Comprehensive Demonstration of Man-in-the-Middle Attack in PDC and PMU Network

Kamakshi Prashadini Swain [a], Amit Tiwari [a], Ankush Sharma [a], Saikat Chakrabarti [a], Amey Karkare [b]
[a]*Department of Electrical Engineering*
[b]*Department of Computer Science & Engineering*
Indian Institute of Technology Kanpur, India
Email: kamakshi@iitk.ac.in, amittw@iitk.ac.in, ansharma@iitk.ac.in, saikatc@iitk.ac.in, karkare@iitk.ac.in

***Abstract*—The modernization of power systems has facilitated better communication infrastructure but raised concerns regarding privacy and security of the transmitted data. This paper demonstrates a comprehensive man-in-the-middle (MITM) attack in a synchrophasor network. The stealth of the MITM attack is presented in this paper, and it shows how the adversary's presence remains undetected in the network. The intercepted communication between the phasor measurement unit (PMU) and phasor data concentrator (PDC) is examined. PDC analyzes the spoofed data without setting any alarms to network operators, thus affecting the power system automation. An experimental implementation of the MITM attack is carried out in a laboratory-scale setup, using commercial PMUs, PDC, and various routers to demonstrate the stealth and effectiveness of the attack.**

***Index Terms*—Cyber attack, MITM attack, network security, smart grid, stealthy attack**

I. Introduction

The transition of traditional power systems towards smart grids aims for the system's progression by improving the reliability, resiliency, and robustness of the grid operation. However, with the development of improved and flexible power system operations, the complexity in terms of security has increased. One such significant challenge to smart grid function is cyber security. Recently known cyber attacks on power systems have revealed the attack's risk, scale, and impact. Stuxnet [1], the cyber-attack against Ukraine's power grid had a massive effect on the end-users. Smart grid is mainly dependent on intelligent electronics devices (IED), flexible communications infrastructures, distributed control centers, and metering infrastructure for information/ signal exchange.

Broadly, the power system functions in a three-layer hierarchy: corporate, control center, and substation [2]. At the corporate level, vital functions of both operational management and business management are performed. These include planning, accounting, and asset management. Operations at the control center include monitoring, forecasting, system analysis, logging, raising fault/ alarm flags, and emergency operation. The Control center also administers the information exchange between the national load dispatch center (NLDC) and regional load dispatch center (RLDC). At the substation level, various functions are managed by sending control signals to the field devices and executing commands issued by the control center. This is achieved by the data exchange between the remote terminal units (RTUs) and IEDs. PMUs and PDCs are also utilized for collecting data to/ from the control center at a very fast rate, i.e., every 20ms for 50Hz system. This resulted in the inception of power system automation, which integrates one or more control centers, with each control center supervising various substations. In control centers, synchrophasor technology may be used for continuous and fast measurement, monitoring, and control of the power system.

A synchrophasor network includes PMUs, local PDCs, central PDC, and routers. The deployment of PMUs has improved grid management. However, delayed, missing, and malicious measurements from PMUs in a closed-loop application may lead to the maloperation of power system control signals. Concerns about the dependability and security of communication networks will affect the secure operation of the synchrophasor network [3]. Cyber-attacks are classified based on which security objective is compromised. The smart grid can be vulnerable in three aspects:

- Communication vulnerability: The supervisory control and data acquisition (SCADA) system and the synchrophasor network are generally the main target of cyber-attacks on the communication side. The use of a variety of communication protocols to connect the utility operation centers with system operation makes the smart grid vulnerable to attack.
- Hardware vulnerability: The remote-controlled devices deployed with substation devices, such as circuit breakers and measurement devices, make the system vulnerable to attacks.
- Software vulnerability: Applications and programs installed on utility computers and control centers are prone to cyber-attacks.

Power system operators have dedicated communication

links between the corporate and control centers. Local area network (LAN) and internet protocol (IP)-based communication protocols are usually implemented in the communication links of the power system. The complex communication network exposes the power system to inherent vulnerabilities of these telecom protocols. It makes the system susceptible to various cyber-attacks, such as denial of service attacks, IP spoofing, MITM attacks, etc. The most common class of cyber attacks on the smart grid is the MITM attack [5]. As per author's knowledege a comprehensive demonstration of MITM attack is not presented in context of power system automation.

The impact of the MITM attack is demonstrated on the reactive power compensation unit in [4]. Various surveys have classified and categorized the cyber-physical attacks in power systems [6]. Cyber vulnerabilities in smart grids are primarily associated with the networking and communication infrastructure [7], [8]. The attack scenario on a maritime surface vessel's automatic identification system (AIS) is discussed in [9]. The attacker intercepts the AIS communication and tampers with the online tracking system. An adversary can also target the smart home automation system using a MITM attack. Reference [10] presents interception of MITM attacks in IEEE 802.15.4 network. Researchers in [11], [12] presented that MITM attack in smart TV can redirect unauthenticated HTTP requests to malicious websites, thereby gaining access to the smart TV. Various studies have presented cause-effect scenario for MITM attack, however a comprehensive demonstration of MITM attack in synchrophasor network is not discussed in literature.

The objective of this study with MITM attack demonstration is two-folds. Firstly, the underlying vulnerability of the synchrophasor network is analyzed, which is then exploited to implement the MITM attack. Secondly, an offensive and defensive viewpoint is analysed and discussed briefly for the vulnerable smart grid network. This paper presents a systematic demonstration of the real setup to characterize the magnitude of the MITM attack on the synchrophasor network. The systematized and comprehensive elements of the offensive MITM framework introduces the purpose and flow of MITM attack. The attack framework is designed based on the threat actors, network gateways, and target. Networks are sperated by each other with incorporation of differnet routers. In contrast to the theoretical studies in the literature, this work is implemented on actual devices in a laboratory setup. The exact structure of the synchrophasor network presents the efficacy of the MITM attack.

The rest of the paper is organized as follows. MITM attack progression and its implementation are discussed in Section II. Section III presents the real-world cyber-attack use case towards the MITM attack, followed by a discussion on the intercepted traffic. Section IV concludes the paper.

II. MITM Attack

MITM attack can be perceived as active eavesdropping in which the adversary intercepts the communication between the client and server and transmits forged/ manipulated information between them. In an MITM attack, the adversary exploits the server by sending a certificate with a public key to the client. The authentication of this certificate makes the entire communication path vulnerable to cyber-attack. The inherent weakness of communication protocols and distributed PMUs are considered to demonstrate the MITM attack framework. The attack scenario shows a man/ attacker between the PMU and PDC communication and how the session is intercepted in a synchrophasor network without raising alarms.

The experimental setup consists of two Core i7-7700 CPUs and 3.6 GHz desktops to serve as client and server. Three different routes were utilized to represent the change in the network. The communication of the PDC and PMUs is performed through a local area network (LAN). A client-server configuration between PDC and PMU is transmitted via TCP protocol. PMU from two different makers, SEL and Arbiter, was considered for the experimental setup. OpenPDC accounted for the processing of high-speed time series data [14]. The laboratory setup consists of additional software, Wireshark [13] and command line interface (CLI) programming in Python. Wireshark is used to capture network traffic. The offensive MITM attack framework executes in two phases: attack propagation and implementation.

A. MITM Attack Progression

The first crucial step is to sniff data transmission traffic between PMU and PDC by the attacker's network. This framework uses an active approach to intercept the traffic using address resolution protocol (ARP) spoofing. In ARP spoofing, the attacker system's media access control (MAC) address is mapped with the PDC's network router. The spoofing will result in the diversion of traffic towards the attacker's system. In this work, ARP spoofing was implemented using Ettercap.

When PMU and PDC communicate, the PDC sends an acknowledgment in response to every packet sent by PMU in the transmission stream. The acknowledgment consists of two values, namely, the "Acknowledgement number and Sequence number." This management of sequence is inherited in TCP protocol. The attacker system utilizes these parameters to break the authentication cycle between the PMU and intended PDC.

The attacker can access the acknowledgment and sequence number, exchanged between the PMU and PDC by sniffing the traffic using Wireshark. An essential step towards hijacking the communication session by the attacker relies on the acceptance of forged authentication keys by PMU and PDC during a TCP handshake. When observing the synchrophasor network traffic, this setup appears to be a secure connection. However, in reality, the attacker controls the entire session.

B. MITM Attack Implementation

The threat model of the work is built upon the assumption that the attacker has access to the substation network and IP address of the PDC. The implemented scenario is presented

in Fig. 1, in which PMUs and PDC are located at separate networks, with router A and B, respectively.

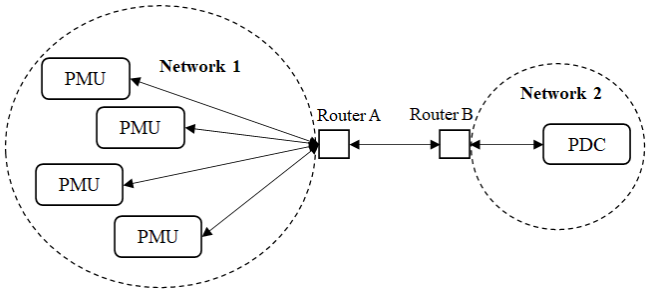

Fig. 1. Communication flow in synchrophasor network with differnt routers

In the threat model, routing entry of the PDC was again entered with the attacker system's IP address. With this redirect, the data packets intended for PDC will reach attacker's system too. This is achieved by internet control message protocol (ICMP) redirect message. After sending forged ICMP redirects, attacker' IP is now registered with PDC'S MAC address. The schematic of ICMP redirect is presented in Fig. 2.

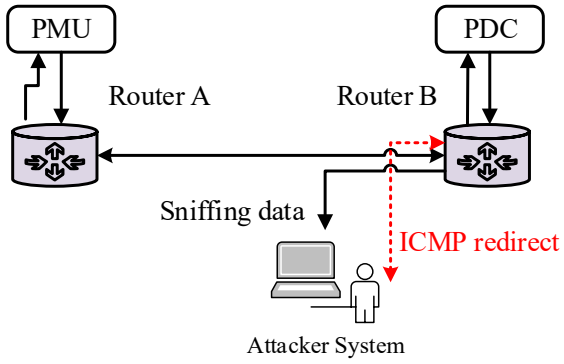

Fig. 2. ICMP redirect message routing towards attacker's system

The routers on the data link layer use ICMP redirect messages to broadcast the host (PDC in this case) regarding a better route for packets to reach the intended destination port. With this process, the incoming and outgoing traffic of the PDC routes through the attacker's system. Fig. 3 gives the snapshot of captured traffic while redirecting the route to the attacker's system.

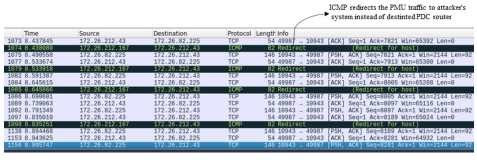

Fig. 3. ICMP redirect message routing towards attacker's system

The successful MITM attack depends on the timely enabling/ disabling of IP forwarding and ARP spoofing during an entire session. IP forwarding is the process by which a packet is routed using a specified path. This process uses routing information to select the path to send a packet over multiple networks. In the presented framework for the MITM attack, IP forwarding is used to intercept the data traffic intended for the PDC and with ARP poisoning of routing table, the traffic is redirected to the attacker's IP address. The packet header contains the destination address, which is altered during IP forwarding. When IP forwarding is disabled, the session between PMU and PDC is terminated and hijacked by the attacker.

The forged packets must be fabricated such that the PDC should accept them. This was achieved by extracting information from the last transmitted packet from the PMU to the PDC. Information regarding the transmitted packet is extracted prior to IP forwarding disable. The information contained in the captured packet is packet length, port number, TCP header information, and raw paylaod. The captured packet from the PMU from an attacker's perspective to attempt MITM attack is shown in Fig. 4.

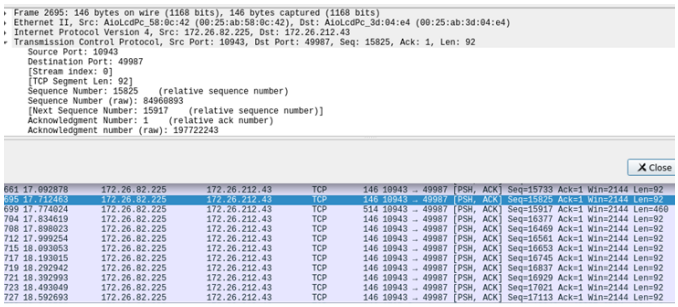

Fig. 4. Packet captured in Wireshark to sniff the sequence number

With the extracted information from the last packet, the attacker's system creates a sequence of forged packets.

The actual data packets had the flags PSH and ACK. An additional flag is added to the forged packet, namely, the urgent flag, URG, to differentiate the forged data packets from the actual packets. The forged packets are transmitted to the PDC by enabling IP forwarding. At this instance, PMU will connect with PDC by sending out a packet with correct header information. The forged packets are formed in such a manner that they will not require acknowledgment from PDC after transmitting each packet. This objective was achieved by incrementing the sequence number of the successive packet, which implies that the packets are acknowledged by the PDC. In this manner, a successful session of the forged packets is transmitted to the PDC as shown in Fig. 5. However, during this period, the packets from PMU undergo retransmission, as shown in Fig. 6.

The schematic of the actual synchrophasor network setup for the MITM attack demonstration is shown in Fig. 7. The extracted information is transmitted to attacker alias in other sub-network where packets are forged and then sent to PDC.

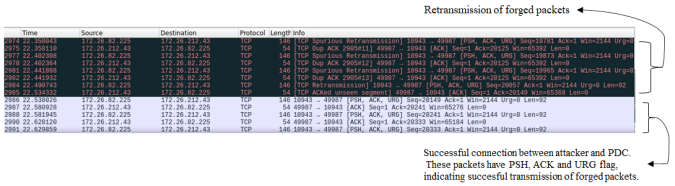

Fig. 5. Successful transmission of forged packets between attacker and PDC, indicating successful attempt to MITM attack

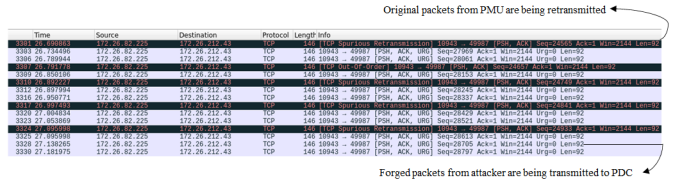

Fig. 6. Retransmission of actual packets from PMU to PDC, indicating that the attacker has disabled the healthy data transmission of PDC-PMU

This ensures the headers of forged packets are identical to PMU's packet at data link layer. The stealth of the MITM attack can be measured from this demonstration. The presence of the attacker remains undetected, and meanwhile, the adversary may spoof target information.

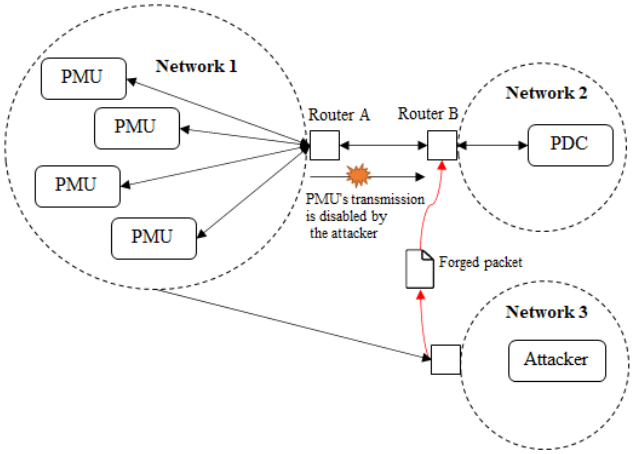

Fig. 7. Setup for MITM attack when attacker is outside the synchrophasor's network

III. Results and Discussion

The power system components can be classified into power applications and supporting infrastructure, in which the supporting infrastructure relies mainly on the communication network. Synchrophasor network is one such support system that is critical for power system monitoring. MITM can be implemented using various techniques. The most common procedures are ARP poisoning, domain name system (DNS) spoofing, ICMP redirection, dynamic host configuration protocol (DHCP) spoofing, and SSL hijacking. This section analyzes the communication scenario with the legitimate user and with the attacker in the middle.

The attack scenario is analyzed as two cases; (i) communication flow between the PMU and PDC and (ii) between attacker and PDC.

A. Communication flow between the PMU and PDC

In this case, the communication between PMU and PDC is not disturbed. The attacker passively sniffs the traffic and gathers information regarding the system, network gateways, and details about the data packet. A snapshot of such a packet is shown in Fig. 8.

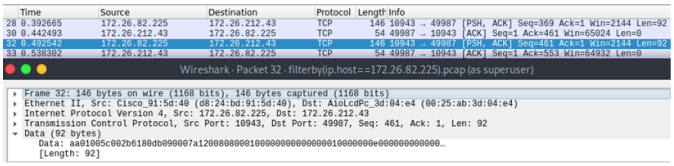

Fig. 8. Actual packets from PMU to PDC

B. Communication flow between the attacker and PDC

In this case, the attacker intercepts the communication between the PMU and PDC using the methodology explained in Section II. With successful packet extraction, forged packets are fabricated such that the PDC cannot differentiate between the actual and forged data packets. Successful transmission of the developed forged data packet is shown in Fig. 9.

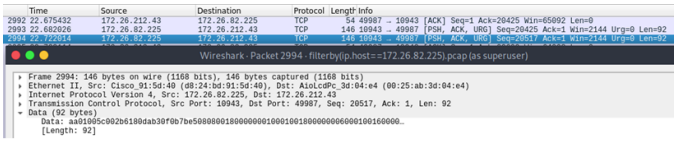

Fig. 9. Forged data packets from attacker to PDC

In this case, the ICMP redirection transmits the attacker's IP address as the next possible path, and hence, the packet traffic is directed to the attacker's IP address. Depending on the stealth of the attacker, the broadcasted IP address can have random values so that the attacker is in incognito mode. The connection between the PMU and PDC is controlled by IP forwarding. PMU tries to establish a connection with PDC in each session, but the attacker's packets are fabricated to surpass the legitimate PMU's connection time. Thus, the attacker successfully establishes the connection unless the PDC ends the link from its end.

Current research has tried to improve the detection and mitigation techniques of MITM attacks. Some of the primary defense mechanism for various categories of MITM attack is presented in Table I.

Protection of synchrophasor networks against cyber-attacks can have an offensive and defensive mechanism. Proper configuration of a cyber asset may reduce the vulnerabilities level; in some cases, a regulatory body can also enforce some guidelines to reduce the vulnerabilities associated with the

TABLE I
DEFENSE MECHANSIM FOR MITM ATTACK

Attack Technique	Description	Defense Mechanism
ARP Spoofing	Attacker modifies ARP table and alter mapping of host's MAC address with target IP	Cryptography based solution
DNS Spoofing	Attacker modifies the cache position and redirect legitimate traffic	Cryptography based solution
IP Spoofing	Attacker creates IP packets with modified source address to hide identification to impersonate target system	Router/ switches based solution, Migration from IPv4 to IPv6 will facilitate end-to-end transparency.

device. The potential attacks on communication links can be reduced by identifying the dependencies of cyber assets and critical systems in the control center.

Offensive Viewpoint

Concerns from the domain industry have already been raised about the potential MITM attack and its impact on the communication infrastructure of power systems. MITM attack can be accomplished using various techniques. One such technique, using ARP poisoning and ICMP redirect, is discussed in this work. Anyone, who has gained access to the network information and transmitted packets, can implement this attack. There are several tools available for performing an effective MITM attack for both windows and Linux environments. For this purpose, the defensive mechanism incorporated must be robust.

Defensive Viewpoint

The best defense is a good offense. This adage can also be applied to cyber-physical security in power systems. Unless the system operator is well versed with the vulnerable operation of cyber assets, no defense approach can work effectively. In this paper, the vulnerability of the synchrophasor network is exploited to implement a MITM attack. The network can be made robust against ARP poisoning by assimilating the router's firewall and MAC binding features of switches.

To summarize, defense mechanism discussed here cannot exclusively provide security against MITM attacks, considering complexity of attack. However, the inclusion of cryptography-based authentication techniques can maximize the chance of preventing MITM attacks in practice. Considering the disseminated nature of this vulnerability as presented in this paper, effective mitigation techniques are the need of the hour.

IV. CONCLUSION

In this paper, an MITM attack in a synchrophasor network is implemented and demonstrated in a laboratory setup using various routers and different network settings to signify the change in the network. The attack aims to hijack the actual communication between the PDC and PMU. In this process of interception of communication, the attacker sends malicious packets to the PDC instead of the actual packets. It has been observed that the PDC cannot differentiate between the data packets coming from the PMU and those coming from the attacker. PDC processes all the packets without raising any alarm to the system operators. The comprehensive demonstration of the attack gives a broad picture regarding various threat actors, network elements, and targets in a synchrophasor network.

The MITM attack scenario, being demonstrated on commercial setup, highlights the potential vulnerabilities in the present communication and cyber assets in the control center. It also promotes the research aspect towards the significance of implementing defensive techniques. The defense strategies against the discussed attack may include an authentication-based handshake initiation in addition to a cryptography-based multi-factor authentication technique. Moreover, 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] Case, D.U., Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 2016.
[2] Wei, D., Lu, Y., Jafari, M., Skare, P.M. and Rohde, K., Protecting smart grid automation systems against cyberattacks. IEEE Transactions on Smart Grid, 2(4), pp.782-795, 2011.
[3] Zhong, X., Jayawardene, I., Venayagamoorthy, G.K. and Brooks, R., Denial of service attack on tie-line bias control in a power system with PV plant. IEEE Transactions on Emerging Topics in Computational Intelligence, 1(5), pp.375-390, 2017.
[4] 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.
[5] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J., A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), pp.3453-3495, 2018.
[6] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," IET Cyber Phys. Syst. Theory Appl., vol. 1, no. 1, pp. 13–27, Dec. 2016.
[7] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.
[8] Stephens, J.C., Wilson, E.J. and Peterson, T.R., Smart grid (R) evolution. Cambridge University Press, 2015.
[9] Giraldo, J., Cárdenas, 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.
[10] Lomas, N., Critical flaw identified in zigbee smart home devices, 2015.
[11] W. Candid. How My TV Got Infected With Ransomware and What You Can Learn From It. [Online]. Available: https://www.symantec.com/connect/blogs/how-my-tv-got-infectedransomware- and-what-you-can-learn-it, 2015.
[12] D. Fisher. What's on TV Tonight? Ransomware. [Online]. Available: https://www.onthewire.io/whats-on-tv-tonight-ransomware/ , 2016.
[13] Sanders, C., Practical packet analysis: Using Wireshark to solve real-world network problems. No Starch Press, 2017.
[14] 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.