# Wireless Instrusion Detection Systems

Sampreety Pillai(2101CS71), M Shanmukha Priya(2101CS40)

April 21, 2025

Word count: 4416

## 1 Introduction

Wi-Fi networks based on the IEEE 802.11 standard are naturally exposed to Denial-of-Service (DoS) attacks, especially at the MAC layer. This is because wireless signals are broadcast to everyone nearby, and the protocol has some known flaws—like the hidden node issue and the fact that many management messages aren't protected or verified.

The system uses the Distributed Coordination Function (DCF) to avoid data collisions. It includes methods like RTS/CTS handshakes and random backoff times. But attackers can misuse these to take over the network and block others from using it. They can also pretend to be someone else by faking MAC addresses. This lets them carry out attacks like sending fake disconnect messages (deauthentication/disassociation) or messing with devices in power-saving mode.

Other attacks flood the network with too many requests: like probe requests or authentication attempts—causing the access point (AP) to slow down or crash. Attackers might also send fake control messages to stop real users from getting access to the network.

Traditional intrusion detection systems (IDS) aren't always great at spotting these problems. They often give false alarms or can't detect attacks quickly enough. To help with this, newer and smarter methods have been developed.

### 1.1 Intrusion Detection Systems

Intrusion Detection Systems (IDS) are designed to identify malicious activities or policy violations within a computer network or system. They can be categorized into four main types: (1)

- Signature-based intrusion detection systems (IDS) work by using a database of known attack patterns, called "signatures." They constantly watch the network traffic and check if anything

matches one of these patterns. For example, a Wi-Fi-focused IDS would keep a list of known Wi-Fi attack types and look for those in the traffic going through the network. These systems are fairly easy to set up and work well against attacks that are already known.
However, they have a big downside—they can't detect new or slightly changed attacks unless the database is regularly updated with the latest threats. That means they can miss brand-new (zero-day) attacks or clever variations of old ones.

- Anomaly-based intrusion detection systems (IDS) work by first learning what "normal" behavior looks like on a network. Once they have this baseline, they watch for anything unusual and flag it as a possible threat. For Wi-Fi networks, this means understanding how traffic usually flows and how devices typically behave.
  Since many Wi-Fi attacks involve doing things that break the normal rules, this type of IDS can often spot new or modified attacks that signature-based systems might miss.
  But figuring out what "normal" looks like can be tricky, and these systems sometimes raise too many false alarms by flagging harmless activity as suspicious.

- pecification-based IDS uses a set of rules and thresholds that define the expected behavior for different network components such as nodes, protocols, and routing tables. A human expert provides the features provided in the specification-based IDS.
  If any behavior falls outside the permitted range defined by these specifications, it is treated as suspicious or malicious. The accuracy of this approach hinges heavily on the quality and comprehensiveness of the specifications provided.

- Hybrid intrusion detection systems (IDS) try to bring together the best parts of signature-based, anomaly-based, and specification-based methods. By using a mix of these approaches, they can cover more types of attacks and improve detection accuracy. This combination allows hybrid systems to catch both known threats and unusual behavior, making them more effective overall.

## 1.2 Wi-Fi Intrusion Detection Systems

Wi-Fi Intrusion Detection Systems (IDS) can be broadly categorized based on the network layer where they perform their monitoring and analysis. These categories include: (1)

- Physical layer based intrusion detection systems work at the lowest level of the network and focus on the actual wireless signals. They use features like signal strength, signal to noise ratio (SNR), and other radio measurements, often collected using multiple antennas, to spot unusual or suspicious activity. These systems are especially good at detecting attacks such

as jamming, where someone floods the airwaves with noise to block communication, or MAC spoofing, where a device pretends to be someone else on the network.

- MAC layer based intrusion detection systems work by checking the control information in Wi-Fi signals. They look at things like frame headers to find unusual behavior on the network. This helps them spot threats such as fake access points, forced disconnections, and other ways the Wi-Fi rules are misused. By noticing patterns that do not fit normal activity, they can catch signs of an attack.

- Cross layer intrusion detection systems combine information from both the physical layer (signal strength, noise levels) and the MAC layer (Wi-Fi control messages) to get a clearer view of network activity. By looking at both types of data, these systems can detect more types of attacks. For example, they can spot problems in the signal, like jamming, while also checking if devices are breaking Wi-Fi rules, like pretending to be a real access point.
  This method is better at finding complex or hidden attacks that might be missed by systems that only look at one layer. It makes it harder for attackers to hide because both the signal and behavior are being checked together.

The Wi-Fi IDS that detects attacks on the physical layer uses signal strength through multiple antennas to detect the attacks on the Wi-Fi network. Physical layer Wi-Fi IDS' detect attacks like network jam- ming attacks and MAC address spoofing attacks on the Wi-Fi network. Design and development of physical layer Wi-Fi IDS is complex as it has to account for signal fading, noise, changes in the medium, and the effects of user movement. Wi-Fi IDS' that secure the data link layer use the data obtained from the Wi-Fi frame to detect attacks. Open source intru- sion detection systems like Snort and most of the commercial Intrusion detection systems available like AirMagnet [28] and some detection engines in Air Defense [29] use a signature- based (it is often referred to as misuse) detection approach to detect Wi-Fi attacks. However, misuse detection approaches depend on the use of attack signatures to detect attacks and are unable to detect modified attacks, and zero-day attacks

## 1.3 Wireless Intrusion Detection Systems(WIDS)

WIDS is an Anomaly Based Intrusion Detection System for Wi-Fi networks. WIDS models the normal behavior of the Wi-Fi protocol by monitoring the state transitions of the Wi-Fi protocol state machine, as the state machine captures the protocol's normal behavior through its state transitions. This method looks at the raw Wi-Fi frames and breaks down the traffic between a source and a destination into what's called "observation-wireless flows." An observation-wireless flow is just a continuous stream of frames or packets between two devices, recorded at specific time intervals. It shows the

different steps the protocol goes through during communication.
For example, in the Wi-Fi protocol, the flow might start with Authentication frames, then move to Association request frames, followed by Data frames, and finally end with Deauthentication frames.(1)

# 2 MAC layer based Intrusion Detection Systems

## 2.1 IEEE 802.11 MAC layer protocol and vulnerabilities

The protocol addresses the fact that Collision Sense Multiple Access (CSMA) is not sufficient to eliminate collisions in ad hoc networks or wireless LANs. It uses a distributed co-ordination function or DCF that is based on the exchange of control messages. A sender sends a Request to Send (RTS) message and in response a receiver sends a Clear to Send or (CTS) message if it is able to accept the message. Any node that overhears either of the messages is rendered silent. Thus the channel is available for the exclusive use of the communication under discussion. When a node wishes to transmit data it senses the channel to find out if any transmissions are in the vicinity. If there are any nearby transmissions or if a response to an RTS message is not received within a pre-determined number of attempts the node backs off in accordance to the binary exponential back-off scheme (2)

- Distributed Coordination Function (DCF)
  DCF is a way to control how devices share the Wi-Fi channel. It works by using a four-step process to help avoid collisions:
  - Request to Send (RTS): When a device wants to send data, it checks if the channel is free. If it is, the device sends a request (RTS) to the receiver..
  - Clear to Send (CTS): If the receiver is ready and the channel is clear, it replies with a "Clear to Send" (CTS) message.
  - Channel Reservation: Other nearby devices that overhear the RTS or CTS messages know the channel is in use, so they hold off on sending their data to avoid interfering.
  - Data Transmission: Once everything is set, the sender sends the data, and the receiver sends an acknowledgment (ACK) if everything was received correctly.
- Collision Avoidance and Backoff Mechanism
  If the channel is busy, or if the sender doesn't get a CTS response after trying several times, it starts a backoff process. This process is based on the Binary Exponential Backoff (BEB) algorithm, which makes the sender wait longer each time it fails. The longer wait time reduces the chances of the same collision happening again.

However, this method tends to favor the device that last successfully transmitted, which can sometimes lead to unfair channel access for other devices.

- The Capture Effect and Its Exploitation

  This problem is known as the capture effect, where busy devices that often get access to the channel end up using most of the transmission time. Meanwhile, devices that are less active or farther away keep having to wait, causing unfair use of the network. Malicious devices can exploit this by:

  – Continuously transmitting large volumes of data.
  – Repeatedly initiating RTS/CTS exchanges, or
  – Adjusting timing to take over the channel.

## 2.2 MAC Layer DoS attack on 802.11

- **Masquerading Attacks**

  In masquerading attacks, an attacker spoofs the MAC address of a specific station or AP. Due to the open nature of the wireless medium, an attacker can easily sniff wireless traffic in order to find the identities of the devices on the network. Those identities can then be easily spoofed by using device driver software. Below is a list of the attacks discussed in the literature until now.: (3)

  – **Deauthentication Attacks**

    In the 802.11 Wi-Fi protocol, every device has to go through an authentication process with the access point (AP) before it can connect to the network. As part of this process, either the AP or the device can end the connection by sending a special message called a deauthentication frame.

    The problem is that these deauthentication messages are not protected. They aren't encrypted or checked for authenticity, which makes them easy to fake. An attacker can take advantage of this by sending a fake deauthentication message using the MAC address of either the AP or the device. When the target receives this fake message, it thinks it's being told to disconnect—so it does.

    If the attacker keeps sending these fake messages, the device gets disconnected again and again, making it impossible to stay online. This kind of attack can target a single device or even all devices connected to a network.

    There are many tools, like Airjack, Void11, and KisMAC, that can be used to launch these attacks automatically.

- **Disassociation Attacks**

  Disassociation attacks are very similar to deauthentication attacks and take advantage of the same type of weakness. After a device connects to a Wi-Fi network through authentication, it goes through an association step to fully join the network. The rules say that a device can only be connected to one access point (AP) at a time, and either the device or the AP can end this connection by sending a disassociation message.

  Just like deauthentication messages, these disassociation messages are not protected. That means attackers can easily fake them. If a device gets one of these fake messages, it gets disconnected from the network right away.

  While both types of attacks are harmful, deauthentication attacks usually cause more trouble because they force the device to go through the full login process again, which causes longer delays and more disruption.

- **Power-Saving Exploits**

  In order to conserve power, the IEEE 802.11 clients can enter a sleep mode during which they are unable to transmit or receive. During this time the AP buffers all inbound data for the sleeping node until the client polls the AP for its data. An attacker can exploit this mechanism by:

  * Spoofing the polling message on behalf of a sleeping client, causing the AP to mistakenly believe the client has received its buffered data, prompting it to discard those packets.
  * Forging TIM (Traffic Indication Map) frames, which inform clients whether the AP has data pending for them. A spoofed TIM can deceive a client into believing no data is available, resulting in missed communications.
  * Injecting falsified synchronization frames (e.g., timestamps or TIM intervals), which can misalign a client's wake/sleep schedule, causing it to miss important frames or fail to reconnect with the AP.

- **Resource Depletion Attacks**

  Resource depletion attacks normally target shared resources such as the AP to exhaust its processing and memory power so that it can no longer provide services to other (legitimate) stations. These attacks can be accompanied by more sophisticated attack such as introducing rouge access points to hijack the abandoned stations. Some common resource depletion attacks discussed in the literature are described below..(3)

  - **Probe Request Flood**

In IEEE 802.11 networks, client devices send Probe Request frames to look for nearby Wi-Fi networks. Access points (APs) reply with details so the client can connect.

In a probe request flood attack, a hacker sends a huge number of fake probe requests. Each one uses a random, made-up MAC address, making it look like hundreds or thousands of devices are trying to connect. This overloads the AP, slows it down, and can cause delays, dropped packets, or even stop real users from connecting at all.

– **Authentication Request Flood**

An authentication flood attack happens when an attacker sends a huge number of fake authentication requests, each with a different fake MAC address. The access point (AP) tries to follow the rules and treats each request as real, using up memory and resources for every one.

As the fake requests pile up, the AP's memory fills up, and it can no longer handle new requests—even from real devices. If there's no MAC filtering or rate-limiting in place, it's very hard to stop this kind of attack.

– **Association Request Flood**

When a device tries to join a Wi-Fi network, it sends an Association Request to the access point (AP). The AP then stores the device's info in an association table, which is kept in its memory. According to the IEEE 802.11 standard, an AP can handle up to 2007 connected devices at once, but the real limit depends on the AP model.

If this table gets full, the AP won't let any new devices connect. An attacker who has broken WEP security can send fake requests using random, real-looking MAC addresses. By flooding the AP with these fake Association Requests, the attacker fills up the table and blocks new devices from joining.

According to the MAC protocol, an AP will not accept an Association Request sent by a station in unauthenticated and unassociated state. However, surprisingly, contrary to the specification, many APs also respond to association requests in their initial states

– **Media Access Attack**

IEEE 802.11 uses a virtual carrier sensing mechanism, specifically the Network Allocation Vector (NAV), to help address the hidden terminal problem. Control frames such as RTS (Request to Send), CTS (Clear to Send), and ACK (Acknowledgement) contain a duration field that informs nearby nodes of expected channel occupancy time. An attacker can disrupt normal communications by repeatedly sending RTS/CTS frames with unusually large duration values, thus causing nearby legitimate nodes to defer their transmissions unnecessarily. By constantly keeping the NAV value above zero, the attacker effectively

prevents access to the medium, resulting in significant performance degradation and denial of service.

TYPES OF DOS ATTACKS AND COUNTERMEASURES

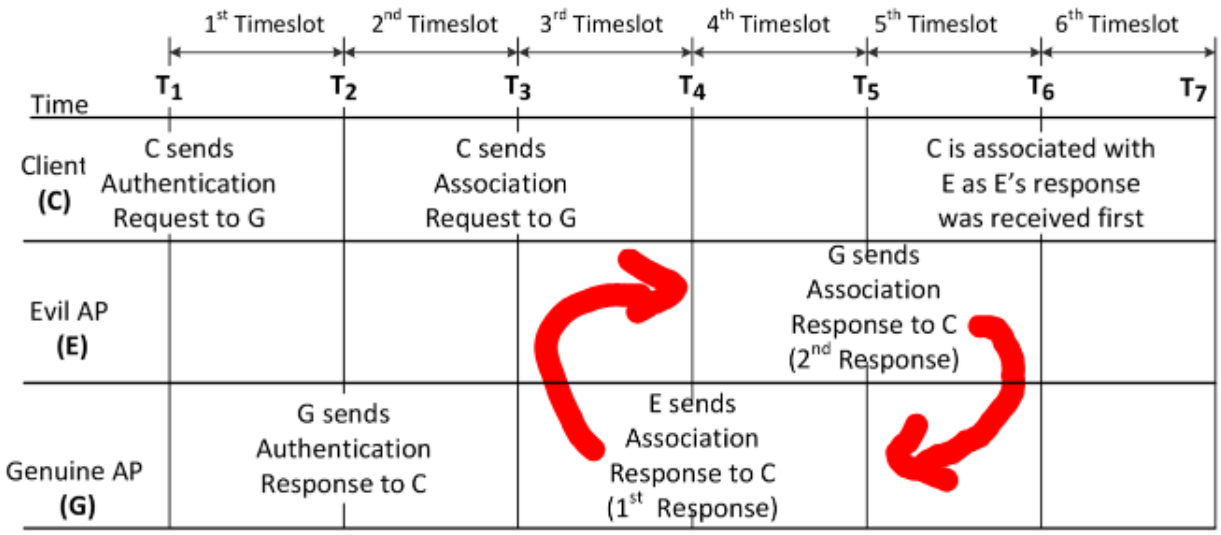
| Attack | Target | Existing countermeasures |
|---|---|---|
| Probe Request Attack | AP | Signal Print |
| Authentication Request Attack | AP | Signal Print, Client Puzzle |
| Deauthentication Attack | Station and AP | Signal Print, MAC Spoof Detection, Delaying the effects of request |
| Association Request Flood | AP | Signal Print |
| Deassociation Attack | Station and AP | Signal Print, MAC Spoof Detection, Delaying the effects of request |
| Virtual Carrier Sense Attacks | Medium Access | Explainability of Collision, Spatial Retreats |
| Sleeping Node Attack | Station and AP | Limiting Duration Field Value, Signal Print, MAC Spoof Detection |

(3)

## 2.3 Examples of MAC Layer based Intrusion Detection Systems

### 2.3.1 Evil Twin attack IDS

. An evil twin AP is setup by an attacker to tempt clients into connecting to it and redirecting them to fraudulent websites to steal client information. The attacker spoofs the MAC address and the Service Set IDentifier (SSID) of the genuine AP 1 to setup evil twin. When a client sees the list of avail- able Wi-Fi APs, it sees only one AP instead of two APs as the evil twin AP spoofs both the MAC address and the SSID of the genuine AP. Most of the modern operating systems (OS) are configured to connect to the AP providing higher signal strength in-case there are multiple APs associated with the same SSID. In presence of an evil twin AP, if the signal strength of the evil twin exceeds the signal strength of the genuine AP, the client(s) get associated with the evil twin AP. Higher signal strength leads to higher throughput and less frame loss. Hence a client always prefers to opt for APs offering higher signal strength. (4)




Existing intrusion detection system:

- Monitoring Wi-Fi Traffic: Tools like sniffers can watch network traffic and look for unusual AP MAC addresses or SSIDs to spot fake access points. But this doesn't work well against Evil Twin APs, because they copy both the name (SSID) and MAC address of the real AP, making them hard to tell apart.
- Timing and Feature-Based Methods: These approaches check for things like response delays (e.g., round-trip time or time between packets) that might happen if the Evil Twin forwards data through another device
- Problems: These methods can be tricked by normal network delays, fooled if the attacker is directly connected, and they use a lot of processing power
- IDS Approaches: Signature-based IDS only detects known attacks. Anomaly-based IDS struggles with Evil Twin detection due to lack of statistical deviation between normal and attack behavior.

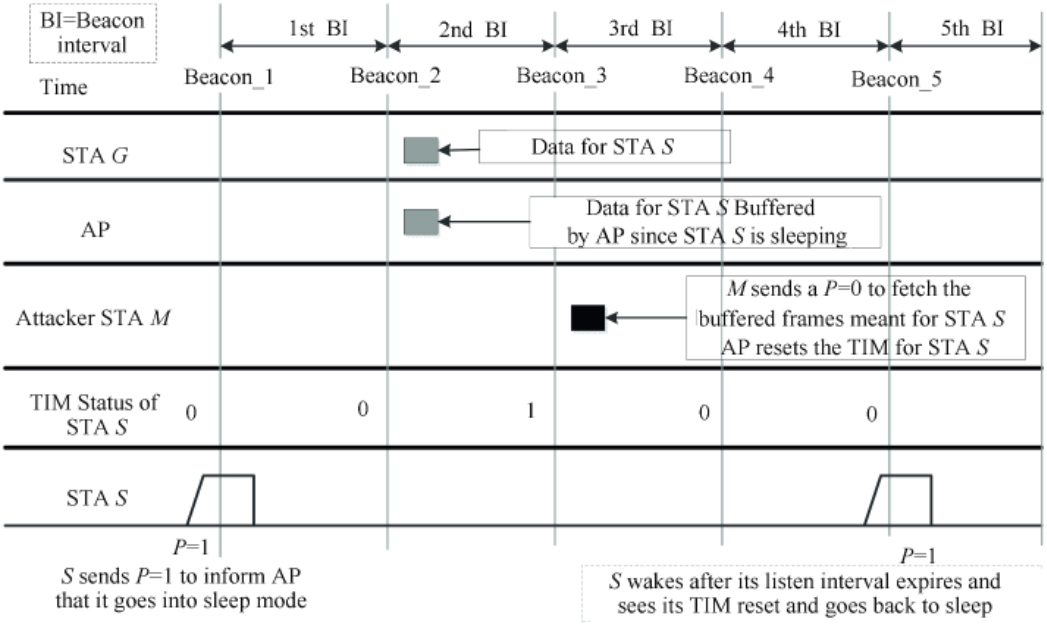
New improvised approach:

The detection of an Evil Twin access point (AP) is based on monitoring the sequence of authentication and association frames exchanged between a client and APs. The Intrusion Detection System (IDS) first observes the authentication request and response frames, followed by the client's association request. It then checks if the client receives one or multiple association responses. If only one response is received, the network is assumed to be operating normally. However, if two association responses are observed, it raises suspicion, as it could indicate the presence of an Evil Twin AP. That said, multiple responses can also occur under normal conditions—such as when an AP retransmits an

association response due to a lost acknowledgment. To distinguish between genuine retransmissions and an Evil Twin attack, the IDS analyzes specific fields in the responses: the retry bits (to detect retransmissions), sequence numbers (to verify frame order), and the Association ID (AID). Differences in these parameters can confirm the presence of an Evil Twin AP attempting to impersonate a legitimate one. (4)

### 2.3.2 Ps Poll DoS attack IDS

Wi-Fi devices, especially those operating on battery power, must carefully manage energy consumption to extend their operational lifetime. To support this, the IEEE 802.11 standard includes a power management feature that allows wireless stations (STAs) to enter a low-power sleep mode while still maintaining network connectivity. During this sleep period, the access point (AP) temporarily stores any frames intended for the sleeping STA. When the STA wakes up, it can send a null data frame or a Power Save Poll (PS-Poll) frame to request the delivery of these buffered frames.




(5)

However, this system can still be tricked by a Power Save Denial of Service (PS-DoS) attack. In this attack, a hacker sends fake PS-Poll or null data frames, pretending to be a sleeping device (STA). The access point (AP) thinks the request is real and sends the stored data to the attacker. Later, when the real device wakes up, its data is already gone.

These attacks are hard to detect or stop. Most current solutions need changes to the Wi-Fi protocol, special encryption, or expensive hardware to catch the attack making them costly, hard to manage, and tricky to set up in large networks. Plus, because the attacker copies normal traffic patterns and doesn't change how the network usually behaves, traditional signature- or anomaly-based

IDS have a tough time spotting this kind of attack.(5)

An STA in sleep state must periodically wake up and listen to the beacon frame. An STA uses the value of listen interval (LI) for waking up periodically. If an STA is in sleep state, it must wake up after LI number of beacons to check for the presence of buffered frames at the AP. For example, if the STA is in sleep state and its LI is 5, the STA needs to wake up every 5th beacon to check if any frame(s) is (are) buffered at the AP. The value of LI is decided during the association process. The LI is a 2 byte element in the association request frame sent by the STA to the AP. The AP needs to buffer the frame(s) for a sleeping STA at-least for the corresponding STA's LI number of beacon frames. A sleeping STA wakes up after the LI duration and reads the TIM element of the beacon frame. If the AID of the STA is set (reset) in TIM, it implies that data is buffered (not buffered) at the AP. The STA sends a null data frame with Power Mgmt bit set to 0 to retrieve the buffered frame(s) at the AP. If a STA continues to remain in sleep state even after its LI expires, the AP discards the buffered frame(s) for the corresponding STA.

This mechanism ensures energy-efficient communication by allowing STAs to conserve battery life without sacrificing data delivery. However, it also places responsibility on the STA to adhere to its LI schedule; otherwise, it risks losing important data stored temporarily by the AP. (5)

There are however, better intrusion detection systems to realise the occurrence of a ps DoS attack:

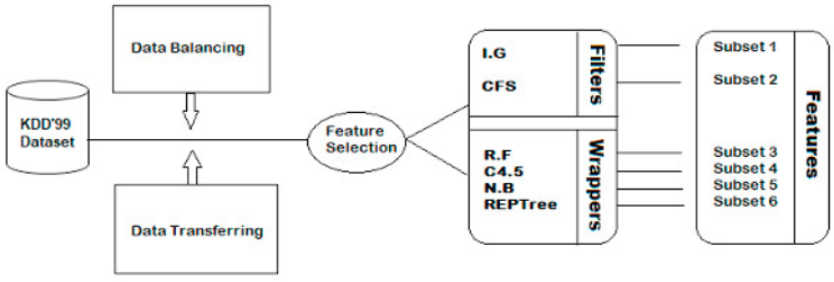
If the buffered frames for a STA are fetched before the expiry of its LI, IDS marks this activity as suspicious. Such activity cannot be directly marked as attack since the 802.11 standard does not prohibit or restrict the Wi-Fi STAs to wake up earlier than their scheduled waking up. This is plausible as it may happen that the STA may have to transmit some critical data for which it may have to break its sleep cycle. So, every STA that wakes up earlier than scheduled cannot be assumed to be an occurrence of the PS-DoS attack. However, in the proposed scheme we have the dummy STAs as part of detection methodology. The dummy STAs are software controlled and their communication is handled by the IDS. The IDS ensures that the dummy STAs never wake up before the expiry of their LI. Only the IDS possesses the dummy STA's MAC address and is regularly updated by the IDS. The need for updating the dummy MAC address and other characteristics of the dummy STAs are explained later. Upon observing an early wake up frame3 for any STA(s) associated with the monitored AP, the IDS sends a power save probe to the dummy STA. As the dummy STA is in sleep state at the time IDS sends a power save probe, the frame is buffered at the AP. The power save probe is a simple 802.11 data frame sent from IDS destined to the dummy STA. If the buffered frame(s) meant for the dummy STA are fetched before the expiry of the LI of the dummy STA under question,

the presence of the PS-DoS attack is confirmed

The clever part of this detection mechanism lies in what happens next: if the IDS detects that the buffered frame(s) meant for the dummy STA are fetched before its LI expires, this clearly signals malicious behavior. Because the IDS controls the dummy STA and knows it has not initiated any request, the early retrieval must have been triggered by an unauthorized entity impersonating the dummy STA. This indicates that an attacker is likely attempting to retrieve buffered frames on behalf of sleeping STAs, confirming the presence of a PS-DoS attack. (5)

### 2.3.3 Probe DoS attack IDS

Probe attacks are aimed at gathering information about the target network from a source that is often external to the network. Denial-of-Service (DoS) attacks results in an interruption of the service by flooding the target system with illegitimate requests. Although anomaly-based methods are not widely commercialized due to the high rate of false alarms generated, they are of a crucial importance as they can detect zero-day attacks, and thus more related research works are conducted. One of the main techniques used in network anomaly-based systems, is to monitor and capture network traffic, and analyze different features of a TCP/IP connection to look for anomalous patterns that indicate the presence of an eventual attack. KDD'99 use 41 features as described in MADAM ID Framework, participating in the DARPA Intrusion Detection Evaluation Program. The 41 features are classified into intrinsic features that are used for general analysis, and traffic and content features, each designed to detect a specific type of intrusions when combined with intrinsic feature. Using the 41 features in model building is likely to impact both accuracy and efficiency as some features can be redundant or irrelevant. This can be problematic in high speed networks where any delays can make the system to be compromised for some period of time before raising any alarms.(6)




To deal with these problems, a lightweight machine learning-based Intrusion Detection System (IDS) can be used to spot Probe and DoS attacks in fast networks. The goal is to keep the system simple and fast, while still being accurate.

This is done by smartly picking only the most useful features from the data. The system uses

Information Gain (IG) and Correlation-based Feature Selection (CFS) to figure out which features are most important. Then, it uses machine learning models like Naive Bayes (NB), C4.5 decision trees, Random Forest (RF), and REPTree to test different combinations of features and see which ones work best for detecting attacks. (6)

(6) The detection mechanism works as follows: network data is first preprocessed by converting symbolic features into numeric form and balancing the dataset to prevent bias (as DoS attacks dominate the original dataset). Then, selected features are fed into the chosen machine learning classifiers to build detection models. During operation, the IDS monitors network traffic in real time, extracts the selected features, and uses the trained models to classify the traffic as normal or malicious. The system was also tested on novel attack types not present in the training data and showed high detection rates for Probe attacks, confirming its generalization ability. (6)

## References


[1] P. Satam and S. Hariri, "Wids: An anomaly based intrusion detection system for wi-fi (ieee 802.11) protocol," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 1077–1091, 2021.

[2] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the mac layer in wireless ad hoc networks," in *MILCOM 2002. Proceedings*, vol. 2, 2002, pp. 1118–1123 vol.2.

[3] T. Farooq, D. Llewellyn-Jones, and M. Merabti, "Mac layer dos attacks in IEEE 802.11 networks," in *Proceedings of the 7th Annual Conference on Communication Networks and Services Research (CNSR)*. IEEE, 2009, pp. 418–423.

[4] M. Agarwal, S. Biswas, and S. Nandi, "An efficient scheme to detect evil twin rogue access point attack in 802.11 wi-fi networks," *International Journal of Wireless Information Networks*, vol. 25, no. 2, pp. 130–145, 2018.

[5] M. Agarwal, S. Purwar, S. Biswas, and S. Nandi, "Intrusion detection system for ps-poll dos attack in 802.11 networks using real time discrete event system," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 4, pp. 792–808, 2017.

[6] T. AIT TCHAKOUCHT and M. EZZIYYANI, "Building a fast intrusion detection system for high-speed-networks: Probe and dos attacks detection," *Procedia Computer Science*, vol. 127, pp. 521–530, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918301637


(1) (5) (4) (2) (3) (6)