hassle.

D LINK ROUTER

It is used for connecting multiple devices to a network and also to maintain network traffic
.This router is very apt for home networks and makes downloading ,uploading of files etc. smoother.

KALI LINUX

An expertly crafted operating system created specifically for network analysts and penetration testers is called Kali Linux. The fact that Kali Linux comes pre- installed with a range of tools makes it a veritable Swiss Army knife for ethical hackers. Formerly known as Backtrack, Kali Linux now positions itself as an expert successor with cutting-edge testing tools. As opposed to BackTrack, which included a large collection of pointless programmes and multiple tools that all served the same purpose. As a result, Kali Linux makes ethical hacking much simpler.

WI-FI ADAPTERS

A USB wireless adapter connects to our computer's USB port and enables Wi-Fi communication with other devices. This enables us to connect to wireless networks and communicate with other Wi-Fi-enabled computers. The top Wi-Fi adapters for Kali Linux are as follows: Panda PAU06, Alfa-AWUS036NH, Alfa-AWUS036NEH, and Alfa-AWUS036NHA-Wireless B/G/N USB Adapters.

CLASSIFICATION OF DEFENSE MECHANISMS

The defense mechanisms can basically be classified depending on the stage at which the defense mechanism comes into play.The stages are :

Defence mechanisms at Stage 1:

Defense mechanisms in this stage defend against attackers before they acquire a Man in the Middle position between the client and a legitimate access point. This is done by recognizing the notorious devices ,channels etc.

Defence mechanisms at Stage 2:

These are employed after the attacker manages to acquire an intermediate position between the client and access point without being recognized as malicious. Several attacks such as key reinstallation attacks, FragAttacks,Dos attacks etc are some such MC-MitM enabled attacks.

However , our focus is on defending a smart environment against DoS attacks.

PROBLEM STATEMENT

A recent study on Wi-Fi security threats reveals that 87% of examined routers do not adhere to PMF requirements. e. Our investigation also showed that because most existing mechanisms need the installation of extra security modules, establishing their new solutions on residential routers, or configuring every Wi-Fi client, they are not flexible enough to be implemented in IoT contexts. We draw attention to the fact that a smart environment contains a number of IoT devices, and the defense mechanism cannot be based on the assumption that each of these devices will need to be updated, changed, or replaced with a new model. Due to complicated setups, setting up certain networks, installing firmware, etc., using existing protection systems places is rather complicated for common man.

RESEARCH CHALLENGE

In context of a smart environment such as a smart home, there may be several IoT devices that rely on different wi-fi protocols. Say, WPA for legacy devices,WPA2 for majority of the devices that are in use today,WPA3 for emerging as well as recently bought devices. Also, some of the IoT device manufacturing companies may not provide for patches in order to resolve vulnerabilities such as key reinstallation attacks. Besides, many IoT devices are not compliant with Protected Management frames (PMF) , a practical solution against several Man in the Middle attacks or DoS attacks .

TECHNICAL FEASIBILITY ANALYSIS

We analyze the technical feasibility of the existing mechanisms in terms of the following metrics:

1. Wi-Fi standard: This indicates whether the existing devices will need any changes in any of the wi-fi standards they rely on.
2. Compatibility : This indicates whether new capabilities will have to be installed on the existing devices in order to apply the proposed mechanism on them.
3. PMF/firmware requirements: Whether the existing devices would

need to undergo any firmware updates or whether they should essentially have PMF implemented on them in in order to implement the proposed mechanism on them.

4. Third-party software /hardware integration: This indicates if any third-party software is required for the suggested defense mechanism to be implemented. Also , whether additional hardware or storage is necessary.
5. Computational complexity : The computational complexity (high or medium or low) depending on the computational overhead such as memory requirements, processing speed etc.
6. Technical overhead: The amount of technical knowledge a user of the proposed mechanism would require (High or medium or low)High if he would have to install a software or integrate a hardware ,medium if he would have to configure any settings, low if he just needs to run the mechanism.

RELATED WORKS

Intrusion detection in wireless networks has made very little progress at the lower OSI layers (layer 2 and below).

[1] WIDS: An Anomaly Based Intrusion Detection System suggests analysing anomaly behaviour to detect Wi-Fi attacks with fewer false alarms, but as the size of an n-gram increases, the probability of an n- gram not being observed during the training phase also increases, leading to reduced IDS's accuracy during the testing phase.

[2] The paper suggests SLGBM, an intrusion detection approach for wireless sensor networks. Due to the limitations of sensor nodes' resources, significant redundancy, and strong correlation of network data, existing intrusion detection algorithms for Wireless Sensor Networks (WSN) suffer from problems like low detection rates, large calculations, and high false alarm rates. To reduce the computational cost, the sequence backward selection (SBS) approach is used to first lower the data dimension on the feature space of the original traffic data. However, the performance of the backward selection approach is subpar when considering a tiny fraction of the dataset, and the Light GBM algorithm likewise overfits small data.

[3] The goal of this study, A Lightweight Intrusion Detection System for the Internet of Things, is to provide a lightweight attack detection technique utilising SVM to find an adversary attempting to inject extra data into the IoT network. However, SVM frequently exhibits poor performance when the target classes overlap. For instance, the SVM won't perform well if there are more training data samples than features for each data point.

[4] This paper proposes the use of big data techniques known as Apache Spark for feature selection and clustering along with the incorporation of both behavioural and content-based features simultaneously to improve prediction accuracy. This paper applies big data based deep learning systems to intrusion detection. but Big Data privacy and protection is a significant concern for security management system makers.

[5] An anomaly-based intrusion detection system for the Wi-Fi (IEEE 802.11) Protocol is known as WIDS. This study suggests analysing anomalous behaviour in order to identify Wi-Fi assaults with fewer false alarms. The proposed WIDS models use data structures like n-grams and observation flows to track the Wi-Fi

protocol's typical behaviour. but The probability of an n-gram not being seen during the training phase likewise rises as an n-size gram does, which lowers IDS's accuracy during the testing phase. IDS find it exceedingly challenging to identify minimal deauthentication attacks since they have such a little footprint.

[6] This research suggests an intrusion detection system based on CNN that uses a novel mapping technique to convert tabular data into grid-based data. Here, we use a matrix of attribute sequences to exploit the tabular data of wireless attacks and map it into visuals. However, using multi-class datasets causes binary issues, and the execution time issue is a significant disadvantage of CNN.

[7] This study suggests a straightforward technique to identify Denial of Service called Change-point monitoring (CPN) (DoS attacks). The Sequence Change Point detection is used in CPN. For DoS detection, CPM makes use of the underlying protocol behaviours. The advantages of CPN are that it is 1) stateless, has no computational cost, and is hence resistant to flooding attacks, 2) robust detection is achieved by using the nonparametric CUSUM approach, and 3) it is indifferent to locations and traffic patterns. However, CPM is ineffective if the same session's packets pass through multiple leaf routers, and the erratic nature of Internet traffic makes it more difficult to identify attacks.

[8] For 802.11 networks, this research presents a machine learning-based jamming detection method that uses widely available hardware. The method was put through an experimental evaluation,

which demonstrated its exceptional accuracy for both true positives and negatives in indoor and mobile outdoor scenarios, under various propagation conditions (good- and bad-links, with and without concurrent traffic from neighbouring networks), and for constant and reactive jammer types. However, malicious radio waves are used to undertake OSI layer 1 jamming attacks. Jamming attacks can seriously harm the performance of wireless networks.In this research, identity-based threats are detected using signal prints based on the RSSI method. To determine the sender, we use the Received Signal Strength Indicator (RSSI). However, the work did not offer any support against actual assaults. We may create a signal print for the sender by combining the RSSI data collected at several nodes. When applying signalprints to WSNs, one must take into account battery discharge and the absence of a centralised authority. This study describes a method for addressing these issues. It is also clear from the fluctuation in RSSI with distance that this method is best suited for dense networks.Due to its vulnerability to obstruction and interference from objects and environmental factors, RSSI method has a low level of stability.

[9] In this study, the letter-envelope protocol is used to provide a defence against farewell attacks in 802.11 networks and a mechanism to authenticate management frames and thwart deauthentication attempts. The protocol can be readily implemented in both existing systems and upcoming 802.11 devices because it is used as an extension to current

802.11 specifications. The changed device drivers, however, are limited to a specific chipset, and no open-source alternative was offered. The present device driver that we changed only functions on Linux-based wireless devices with an Atheros chipset

CONCLUSION

A signature based wireless intrusion detection system that we describe in this paper can be implemented against deauthentication and disassociation attacks in a world that is increasingly becoming WPA3-centric in every smart environment. The lightweight signature based intrusion system can be easily integrated into any Wi-Fi-based IoT environments without any modification of network settings or existing devices, and provide continuous security against deauthentication and disassociation attacks.

FUTURE WORKS

The scope of the proposed system can get much wider in a world that is becoming increasingly wireless mainly due to flexibility reasons. Whole companies might rely on the

FUTURE WORKS

The scope of the proposed system can get much wider in a world that is becoming increasingly wireless mainly due to flexibility reasons. Whole companies might rely on the technique we suggest. It can

with further modifications , find use in critical governmental applications as well.

REFERENCES

[1] P. Satam and S. Hariri, "WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol," in IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 1077-1091, March 2021, doi: 10.1109/TNSM.2020.3036138.

[2] S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020, doi: 10.1109/ACCESS.2020.3024219

[3] S. U. Jan, S. Ahmed, V. Shakhov and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," in IEEE Access, vol. 7, pp. 42450-42471, 2019, doi: 10.1109/ACCESS.2019.2907965.

[4] W. Zhong, N. Yu and C. Ai, "Applying big data based deep learning systems to intrusion detection," in Big Data Mining and Analytics, vol. 3, no. 3, pp. 181-195, Sept. 2020, doi: 10.26599/BDMA.2020.9020003.

[5] S. Gao, Z. Peng, B. Xiao, A. Hu, Y. Song and K. Ren, "Detection and Mitigation of DoS Attacks in Software Defined Networks," in IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1419-1433, June 2020, doi: 10.1109/TNET.2020.2983976.

[6] M. E. Aminanto, R. S. H. Wicaksono, A. E. Aminanto, H. C. Tanuwidjaja, L. Yola and K. Kim, "Multi-Class Intrusion

Detection Using Two-Channel Color Mapping in IEEE 802.11 Wireless Network," in IEEE Access, vol. 10, pp. 36791-36801, 2022, doi: 10.1109/ACCESS.2022.3164104.

[7] Haining Wang, Danlu Zhang and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208,Oct.-Dec. 2004, doi: 10.1109/TDSC.2004.34.

[8] O. Puñal, I. Aktaş, C. -J. Schnelke, G. Abidin, K. Wehrle and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, 2014, pp. 1-10, doi: 10.1109/WoWMoM.2014.6918964.

[9] S. Misra, A. Ghosh, A. P. S. P. and M. S. Obaidat, "Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints," 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, 2010, pp. 35-41, doi: 10.1109/GreenCom-CPSCom.2010.61.

[10] T. D. Nguyen, D. H. M. Nguyen, B. N. Tran, H. Vu and N. Mittal, "A Lightweight Solution for Defending Against deauthentication/Disassociation Attacks on 802.11 Networks," 2008 Proceedings of 17th International Conference on Computer Communications and Networks, 2008, pp. 1-6, doi: 10.1109/ICCCN.2008.ECP.51.