Demonstration of MITM attack in Synchrophasor Network using MAC spoofing

Amit Tiwari
amittw@iitk.ac.in

Ankush Sharma
ansharma@iitk.ac.in

Saikat Chakrabarti
saikatc@iitk.ac.in

***Abstract*—Communication is critical for power system operation and control. Data transfer via digital means is vulnerable to security and privacy concerns. MITM attacks pose a risk to the data integrity of synchrophasor values transferred as digital data within the smart grid. The purpose of this research is to demonstrate how utilizing MAC spoofing can improve the stealth and robustness of MITM attacks in synchrophasor networks. After a session hijack, when false data was eventually injected, it was evaluated and processed by the Phasor data concentrator, ensuring consistent networking and the attacker's non-detectability. For generic experiment results, different sub-networks based on the master-slave topology of synchrophasor networking and commercially available PMU and PDC were used in a laboratory-scale setup.**

Keywords—Cyber attack, Power system, MITM attack, Synchrophasor Network, Smart grid, MAC Spoofing, TCP sequencing

I. Introduction

Smart grid optimization in power systems necessitates continual monitoring of its sub-components. Monitoring measures rely significantly on communication among power grid sub-components. This also improves power system control. Synchrophasor networks are one such critical component of the power grid. Synchrophasor Measurement Units (PMU) are used to measure system states in millisecond increments. A significant number of PMUs are employed to cover bigger networks. The measurements by the PMU are sent to the PDC following IEEE C37.108 protocol, which is then fed to the control center for further analysis. This transmission of measurements uses interconnected networking between devices installed in different sub-network following master-slave topology. Given the importance of measures in control, these messages must maintain integrity and authenticity.

MITM cyber operations pose a risk to the communication system. MITM attacks come in numerous forms, including false data injection, session hijacking, authentication control, and denial of service. Following the assault, power system state estimation can be used to minimize inaccuracies and inconsistencies caused by faulty data from system equipment. This study illustrates the feasibility of inserting bad data into a synchrophasor network via a MITM attack, intending to provide insight into steps taken before any attack. Several surveys [5] have been undertaken to analyze potential cyber risks and responses in power networks [3][6]. In addition to the precision of measurements, there are other cyber threats [8][10] in power grid communication, such as denial of service (Dos) attacks, which result in the unavailability of components established in smart grid network, false data injection, deployment of malwares[4] resulting in authentication control, which results in more severe damage, such as blackout to smart grid communication and transmission network[13]. This study shows a MITM attack on a TCP-based synchrophasor the network that results in session hijacking and false data injection. The current study focuses on giving a technical understanding of the attack process, which will aid security analysts in the development of effective threat detection and mitigation solutions in the future.

The previous study discusses MITM attacks on synchrophasor networks[7], taking into account multiple PMU/PDC communication standards[15]. This document illustrates a MITM attack on a synchrophasor network following the IEEE 37.108 standard. The delivery of packets inside a local network is associated with the MAC address[4] of devices within the network, while the delivery of packets coming from the outer network is associated with the MAC address of routers. This implies that by changing the MAC address along with the sequence number(TCP) of packets, the attacker can ultimately keep the network connection stable and synchronized while injecting false packets[14]. Spoofing attacks use ARP Cache poisoning to sniff. The main practice for ARP poisoning[14][7] is to transmit ARP/ICMP packets that inherit the attackers' IP/MAC address [7] and re-route the packets from the original destination. This facilitates eavesdropping by the third party in ongoing communication. The information gained in this step is further used to exploit the system. After comparing the generic sniffing approach (ARP spoofing) as studied in earlier research[4][14][7], this example sniffs packets using MAC spoofing rather than ARP spoofing, resulting in a stealthier attack. Figure (2) depicts the different approaches to MAC/ARP spoofing. The primary parameters that contribute to the stealthiness of demonstrated MITM attacks are later outlined in this study for the future-based solution.

A. Smart Grid Synchrophasor Network

The Phasor Measurement Unit (PMU) is a device that allows synchronized measurement of the voltage and current of electrical systems and is sent to the control center via a different Phasor Data Concentrator (PDC). This is shown in figure (1) below:

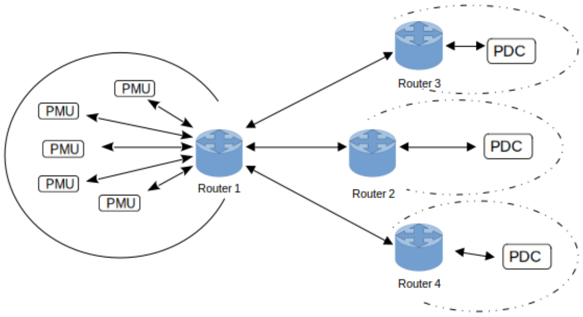


Figure 1: PMU and PDC in a communication network

IEEE C37.108 protocol is used for measurement and data transfer in power systems between PMU and PDC using various types of frames [1].

B. DHCP Protocol

By serving as a server, the DHCP protocol simplifies the process of IP allotment inside a network. When a DHCP-enabled client connects to the network, the server maintains a pool of IP addresses and leases one to it. Because IP addresses are dynamic (leased) rather than static (issued permanently), addresses that are no longer in use are immediately returned to the pool for reallocation.

C. TCP Sequencing

The sequence number is a counter used in TCP protocol to keep track of every byte sent outward by a host. If a TCP packet contains 100 bytes of data, then the sequence number will be increased by 100 after the packet is transmitted. While after receiving 100 bytes, the ACK flag of length 0 would be sent as an acknowledgment by the receiving host. Every TCP packet contains these numbers in the TCP header. This helps in enabling ordered and reliable data transfer for TCP streams. It allows the retransmission of lost packets.TCP Retransmission occurs when the time-out counter expires before receiving the acknowledgment or 3 duplicate acknowledgments are received from the receiver for the same received segment. In case the sender sends a packet considering it was lost, even though the receiver sent an acknowledgment, then sent packets are termed as spurious retransmission on the receiving end.

II. MITM ATTACK

A man-in-the-middle (MITM) attack occurs when a malicious user inserts himself into communication between two users in order to eavesdrop or impersonate one of the hosts, giving the impression that a regular flow of information is taking place. Sniffed information during private communication is then used for false packet injection or converting sniffed information to other attack vectors such as Denial of service. The attack scenario demonstrated in this paper shows an attacker between the PMU and PDC communication and how the session can be intercepted in a synchrophasor network.

Sniffing is the basis of any MITM attack. This provides the attacker with information that is further used for the exploitation of the system. To intercept a communication attacker must bring the packets sent by PMU to PDC on the attacker's system. This is achieved by poisoning the ARP table within the sub-network, such that the routing path assigned to packets leads them to the attacker. This means the router of the PDC sub-network must recognize the attacker as the PDC. Once the attacker starts intercepting the stream of packets sent by the PMU, the attacker extracts and analyzes the information within one of those packets and gets ready for sending the forged frames. Since the speed of transmission by actual PMU is generally many frames/sec it is obvious that some packets will be exchanged after the attacker has sniffed the packet. To move from sniffed sequence number to the sequence number which is expected by the PDC, the attacker creates a disruption in communication between PMU and PDC in a partially controlled way,e.g by disabling then enabling IP forwarding, right after sniffing the packet. This ensures the exchange of a minimum number of packets in the meantime. The marginal difference in sequence number, if still left can be compensated by the higher transmission speed of the attacker. Eventually, the attacker gets the connection and PDC starts analyzing forged data frames as sent by the attacker.

There are two instances in this process where the attacker can be caught and identified. Firstly, while sending the ARP or ICMP packets, the IP and MAC address used by the attacker is revealed in those sent packets. Secondly, the attacker relies on disruption of communication for an effective MITM attack, by either turning the PMU transmission off or by using IP forwarding so there is no issue in communication while the attacker sends the forged packet to PDC. In any case, disruption is not in full control of the attacker, it depends on the network and how much time will it take to reset the ARP table within the network. If this time taken by the router is greater than the connection reset interval of PDC, then the actual connection will reset and MITM will fail.

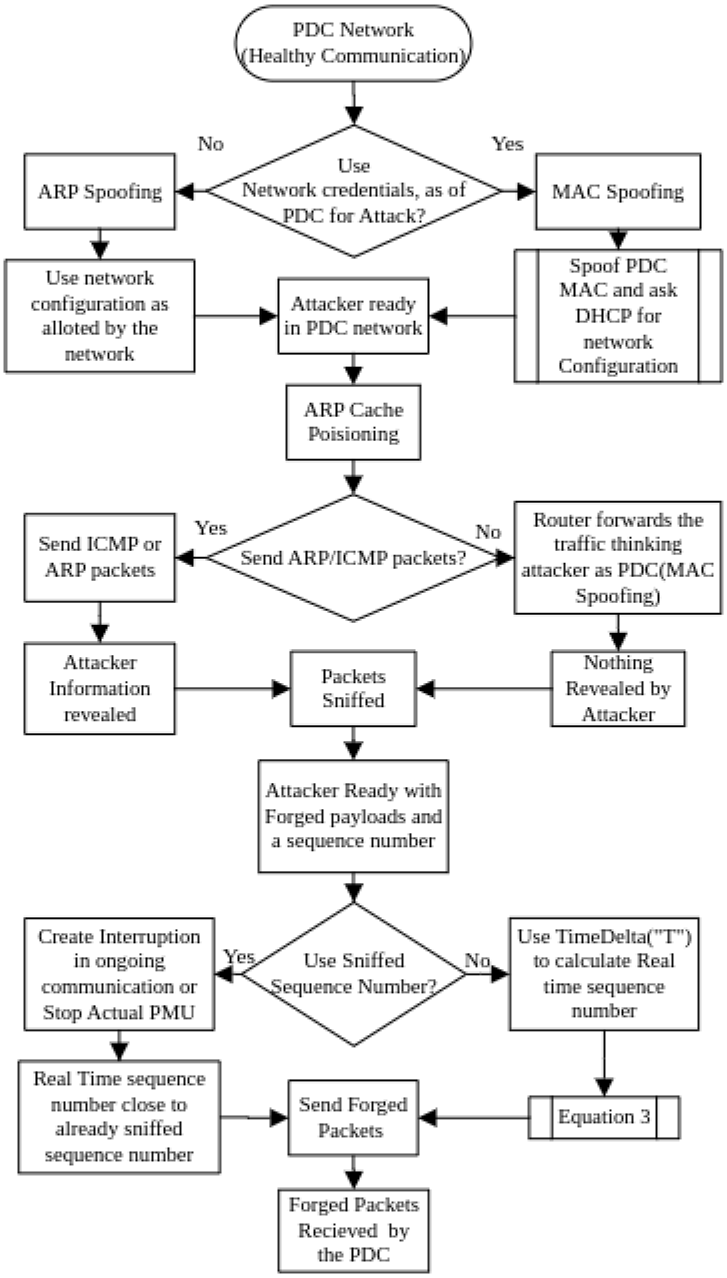


Figure 2: Comparison in the approach of MITM attack

The experimental setup consists of three Core i7-7700 CPUs acting as PDC, Attacker, and attacker’s alias. OpenPDC [12] software was used for processing high-speed time series data, accompanied by Wireshark [10] to capture the network traffic. Scapy[17] a powerful interactive packet manipulation python program was used to sniff and forge TCP packets. Three different sub-networks on LAN are used in the demonstration for the feasibility of the MITM attack. Two different PMUs namely SEL and Arbiter using TCP protocol were used while experimenting, The MITM attack in this demonstration is categorized into three phases: sniffing information, processing it, and then using the processed information for hijacking the session.

A. *MITM: Sniffing Information*

1) ARP Poisoning using MAC spoofing

When two devices have the same MAC address and ask DHCP server for an IP, DHCP sends the same IP and other network configurations to both of them. The packets received by the router are forwarded to both of them randomly at a random rate in such a scenario.

2) Sniffing during Demonstration

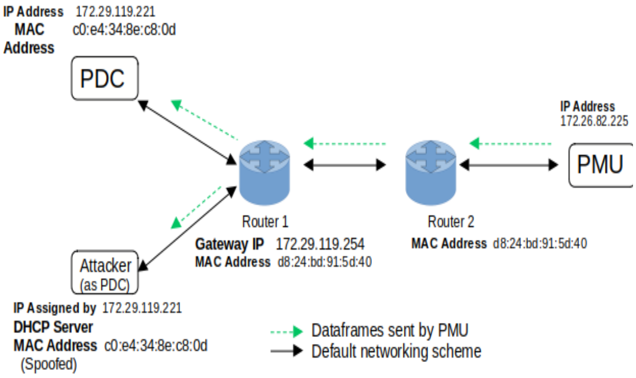

IP Address 172.29.119.221
MAC Address c0:e4:34:8e:c8:0d
PDC
IP Address 172.26.82.225
PMU
Router 1
Router 2
Gateway IP 172.29.119.254
MAC Address d8:24:bd:91:5d:40
MAC Address d8:24:bd:91:5d:40
Attacker (as PDC)
IP Assigned by 172.29.119.221
DHCP Server
MAC Address c0:e4:34:8e:c8:0d (Spoofed)
Dataframes sent by PMU
Default networking scheme

Figure 3: Sniffing using MAC Spoofing(pretending as PDC)

The attacker can either spoof the MAC address of the PDC or that of the Router, in order to intercept packets exchanged between them. Spoofing the MAC of the router will eventually result in a network reset and will create noticeable instability in any network. While spoofing the PDC's MAC, not only keeps the networking system stable but also facilitates sniffing figure (3), This makes the attack stealthier as no information of the attacker is revealed in sending ARP/ICMP packets for sniffing traffic as depicted in figure (2).

B. *MITM: Information Processing*

The attack is implemented on the sequential transmission of IEEE 37.108 payloads exchanged between PMU and PDC with a fixed transmission rate. This sequential communication is maintained by TCP sequence numbers. The length of the TCP payload is added in the last used sequence number for generating a new sequence number. This means if the length of the payload remains constant such as IEEE 37.108 payloads, then if n packets are exchanged after sniffing a packet, adding (n*(Payload Length)) to sniffed sequence number will give the current sequence number as expected by the PDC to the attacker.

Sniffed Packet is used to create a forged packet with a random frequency in a small range of 56Hz to 57Hz for demonstration. 45Hz to 54Hz is the actual range of frequency considered for this demonstration. To distinguish between actual and forged packets attacker has used a TCP URG flag in forged packets along with PSH and ACK flags as used by the actual PMU. If the attacker sends the packet from its device, the attacker's MAC address would be reflected in forged packets, as the attacker and PDC are on the same network. This was avoided by using a third network for sending forged packets. The extracted information from the sniffed packet was sent to the attackers' alias in another sub-network as shown in figure (4).

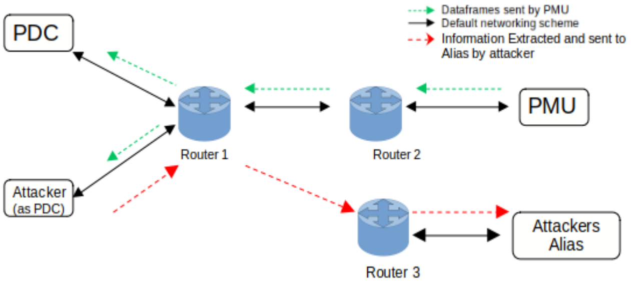


Figure 4: Extracted information sent to Attackers alias in other sub-network using SSH

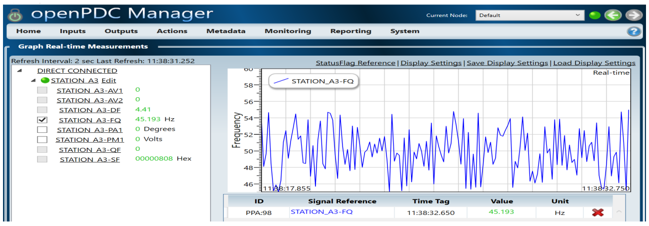
C. *Sending Forged Packets*

When the router of one sub-network receives the packet from any other sub-network, it replaces the source MAC Address in the data link layer with its own MAC address. This means the router will first tag the source MAC as its own and will then forward the packet within its network. This makes attackers forged packet resemble the actual packet as received by the PDC. The similarity in the captured packet by the PDC can be seen in figure (11) and figure (12).

III. Demonstration

A. *Normal Communication*

PMU sends the data frames to PDC at a fixed transmission rate. Each data frame sent during transmission contains estimates of electrical phasor quantities established in the electricity grid.



Current Node: Default

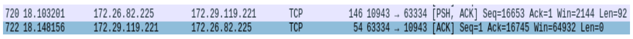
Refresh Interval: 2 sec Last Refresh: 11:38:31.252

DIRECT CONNECTED
STATION_A3 Edit

□	STATION_A3-AV1	0
□	STATION_A3-AV2	0
□	STATION_A3-DF	4.41
☑	STATION_A3-FQ	45.193 Hz
□	STATION_A3-PA1	0 Degrees
□	STATION_A3-PM1	0 Volts
□	STATION_A3-QF	0
□	STATION_A3-SF	00000808 Hex

ID	Signal Reference	Time Tag	Value	Unit	
PPA:98	STATION_A3-FQ	11:38:32.650	45.193	Hz	✖

Figure 5: OpenPDC receiving phasor values sent by PMU



```
720 18.103201    172.26.82.225     172.29.119.221    TCP      146 10943 → 63334 [PSH, ACK] Seq=16653 Ack=1 Win=2144 Len=92
722 18.148156    172.29.119.221    172.26.82.225     TCP       54 63334 → 10943 [ACK] Seq=1 Ack=16745 Win=64932 Len=0
```

Figure 6: Exchange of a single packet between PMU/PDC

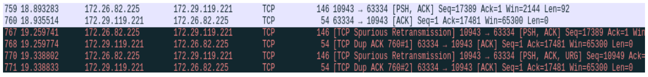
Figure (5) shows a normal communication and value of frequency in the data frame received, while Figure (6) shows the communication of a single payload between PMU and PDC as captured in network traffic.

PDC is equipped with a feature to reset the connection if there is more delay than the initialized value in the connection reset interval(5 seconds in this demonstration). If the attacker causes a delay of more than 5 seconds, the connection would reset, and sniffed information would be of no use then.

B. *MAC Spoofing*

For MAC Spoofing, the attacker disables its networking interface, then changes its MAC to PDC's MAC. When the attacker comes back on the network, it sends a discovery message to the DHCP server with PDC'S MAC and gets the network configuration as of the actual PDC. This results in the redirection of packets, intended for PDC to the attacker. The attacker sniffs the payloads intended for PDC. The delay caused in synchrophasor communication due to spoofing remains minimum,i.e

$$\text{Interruption Interval} < \text{Connection Reset Interval} \quad (1)$$



```
759 18.893283   172.26.82.225    172.29.119.221   TCP    146 10943 → 63334 [PSH, ACK] Seq=17389 Ack=1 Win=2144 Len=92
760 18.935514   172.29.119.221   172.26.82.225    TCP     54 63334 → 10943 [ACK] Seq=1 Ack=17481 Win=65300 Len=0
767 19.259741   172.26.82.225    172.29.119.221   TCP    146 [TCP Spurious Retransmission] 10943 → 63334 [PSH, ACK] Seq=17389 Ack=1 Win
768 19.259774   172.29.119.221   172.26.82.225    TCP     54 [TCP Dup ACK 760#1] 63334 → 10943 [ACK] Seq=1 Ack=17481 Win=65300 Len=0
770 19.338802   172.26.82.225    172.29.119.221   TCP    146 [TCP Spurious Retransmission] 10943 → 63334 [PSH, ACK, URG] Seq=10949 Ack=
771 19.338833   172.29.119.221   172.26.82.225    TCP     54 [TCP Dup ACK 760#2] 63334 → 10943 [ACK] Seq=1 Ack=17481 Win=65300 Len=0
```

Figure 7: Effect of MAC Spoofing

When the attacker resets its MAC back to normal, the data frames lost by PDC during MAC spoofing, are re-transmitted by the PMU for acknowledgment by the PDC. This can be seen in Figure (7). In the same time frame, the attacker starts sending forged payloads using information from sniffed packets such as IDCODE and TCP sequence numbers. TCP sequencing for continuous transmission, in general, can be depicted as in equation 2.

$$\text{Seq\_Num}_{New} = \text{Seq\_num}_{old} + 1*\text{TCP payload}_{Length} \qquad (2)$$

Where Seq_num is the TCP Sequence number. Now, using equation 2 and some margin of error we can rewrite equation 2 as :

$$\text{Seq\_Num}_{New} = \text{Seq\_num}_{old} + (\text{T*Trate})*(\text{length of-} \\ \text{-TCP payload}) + \text{margin of error} \qquad (3)$$

Where 'Trate' is the Transmission rate used by the PMU.

There exists a marginal difference between sniffed sequence number and the real-time sequence number as expected by the PDC(Considering network lag or retransmissions). It is evident from equation 3 that the new sequence number can be expressed as a function of time “T”. Attacker calculated the time interval “T” between the sniffing moment and the moment right before sending the forged packet. The sniffed sequence number is updated using equation 3.

This margin of error in sniffed and real-time sequence numbers can also be eliminated by using a higher transmission rate which will make the sequence number of every next packet close to the actual sequence number and will eventually catch up with the communication. In this demonstration higher transmission rate(almost twice the actual Transmission rate) is used initially and is lowered later after hijacking the connection by the attacker.

C. *Sending Forged Packets*

The attacker sends forged packets using an alias system placed in a different subnetwork. At this moment, both attacker and actual PMU are sending IEEE C37.108 payload to the PDC figure (8). The forged packet is identical in terms of the actual packet and differs only in terms of TCP Sequence number, IEEE C37.108 Parameters such as SOC, FRACSEC, CRC, and frequency of the system (For demonstration).

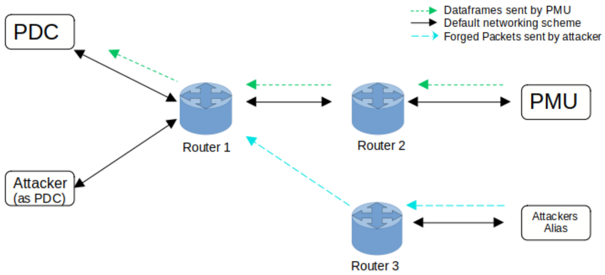
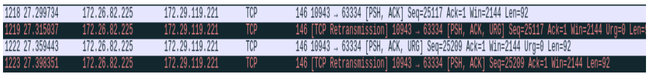


Figure 8: Forged packets sent by Attacker using some other sub-network

Instead of going for the exact sequence number, the attacker increased the transmission rate for forged packets until an acknowledgment from PDC is received. This ensures a possibility when the attacker and PMU will send a packet with the same sequence number, but because of the higher transmission rate compared to PMU, the attacker sends the next packet first and gets connected with the PDC.

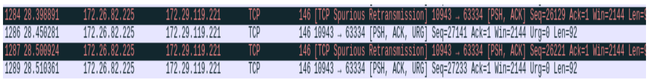


```
1218 27.299734   172.26.82.225   172.29.119.221   TCP    146 10943 → 63334 [PSH, ACK] Seq=25117 Ack=1 Win=2144 Len=92
1219 27.315037   172.26.82.225   172.29.119.221   TCP    146 [TCP Retransmission] 10943 → 63334 [PSH, ACK, URG] Seq=25117 Ack=1 Win=2144 Urg=0 Len=
1222 27.359443   172.26.82.225   172.29.119.221   TCP    146 10943 → 63334 [PSH, ACK, URG] Seq=25209 Ack=1 Win=2144 Urg=0 Len=92
1223 27.398351   172.26.82.225   172.29.119.221   TCP    146 [TCP Retransmission] 10943 → 63334 [PSH, ACK] Seq=25209 Ack=1 Win=2144 Len=92
```

Figure 9: Hijacking the connection

Initially, the attacker started with sequence number 10949 while the PMU was on sequence number 17389 figure (7). This accounts for a difference of 70 frames of six 92 bytes between the attacker and the PMU at the start. Figure (9) shows PMU and attacker both sending data frames with sequence number 25117. This is the instance where the attacker's transmission stream has caught up with the real-time transmission of PMU by using a higher transmission rate. The next Packet i.e Frame 1222 in figure (9) shows the attacker's first packet as received by the PDC with [PSH, ACK, URG] flags. This makes actual PMU use, already used sequence number, and is reflected as TCP retransmission in network traffic.

After receiving a few acknowledgments from the PDC, the transmission rate was reduced by the attacker using a time delay in the driver code. It was done to avoid the possibility of attack detection, using any receiving rate analysis on PDC's end. In absence of the right sequence number actual PMU remains in a state of retransmission as shown in figure (10).



```
1284 28.398891   172.26.82.225   172.29.119.221   TCP    146 [TCP Spurious Retransmission] 10943 → 63334 [PSH, ACK] Seq=26129 Ack=1 Win=2144 Len=
1286 28.450281   172.26.82.225   172.29.119.221   TCP    146 10943 → 63334 [PSH, ACK, URG] Seq=27141 Ack=1 Win=2144 Urg=0 Len=92
1287 28.500924   172.26.82.225   172.29.119.221   TCP    146 [TCP Spurious Retransmission] 10943 → 63334 [PSH, ACK] Seq=26221 Ack=1 Win=2144 Len=
1289 28.510361   172.26.82.225   172.29.119.221   TCP    146 10943 → 63334 [PSH, ACK, URG] Seq=27233 Ack=1 Win=2144 Urg=0 Len=92
```

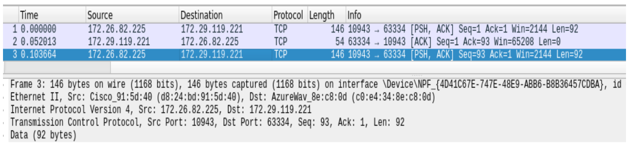
Figure 10: Actual PMU packets in the state of

After hijacking the session, forged packets were modified to increase the output frequency gradually in every packet(22500 steps in between 56-58) such that change in the mean and standard deviation of the last 10 instances remains minimal. The change in output frequency on openPDC can be seen in figure (13).

IV. Results and discussion

Synchrophasor networks are supporting infrastructure for operation and control in the power system. This paper performed a stealthy MITM attack in synchrophasor networks maintaining network stability in the process. The presented approach is divided into three stages: Eavesdropping, processing sniffed information, and then exploitation of the system using the extracted information.

The original packet as received by the PDC before any spoofing and MITM attack is shown in figure (11). It was the aim of the experiment to forge a similar packet and use it such that it is analyzed by the PDC without causing any alarm.

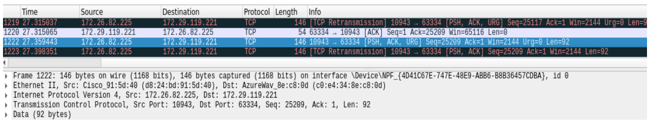


```
   Time       Source          Destination      Protocol Length Info
 1 0.000000   172.26.82.225   172.29.119.221   TCP         146 10943 → 63334 [PSH, ACK] Seq=1 Ack=1 Win=2144 Len=92
 2 0.052013   172.29.119.221  172.26.82.225    TCP          54 63334 → 10943 [ACK] Seq=1 Ack=93 Win=65208 Len=0
 3 0.103664   172.26.82.225   172.29.119.221   TCP         146 10943 → 63334 [PSH, ACK] Seq=93 Ack=1 Win=2144 Len=92

Frame 3: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{4D41C67E-747E-48E9-ABB6-B8B36457CDBA}, id
Ethernet II, Src: Cisco_91:5d:40 (d8:24:bd:91:5d:40), Dst: AzureWav_8e:c8:0d (c0:e4:34:8e:c8:0d)
Internet Protocol Version 4, Src: 172.26.82.225, Dst: 172.29.119.221
Transmission Control Protocol, Src Port: 10943, Dst Port: 63334, Seq: 93, Ack: 1, Len: 92
Data (92 bytes)
```

Figure 11: Original packet with different header fields

After the successful implementation of what is described in section IV the very first packet as received by the PDC and sent by the attacker is shown in figure (12).

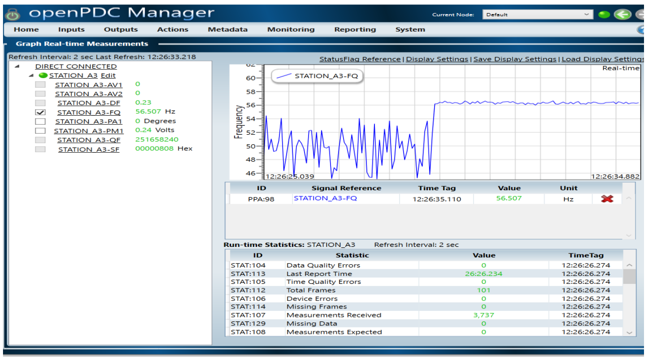


```
     Time       Source          Destination      Protocol Length Info
1219 27.315037  172.26.82.225   172.29.119.221   TCP         146 [TCP Retransmission] 10943 → 63334 [PSH, ACK, URG] Seq=25117 Ack=1 Win=2144 Urg=0 Len=9
1220 27.315065  172.29.119.221  172.26.82.225    TCP          54 63334 → 10943 [ACK] Seq=1 Ack=25209 Win=65116 Len=0
1222 27.359443  172.26.82.225   172.29.119.221   TCP         146 10943 → 63334 [PSH, ACK, URG] Seq=25209 Ack=1 Win=2144 Urg=0 Len=92
1223 27.398351  172.26.82.225   172.29.119.221   TCP         146 [TCP Retransmission] 10943 → 63334 [PSH, ACK] Seq=25209 Ack=1 Win=2144 Len=92

▸ Frame 1222: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{4D41C67E-747E-48E9-ABB6-B8B36457CDBA}, id 0
▸ Ethernet II, Src: Cisco_91:5d:40 (d8:24:bd:91:5d:40), Dst: AzureWav_8e:c8:0d (c0:e4:34:8e:c8:0d)
▸ Internet Protocol Version 4, Src: 172.26.82.225, Dst: 172.29.119.221
▸ Transmission Control Protocol, Src Port: 10943, Dst Port: 63334, Seq: 25209, Ack: 1, Len: 92
▸ Data (92 bytes)
```

Figure 12: First Forged Packet as received by the PDC

The above two results were reflected on the output screen of PDC and can be seen in figure (13). Since forged packets were constructed using user-defined functions in python, change in frequency can be customized by the attacker.



Refresh Interval: 2 sec Last Refresh: 12:26:33.218

DIRECT CONNECTED
- STATION_A3 Edit
  - □ STATION_A3-AV1 0
  - □ STATION_A3-AV2 0
  - □ STATION_A3-DF 0.23
  - ☑ STATION_A3-FQ 56.507 Hz
  - □ STATION_A3-PA1 0 Degrees
  - □ STATION_A3-PM1 0.24 Volts
  - □ STATION_A3-QF 251658240
  - □ STATION_A3-SF 00000808 Hex

ID	Signal Reference	Time Tag	Value	Unit	
PPA:98	STATION_A3-FQ	12:26:35.110	56.507	Hz	✖

Run-time Statistics: STATION_A3 Refresh Interval: 2 sec

ID	Statistic	Value	TimeTag
STAT:104	Data Quality Errors	0	12:26:26.274
STAT:113	Last Report Time	26:26.234	12:26:26.274
STAT:105	Time Quality Errors	0	12:26:26.274
STAT:112	Total Frames	101	12:26:26.274
STAT:106	Device Errors	0	12:26:26.274
STAT:114	Missing Frames	0	12:26:26.274
STAT:107	Measurements Received	3,737	12:26:26.274
STAT:129	Missing Data	0	12:26:26.274
STAT:108	Measurements Expected	0	12:26:26.274

Figure 13: Output of PDC after session hijack

Table 1: Factors responsible for the feasibility of the proposed MITM Attack

Index	Factor	Reason for being a factor
1.	MAC Spoofing	Simply Replacing MAC with routers MAC can prove as an attack on the network
2.	DHCP Server	Allots same IP Address to as many devices coming with same MAC Address
3.	Source Mac address in Data link layer	If a packet is received from an outer network, the information of the source MAC address(router/device) is lost, by the time it is received.
4.	Sync between Transmission Rate and Receiving Rate	The attacker used twice the actual transmission rate but was able to inject false data in PDC.

A. *Analysis of factors responsible for the proposed Attack*

The feasibility of this attack depends on a few common factors that should be accounted as loopholes in our Synchrophasor communication network as mentioned in table 1. For MAC Spoofing, it is required that the DHCP server allots the IP in that network. If static IP is used in sensitive devices within the power system it can provide isolation to devices against such spoofing. In MITM attacks, while sniffing attacker needs to be within the same network as PDC, but while sending forged packets attacker's packet must come to PDC from outside the PDC's network, or else the attacker's MAC would be sent to PDC along with the payloads. On the other hand, the attacker can choose any sub-network for the same, as PDC'S router doesn't know the IP of a device of some other sub-network, so it will have the MAC of PDC's router in the end as the source MAC.

To summarize, the MAC address field plays a vital role in the stealthiness of MITM attacks in synchrophasor networks. This could be used as a variable to increase security against MITM threats. Current research has tried to improve the detection and mitigation techniques of MITM attacks. Various research has been done on developing algorithms, and techniques to mitigate ARP Cache poisoning [10][7]. Encryption has proven to be a very good solution, as it eliminates the possibility of sniffing and ensures data integrity. Implementing encryption of data on top of encryption-based authentication can prove to be an efficient solution. An ideal defense mechanism is impossible to achieve but having multiple layers of security can prove to be an efficient defense system. Some of the defense mechanisms proposed for such MITM and MAC spoofing attacks are listed below:

1) *Mechanism of authentication* for clients trying to connect with the DHCP server.

2) *Static ARP*

This includes the addition of each device in the network to the ARP table of each device, which allows devices to ignore ARP replies in case of a cache poisoning attack.

3) *Encryption based Solution*

- *S-ARP: Key-based solution(public-private)*
- *T-ARP: Token-based solution*
- *SSL/TLS: Certificate-based communication*
- *Implementing IPSec security*

4) *Hardware-based solution*

Port security is provided by many switches these days, this helps in preventing ARP Cache poisoning by allowing only one device with one MAC on the network. Many Routers provide anti-ARP functionality using Dynamic ARP Inspection (DAI).

5) *Stacking protocols to increase the security layers*

Sniffing is imminent in any type of MITM attack. IPSec / transport layer security(TLS) is implemented over specific OSI layers and makes the system more secure. Similarly developing such algorithms which develop a gap or add an extra layer of security in between communication ends can prove to be an efficient solution to MITM/spoofing threats.

The potential MITM attack and its impact on the communication infrastructure of power systems are of great concern. MITM attack varies with the varying technique used for interception of ongoing communication. MAC Spoofing is used for the interception of synchrophasor data, in this work.

V. Conclusion

In this paper, a stealthy MITM attack on synchrophasor networks is analyzed and implemented on a laboratory-scale setup using various sub-networks. The attack presents the technical knowledge of the MITM attack based on MAC spoofing. MAC Spoofing results in the sniffing of packets within a network. In this process after the interception of communication, the attacker sends forged packets to the PDC with a higher transmission rate than PMU, which were received and analyzed, leaving PMU in a state of retransmission. This hijacking of the session is feasible if certain conditions are met while sniffing, forging, and sending packets.

The analysis of performed demonstration gives a broad picture regarding MITM attack, network elements, and targets in a synchrophasor network. It also shows the unreliability of the TCP layer alone in terms of the security of serial communication. The MITM attack scenario, being demonstrated on a commercial setup, highlights the potential threats lying in the synchrophasor network. It also promotes the research aspect towards the significance of continuous monitoring of traffic within the network. The defense strategies against the discussed attack may include static ARP-based solutions and an encryption-based multi-factor authentication technique. In addition, support of network security protocols can have a significant effect on the cyber-physical system security against MITM attacks.

Acknowledgment

This work was supported by the Science and Engineering Research Board under the project SERB /EE /2019547 and Indo-US collaborative project UI-ASSIST.

References

[1] *"IEEE Standard for Synchrophasors for Power Systems," in IEEE Std C37.118-2005 (Revision of IEEE Std 1344-1995) , vol., no., pp.1-65, 22 March 2006, doi: 10.1109/IEEESTD.2006.99376.*

[2] Hadjidemetriou, Lenos, et al. ”Demonstration of man in the middle attack on a feeder power factor correction unit.” 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). IEEE, 2020.

[3] C. Tu, X. He, X. Liu and P. Li, "Cyber-Attacks in PMU-Based Power Network and Countermeasures," in *IEEE Access*, vol. 6, pp. 65594-65603, 2018, doi: 10.1109/ACCESS.2018.2878436.

[4] Khan, Rafiullah & Maynard, Peter & Mclaughlin, Kieran & Laverty, David & Sezer, Sakir. (2016). Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. 10.14236/ewic/ICS2016.7.

[5] H. Zhang, B. Liu and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," in *IEEE Access*, vol. 9, pp. 29641-29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[6] D. Wei, Y. Lu, M. Jafari, P. M. Skare and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," in *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782-795, Dec. 2011, doi: 10.1109/TSG.2011.2159999.

[7] R. Khan, K. McLaughlin, J. H. D. Laverty, H. David and S. Sezer, "Demonstrating Cyber-Physical Attacks and Defense for Synchrophasor Technology in Smart Grid," 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018, pp. 1-10, doi: 10.1109/PST.2018.8514197.

[8] Giraldo, J., Cardenas, A. and Quijano, N., Integrity attacks on real-time ´ pricing in smart grids: impact and countermeasures. IEEE Transactions on Smart Grid, 8(5), pp.2249-2257, 2016.

[9] X. Fu, G. Chen and D. Yang, "Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems," in *IEEE Access*, vol. 8, pp. 103285-103290, 2020, doi: 10.1109/ACCESS.2020.2999585.

[10] W. Gao et al., "ARP Poisoning Prevention in Internet of Things," 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 2018, pp. 733-736, doi: 10.1109/ITME.2018.00166.

[11] Sanders, C., Practical packet analysis: Using Wireshark to solve realworld network problems. No Starch Press, 2017.

[12] Trachian, P., Machine learning and windowed subsecond event detection on PMU data via Hadoop and the openPDC. In IEEE PES General Meeting (pp. 1-5). IEEE, July, 2010.

[13] Case, D.U., Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 2016.

[14] Banu, Sabitha. (2019). A Survey of Computational Intelligence Methods used in handling Man in the Middle Attacks in Machine to Machine Communications..

[15] Farooq SM, Hussain SMS, Kiran S, Ustun TS. Certificate Based Authentication Mechanism for PMU Communication Networks Based on IEC 61850-90-5. Electronics. 2018; 7(12):370. https://doi.org/10.3390/electronics7120370

[16] V. Rohatgi and S. Goyal, "A Detailed Survey for Detection and Mitigation Techniques against ARP Spoofing," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 352-356, doi: 10.1109/I-SMAC49090.2020.9243604.

[17] Bansal, S., & Bansal, N. (2015). Scapy–A Python Tool For Security Testing. *Journal of Computer Science & Systems Biology, 8*, 140-159.