Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 4, 1298-1303

ARP Spoofing-Based MITM Attack in Data Link Layer Using the Hybrid Method- CONVLSTM-ECC

JapneetKaur[1], PreetiSondhi[2]

[1]Research Scholar, M.Tech. (CSE), Universal Institute of Engineering & Technology, Lalru
[2] Assistant Professor, Universal Institute of Engineering & Technology, Lalru
[1]japneetkaurbal@gmail.com, [2]preetisondhi4@gmail.com

Abstract

The ARP protocol is used to determine the MAC Address of a device whose IP address is known. When a device wants to interact with another device on the network, it uses ARP to determine the MAC Address of the device with which it wishes to communicate. The ARP poisoning or ARP spoofing technique is used in the MITM attack. This is accomplished by taking advantage of two security flaws. The first is that each ARP request or response is regarded as legitimate. Simply inform any device on your network that you are the router, and the device will trust you. The simulated data is displayed as a trace graph, which contains the communication records. The trace graph's standard trace format contains 54 features that display all of the packet communication's details. The ConvLSTM model can utilize the data once it has been pre-processed since it removes the unneeded data. The Convolutional LSTM (ConvLSTM) model is an extended form of the LSTM (Long Short-Term Memory) model, which is itself an enhanced version of RNN (Recurrent Neural Network). The proposed the Hybrid ConvLSTM-ECC method, which uses convolutional layers for feature extraction from raw data to detect the Data Link layer's ARP Spoofing-based MITM attack nodes in a wired and wireless context. The output is given into the LSTM model, which predicts detection accuracy and mitigates ARP Spoofing-based MITM attacks by producing signatures for node authentication using the data.

Keywords— ARP, Spoofing, MITM, Attack, Data Link, Layer, Hybrid, Etc

1. INTRODUCTION

In a network, computers communicate with other devices using their IP addresses, but in practise, the communication is done using their MAC addresses. The ARP convention is utilized to decide the MAC Address of a gadget whose IP address is known. When a device wants to interact with another device on the network, it uses ARP to determine the MAC Address of the device with which it wishes to communicate. The MAC address is found via ARP in two steps:

- ✓ The sender device sends an ARP Request with the IP address of the device with which it wishes to communicate. This request is broadcast, which means that it will be received by all devices on the network, but only the device with the designated IP address will answer.
- ✓ After receiving the broadcast message, the device with the same IP address as the message sends an ARP Response to the sender containing its MAC address.

ARP spoofing is a Man in the Middle (MITM) assault in which a programmer sends adulterated ARP messages. Since it ties the aggressor machine's MAC Address to the genuine IP Address, it allows the attacker to

pose as a valid user. The attacker will now get communications meant for the legitimate IP Address once the MAC Address has been connected. ARP Spoofing also allows the attacker to intercept, change, and discard incoming messages. ARP spoofing is only possible on IPv4 addresses with 32 bits, not IPv6 addresses. However, because most of the internet still uses IPv4, it is frequently utilised.

1.1 ARP Spoofing Man in the Middle Attack (MITM)

One of the most unsafe and effective assaults in an organization is a man-in-the-center (MITM) assault. It can only be done once you've established a network connection. It can be used to redirect packet traffic from any client to your device. This implies that each packet transmitted to or from the client will have to transit via your device, and you'll be able to read those packets because you know the network's password and key. Because it's so difficult to defend against, this attack is extremely effective. The ARP poisoning or ARP spoofing technique is used in the MITM attack. This is accomplished by taking advantage of two security flaws. The first is that each ARP request or response is regarded as legitimate. Simply inform any device on your network that you are the router, and the device will trust you. The second security concern is that clients can receive replies even if they did not initiate the request. The Address Resolution Protocol (ARP) is an organization correspondence convention that permits network interchanges to arrive at a particular organization gadget. ARP changes over Internet Protocol (IP) locations to Media Access Control (MAC) addresses and the opposite way around. ARP is generally commonly utilized by gadgets to speak with the switch or entryway that permits them to interface with the Internet. Has keep an ARP store, which is a table that maps IP locations to MAC addresses, and use it to associate with network objections. On the off chance that a host doesn't have the foggiest idea about the MAC address for a given IP address, it conveys an ARP demand parcel, which asks different machines on the organization for the MAC address.

2. REVIEW OF THE LITERATURE

PrernaArote and K. V. Arya (2015) Poisoning the Address Resolution Protocol (ARP) is the beginning stage for modern LAN attacks, for example, disavowal of-administration (DOS) and Man-In-The-Middle (MITM) (MITM). The way that ARP is stateless has a direct impact on network security standards, particularly Ethernet security. The proposed detection mechanism starts with the Central Server sniffing network traffic (CS). Then CS sends a trap ICMP ping packet, analyses the answer for ICMP replies, and successfully finds the attacker. A voting procedure is utilised to elect legitimate CS to forestall ARP harming over a unified framework. CS successfully forestalls ARP harming while at the same time keeping up with framework speed by approving and adjusting IP, MAC > pair passages staying in has store tables. Our strategy depends on the ICMP convention. To recognize and forestall MITM based ARP harming, a democratic procedure with in reverse similarity, minimal expense, low traffic, and simplicity of arrangement is presented.

Min Song, Jaedong Lee, Young-SikJeong, Hwa-Young Jeong, Jong Park (2014) Despite its benefits, pervasive figuring is defenseless against an assortment of goes after and security issues. To build enhanced and safer universal conditions, security worries in the pervasive organization are required. The location goal convention (ARP) is a convention for deciding the IP address of an organization card and its actual location. ARP is intended to work in a wide range of situations. However, because it is designed without security protections against malicious assaults, an attacker can use ARP spoofing to impersonate another host or obtain access to sensitive information. In this research, we offer a new routing trace-based detection scheme for ARP spoofing attacks that can be

utilised to secure the internal network. The change of network movement path can be found by tracing routing. Because the suggested solution does not change the ARP protocol, it ensures excellent consistency and compatibility. It is also basic and stable, as it doesn't utilize an intricate calculation or put extra strain on the PC framework.

AbhishekSamvedi, SparshOwlak, and V.K. Chaurasiya (2014) an enhanced secure address resolution system is provided in this study, which prevents ARP spoofing attacks. The proposed attack is a centralised approach to combating ARP spoofing attacks. In the suggested concept, an ARP spoofing attack is prevented by a central server on a network or subnet.

S. Venkataramulu and ChakuntaRao (2013) Most networks prioritise security, and many businesses carry out an extensive security strategy that traverses a considerable lot of the OSI levels, from the application layer to IP security. Nonetheless, one region that is some of the time disregarded is Layer 2 solidifying, which can leave the organization helpless against various attacks and splits the difference. The planning of an IP address to a MAC address is known as the location goal convention (layer 3 to layer2 planning). Since ARP doesn't give a verification system to inbound solicitation parcels, any client can fake an ARP message containing vindictive data to harm the objective host's ARP reserve. Man-in-the-center (MITM), Denial of administration (DOS), cloning assault, meeting commandeering, and numerous other assaults are all feasible on ARP and can make communication insecure.

3. OBJECTIVES

- To examine ARP Spoofing Man in the Middle Attack (MITM).
- To evaluate the hybrid modelDetection Accuracy Ratio and Average Delay perform.

4. RESEARCH METHODOLOGY

4.1 Proposed Hybrid ConvLSTM-ECC Method

In both wired and wireless networks, a connection is created between the nodes, and traffic is generated. ECC cryptography is a good asymmetric cryptography for data security since it can be used for encryption and decryption. The signature in the packets is an encrypted identity associated with the nodes. The simulated network traffic data is obtained using a trace graph and a time series. Every trace record is represented by a line in the trace graph. The trace record followed the above-mentioned established structures, and it contained 54 features about the communication details.

✓ **The Protocol Methodology**

A simulator is used to evaluate the proposed method. Normal and multicast routing strategies are used to set up wired and wireless networks. The animator is used to visualize the communication. The suggested research looks into the specifics of the packets that are sent between the nodes. In the simulator, the link layer component is responsible for simulating data connection protocols. Though ARP MITM attacks attempt to change the MAC address and IP address pairing of the ARP cache table placed in the Data Link layer, the suggested hybrid method is used in the Data Link layer for the detection of ARP Spoofing based MITM attacks.

✓ **Pre-processing and data collection:**

The simulated data is displayed as a trace graph, which contains the communication records. The trace graph's standard trace format contains 54 features that display all of the packet communication's details. The ConvLSTM model can utilise the data once it has been pre-processed since it removes the unneeded data.

✓ **Convolutional LSTM (ConvLSTM):**

The Convolutional LSTM (ConvLSTM) model is an extended form of the LSTM (Long Short-Term Memory) model, which is itself an enhanced version of RNN (Recurrent Neural Network). RNNs retain a lot of prior knowledge for a short period of time, making training more difficult for particular applications. Furthermore, RNN does not

simulate long-term dependencies, which led to the development of LSTM. By substituting memory cells for the hidden layers of RNNs, LSTMs may learn long-term dependencies, overcoming RNN's limits.

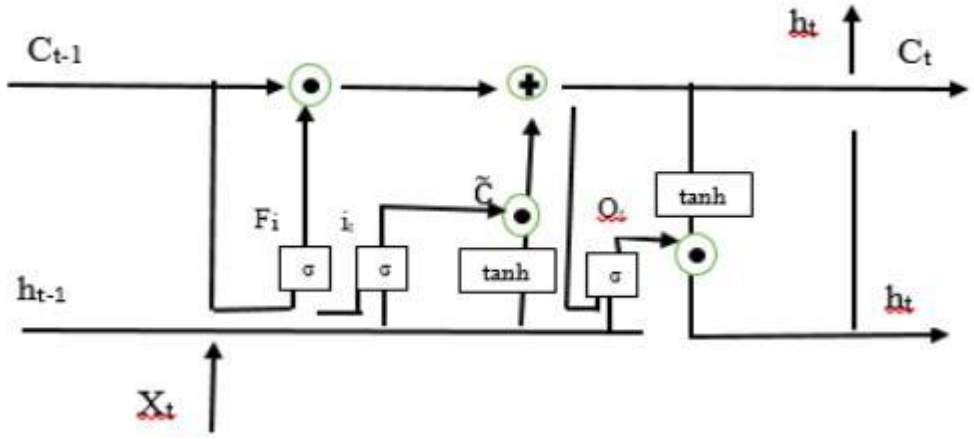

Figure 1: Architecture of ConvLSTM

5. RESULT AND DISCUSSION

A simulated environment is used to test the hybrid model. The ns2 simulator is employed. ns2 is a free open-source tool for designing and simulating several types of networks, including WANET, MANET, and others. The suggested hybrid method outperformed the current GMRARP-AES-RSA methods in terms of detection accuracy. Several publications have utilised different ways to identify and mitigate ARP Spoofing-based MITM attacks.

5.1 Detection Accuracy Ratio

The proportion of True Positive cases to complete positive examples is the Detection Accuracy. Figure 2 depicts the detection ratio results, with values listed in Table 1.

$$DR = \frac{TP}{\mathrm{TP} + \mathrm{FN}}$$

Table 1 Accuracy Detection values

GMRARP-AES-RSA	ConvLSTM-ECC
91	**97**

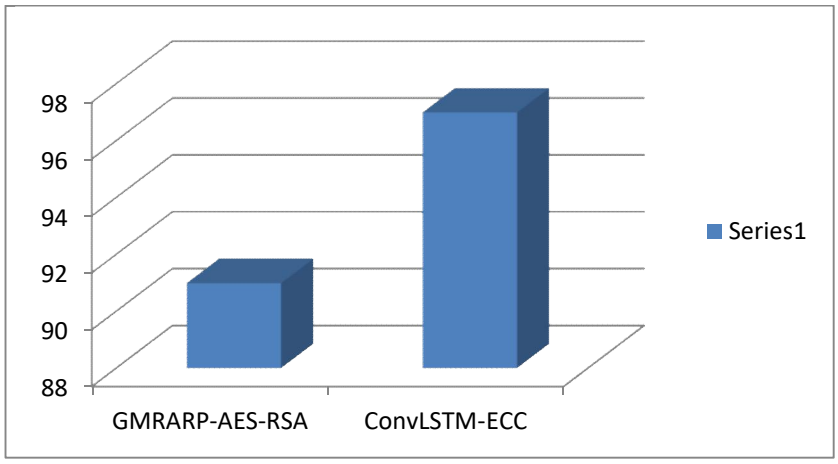

Figure 2: Accuracy Detection Ratios

5.2 Average Delay

The time it takes for packets to arrive at their destination is known as average delay. Furthermore, finding routes and queuing packets for transmission takes time. As a result, it only counts packets that make it to their intended destination. It demonstrates increased performance when the average delay results are minimal. Figure 3 depicts the average delay for the various models. Figure 3 plots the simulated results for ConvLSTM-ECC from 0.000s to 15.000s simulation time, while Table 2 lists the data.

$$Average\ Delay = \frac{\text{Total number of arriving time} - \text{Total number of sending time}}{\text{Total number of Packets}}$$

Table 2 Average Delay values

Existing: GMRARP AES-RSA (bps)	Proposed: ConvLSTM- ECC (bps)
55	31
57	33
80	76
103	97
120	103
143	125
168	161

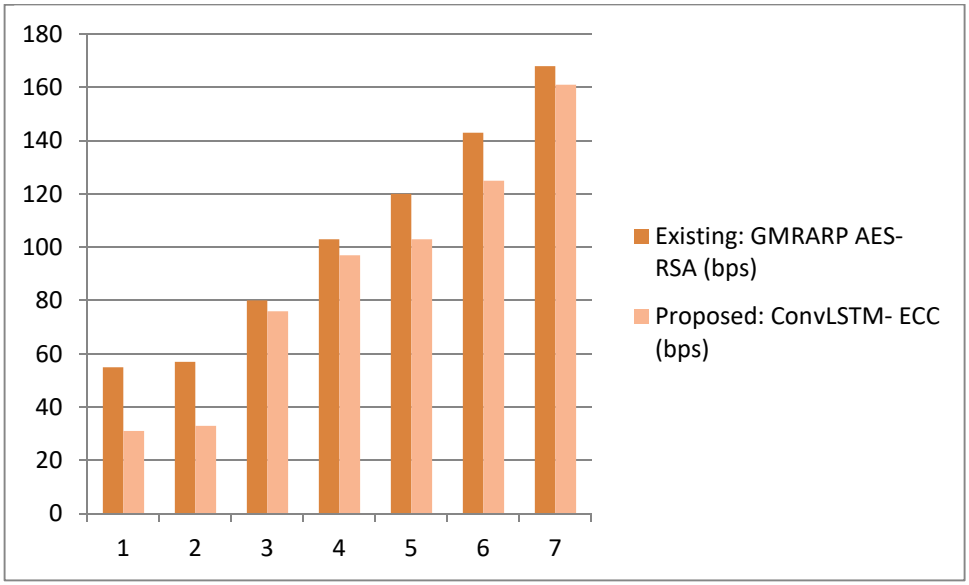

Figure 3: Average Delay

The proposed hybrid ConvLSTM-ECC method employs Convolutional Long Short-Term Memory (LSTM) to predict the detection of ARP Spoofed nodes in the wireless network based on the characteristics of the ARP MITM attack, and then employs Elliptical Curve Cryptography (ECC) to mitigate the nodes by providing authentication between them.

6. CONCLUSION

The suggested hybrid method improves detection accuracy while reducing calculation time without sacrificing service quality, and it outperforms the current method. MITM Resistant Address Resolution Protocol-Advanced Encryption Standard-Rivest Shamir Algorithm-Generalized MITM Resistant Address Resolution Protocol-Advanced

Encryption Standard -Rivest Shamir Algorithm (GMRARP-AESRSA). The packet header has been tampered with in order to launch ARP Spoofing-based MITM attacks. The network traffic is generated between the nodes through gateways in a wired and wireless network setup. The proposed the Hybrid ConvLSTM-ECC method, which uses convolutional layers for feature extraction from raw data to detect the Data Link layer's ARP Spoofing-based MITM attack nodes in a wired and wireless context. The output is given into the LSTM model, which predicts detection accuracy and mitigates ARP Spoofing-based MITM attacks by producing signatures for node authentication using the data.

REFERENCES

1. Arote, Prerna&Arya, K. V. (2015). Detection and Prevention of ARP Poisoning Attack using Modified ICMP and Voting. 10.1109/CINE.2015.34.
2. Song, Min & Lee, Jaedong&Jeong, Young-Sik&Jeong, Hwa-Young & Park, Jong. (2014). DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments. TheScientificWorldJournal. 2014. 264654. 10.1155/2014/264654.
3. Samvedi, Abhishek&Owlak, Sparsh&Chaurasiya, V.K.. (2014). Improved Secure Address Resolution Protocol. Computer Science & Information Technology. 4. 10.5121/csit.2014.4521.
4. Venkataramulu, S. &Rao, Chakunta. (2013). Various Solutions for Address Resolution Protocol Spoofing Attacks. International Journal of Scientific and Research Publications (IJSRP). 3. 1-12.
5. Kun wang, Miao Du, Yanfei Sun, Alexey, and Yan Zhang .Attack detection and Distributed Forensics in Machine-to-Networks, IEEE Network, Nov/Dec 2016,pp:49-55
6. Kwang-Cheng Chena, Shao-Yu Liena. Machine-to-machine communications: Technologies and challenges, Elsevier,2014, Volume 18, pp:3-23.
7. Mauro Conti, Nicola Dragoni and Viktor Lesyk. A Survey of Man in the Middle Attacks, IEEE Communications Surveys and Tutorials, 2016, Vol.18, No.3,pp:2027-2051.
8. SeungYeob Nam, SirojiddinDjurarv,MinhoPark.Collaborative approach to mitigating ARP poisoning-based Man-in –the Middle attacks, Elsevier, Computer Networks, 2013,Pp:3866-3884.
9. J. Belenguer and C. T. Calafate.A low-cost embedded IDS to monitor and prevent man-in-the-middle attacks on wired LAN environments,in Proc. Int. Conf. Secure Ware Emerging Secur. Inf. Syst. Technol., 2007, pp. 122–127.
10. V. Ramachandran and S. Nandi.Detecting ARP spoofing: An active technique, Springer, 2005, pp. 239–250.