Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

A Survey of Computational Intelligence Methods used in handling Man in the Middle Attacks in Machine to Machine Communications

Sabitha Banu. A
Ph.D. Scholar
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India

G. Padmavathi
Professor
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India

***Abstract*—The increase of interconnected objects through Machine to Machine Communication (M2M) is unpredictable. The researchers have predicted that in forthcoming days, around fifty billion objects throughout the world will be connected with each other with the help of internetwork of smart objects. As the network grows the number of cyber threats is also increases. Among all cyber threats, MITM attack is one of the most and major threats in network security. Man-In-The-Middle (MITM) is an attack where an unknown third party captures the communication channel between two or more endpoints. The MITM attacker can intercept, alter, adjust, or replace target victims' communication traffic. Moreover, victims are not aware of the attacker or unknown third party, thus trusting that the communication channel is safe and protected. The MITM attack targets not only the actual information that flows between two or more endpoints , but also the privacy and reliability of the information itself. 95% of HTTPS are vulnerable to MITM attacks. In this paper taxonomy of MITM attack is discussed based on several parameters.**

Keywords*— *Machine to Machine Communications (M2M), MITM , ARP Spoofing , IP Spoofing, SSL/TLS Spoofing, DNS Spoofing, BGP Spoofing

I. INTRODUCTION

Machine-to-Machine (M2M) communications is an emerging communication paradigm that provides ubiquitous connectivity between devices along with an ability to communicate autonomously requiring no human intervention. It is often used for remote monitoring. M2M communications acts as an enabling technology for the practical realization of Internet-of-Things (IoT). The IoT is envisioned as `a global network of connected devices having identities and virtual personalities operating in smart spaces and using intelligent interfaces to communicate within social, environmental, and user contexts. This vision of IoT represents a future where billions of everyday objects and surrounding environments will be connected and managed through a range of communication networks and cloud-based servers.

Today, almost everyone's life is associated with the habit of using Internet or cellular networks. For example, using online home banking, online entertainment and shopping, social networks, etc. All these online services store get to know the entire user's sensitive information, which signifies a key target for attackers. Attackers target business enterprises and organizations, leading to big loss in terms of economy. In this new era "people and things always connected" with the help of the internet, it has become common to read about the attacks to connected things and online services. There are many numbers of cyber-attacks in machine to machine communications emerging in this real world which affects all kinds of businesses.

Machine to Machine Networks are likely to encounter several types of cyber-attacks and it is shown in the Fig 1as follows:

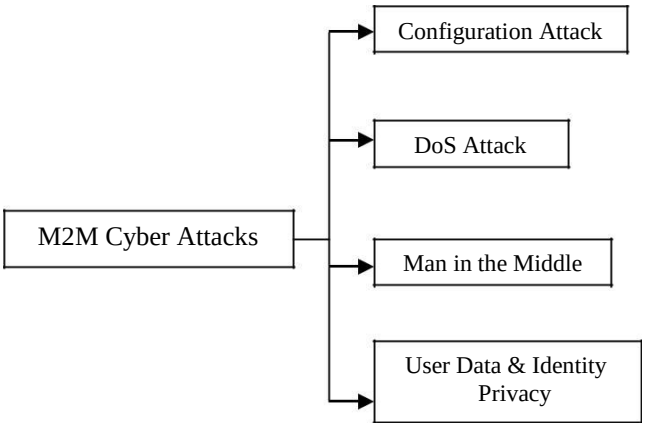

Fig 1. Cyber Attacks in Machine To Machine Communications

Among those most threatening attacks is Man-in-the-Middle (MITM), which gains control over end-users' sensitive information while transferring.

A. *MITM Risks*

Wired Networks: When a man-in-the-middle attack is conducted in a wired network it requires knowing how nodes on a network create a representation of the network, and how the nodes are spoofed. A MITM attack can be carried out in a wired network via ARP spoofing, DNS spoofing, IP spoofing, ICMP spoofing, DHCP spoofing.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

Wireless Networks: Essentially, everyone in the mobile enterprise is a potential target, but the most vulnerable are those in senior or executive positions in business and government.

Hackers are on the lookout for anyone who deals with sensitive information particularly those who might have access to trade secrets or financial data. Anyone who works in R&D or product development should also be cautious.

It's been estimated that nearly three quarters of the top 1,000 free apps in Google Play don't check server certificates, and nearly three quarters of those ignore any SSL errors that pop up when they communicate with the app server.

And before we start wagging fingers too vigorously at Android, Apple iOS devices seem to be just as MITM prone. A vulnerability discovered in April 2015 affected how approximately 1,500 iOS apps established their secure connections to servers. It meant that anyone intercepting data from an iPhone or iPad could access logins and other personal information transmitted via HTTPS.

B. *Contribution of the Paper*

We have provided a detailed survey in this paper about various types of cyber-attacks or threats encountered in machine to machine communications. Among those cyber threats Man in the Middle is considered as one of the major threats. Man in the Middle is categorized in to three based on several parameters which is impersonation, communication channel and location of the target. MITM based on the impersonation which is nothing but spoofing is divided into Spoofing, Man in the Browser spoofing, Border Gateway Protocol Spoofing, STP Mangling, Port Stealing.
Spoofing includes ARP, DNS, ICMP, IP, DHCP where researchers have studied some detection and prevention attack handling mechanisms of ARP and IP Spoofing are consolidated in this paper.

C. *Organization*

The remaining of the paper is structured as follows Section II defines MITM attack and three different MITM categories, namely based on nature of a communication channel, attacker's location in the network and impersonation techniques. Section III, IV and V focus on the different types spoofing based MITM attacks. Section VI reviews few prevention and detection attack handling mechanisms suggested by authors. Section VII gives few Mitigation strategies so that we can prevent our device from different MITM attacks. Section VIII defines some machine to machine communication security risks and Section IX concludes that MITM is one of the biggest threats.

II. MAN IN THE MIDDLE

A Man-in-the-middle refers to a piece of software that sits anywhere between the victim and their intended destination. This software can spy on the communication and in some cases even modify it. A MITM attack can only succeed when the attacker can impersonate each victim to the satisfaction of the other. Various cryptographic protocols consist of some form of end to end device authentication explicitly to prevent Man In The Middle attacks.

Fig 2.Man in the Middle

One way to prevent MITM attacks is to authenticate both the client and server.

The Taxonomy of MITM attacks are

- Eavesdropping
- Masquerading
- Message Modification
- Replaying
- Denial of Service
- Exploiting flaws in design, implementation or Operation

MITM compromises all the Confidentiality, Integrity and Authenticity.

MITM is categorized in to various categories based on the parameters. They are

a) Man in the middle attack based on the impersonation Techniques.

b) Man in the middle attack based on the communication channel in which attack is executed.

c) Man in the middle attack based on the attacker's location and target in the network.

Let us see those categories in detail:

A *MITM based on the impersonation techniques*:

It is also called as Spoofing which means the attacker pretends to be legitimate user for the purpose of stealing the information. MITM attacks are again divided in to subcategories based on the impersonation. They are as follows.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

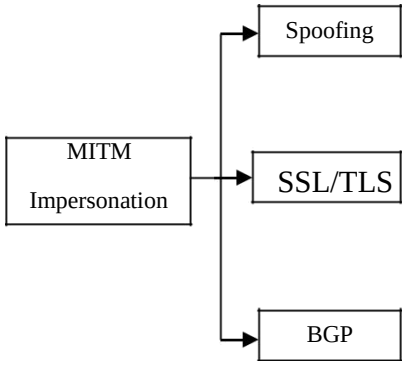

Fig 3. MITM impersonation Attacks

B *Man in the middle attack based on the communication channel*

MITM attacks which happens in various layers of the OSI model are given below fig 3

OSI LAYER	APPLICATION	BGP MITM,DHCP Spoofing based MITM,DNS Spoofing based MITM
	PRESENTATION	SSL/TLS MITM
	TRANSPORT	IP-Spoofing based MITM
	NETWORK	
	DATALINK	ARP based Spoofing MITM

Fig3. MITM attacks in different layers of OSI

C *MITM based on the attacker's location and target in the network* are divided into which is shown in the Fig 4.

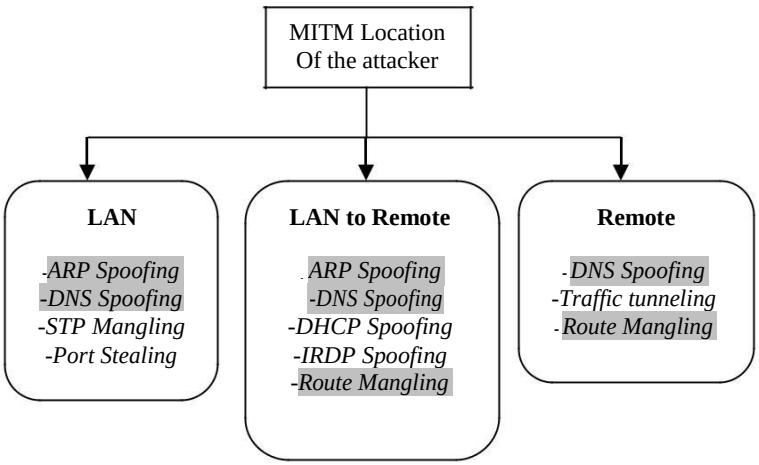

Fig 4. MITM attacks based on the location.

III. SPOOFING BASED MITM

Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because spoofing makes hard to trace the transmitted source, it is also often used in DoS attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions. Common types of MITM Spoofing are as follows:

A. *ARP spoofing based MITM attack*

All the network devices use Address Resolution Protocol for mapping the network addresses and their Media Access Control (MAC) addresses. ARP is very fundamental in LAN connections, because every frame that leaves a system should contain a target or destination MAC address. ARP is an important and trusted protocol and it was not designed to deal with malicious hosts. By adjusting or changing victims' local ARP cache table (adding, updating cache entries), the attacker can be able to inject his malicious data with the host's MAC address with IP of a target host. Therefore, the attacker can create DoS attack, MITM attack and gains control to access the confidential information. ARP spoofing attack may possibly be divided into two types: forging the gateway, and forging the host or a system in the internal network.

At the point when a host requires to connect with another host in an identical network, whose MAC address is obscure, it communicates an ARP Request to all hosts inside the system. Just the host with the reported IP is relied upon to issue a Reply, which incorporates its MAC address. On the other hand, when ARP cache is addressed in a dynamic mode, all the cache entries can be easily forged by duplicate ARP messages, due to lack of proper authentication mechanism. In the meantime, the source machine maintains the entries of all IP and their MAC addresses in the local cache table so that it can process the next communication in the future at a fast manner and evading the broadcast communication. ARP is a stateless protocol in nature and has no security in caching framework. ARP Spoofing is shown in the Fig 4.

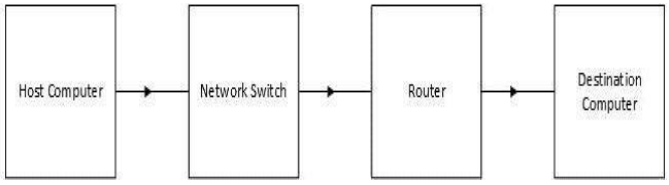

Fig 4. ARP spoofing based MITM

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

B. *DNS spoofing based MITM attack*

A Server of DNS decodes a human understandable domain name format into a numbered IP address format which can be used to route communications between nodes. Normally if the DNS server doesn't know a requested DNS it will ask another server, and the process continues repeatedly. To increase the performance of a DNS server, the DNS server remembers cache of these translations for a short period of time. Whenever it receives any other request for the same translation, it replies without asking any other servers, until that cache expires.

When a DNS server receives a false entry translation it is considered as *poisoned*, and it starts to send the false information to clients. When a DNS server is poisoned, it diverts the traffic to another computer which is know to be an attacker. DNS Spoofing is shown in the Below Fig 5.

One of the maximum outstanding and perilous attacks towards DNS is DNS spoofing that is executed through cache poisoning (DNS spoofing pretty often named as DNS poisoning). DNS carrier makes use of cache system for enhancing overall performance, however it has diverse vulnerable aspects. DNS spoofing consequences in storage via DNS resolver the invalid or malicious mappings between symbolic names and IP addresses. DNS spoofing may be categorized into:

- Stealing or sniffing packets in the process of query reply.
- poisoning the ache entries through the birthday attack;
- hacking on authenticated DNS

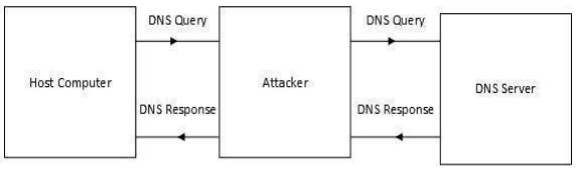

Fig 5 DNS Spoofing based MITM

C. *IP spoofing based MITM attack*

IP is one of the major protocol within the internet, which functions at the network layer of the OSI model. It has the capability of transmitting packets from the source host to the destination host solely based on the IP addresses specified in the packet headers. IP defines the structure of the packets that encapsulates the data to be transmitted or delivered. It also describes addressing methods used to label the datagram headers with source and destination information. Though IP is a connectionless model, which means there may be no information about the transaction state that is used to route packets in the network. Furthermore, IP specifies no approach for validating the authenticity of a packet's source. This means that the attacker could forge the source address with anything he wants. MITM IP spoofing is an attack where an unknown third party seizes a legitimate connection among source and destination. The unknown third party entity controls the flow of communication channel and might dispose of or modify the data sent by source/destination, without the awareness of both authentic endpoints. To attain such results, attackers use a different number of IP spoofing techniques, which could be sorted as below:

1) Blind and non-blind spoofing: when the attacker and the victim are placed inside the same network which provides for possibility to sniff on sequenced arrangement of the packets and acknowledgement numbers is called Non-blind spoofing. When the attacker requests to a network, and examine the sequence of the transmission is called blind spoofing.

2) Internet Control Message Protocol Spoofing: IP use ICMP to send unidirectional messages to execute different testing, errors –reporting and feedback mechanisms. ICMP has an option of redirecting messages, which normally informs the router of a best way. Those messages may be used in a worn way which leads to the launch of MITM attack due to the lack of authentication mechanisms. The assailant catches the ICMP Redirect messages and puts on a show to be the authentic one to course the casualty's activity through its switch, in which it can be listened in and changed. ICMP redirect messages are spoofed by the attacker to route the user's traffic through the router to eavesdrop or modify the messages.

3) DoS Attack: Attacker send thousands of requests to the victim and cause flooding in a very short period of time. It is difficult to trace and stop or block the attackers when the IP address is spoofed. Spoofing makes it difficult to detect the attacker and to deny access to the main cause of the attacks.

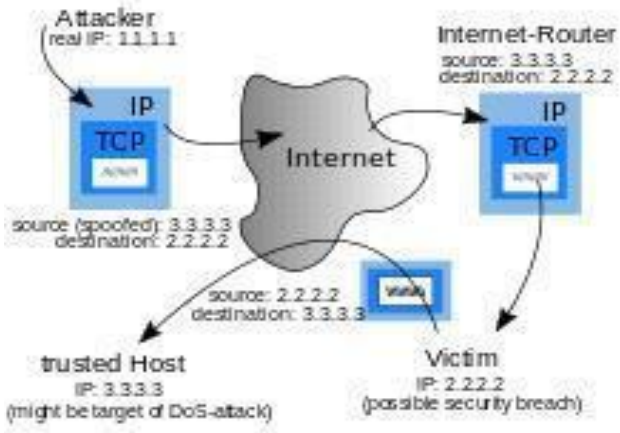

Fig 6. IP spoofing based MITM

D. *STP Mangling*

STP (Spanning-Tree Protocol) mangling refers to the technique used for the attacker host to be elected as the new root bridge of the spanning tree. The attacker may start either by forging BPDUs (Bridge Protocol Data Units) with high priority assuming to be the new root, or by broadcasting STP Configuration/Topology Change Acknowledgement BPDUs to get his host elected as the new root bridge. By taking over

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

the root bridge, the attacker will be able to intercept most of the traffic.

E. *Port Stealing*

This technique is useful to sniff in a switched environment when ARP poisoning is not effective (for example where static mapped ARPs are used).It floods the LAN with ARP packets. The destination MAC address of each "stealing" packet is the same as the attacker's one (other NICs won't see these packets), the source MAC address will be one of the MACs of the victims. This process "steals" the switch's port of each victim. Using low delays, packets destined to "stolen" MAC addresses will be received by the attacker, winning the race condition with the real port owner. When the attacker receives packets for "stolen" hosts, it stops the flooding process and performs an ARP request for the real destination of the packet. When it receives the ARP reply it's sure that the victim has "taken back" his port, so Ettercap can re-send the packet to the destination as is. Now we can re-start the flooding process waiting for new packets.

IV. SECURE SOCKET LAYER/TRANSPORT LAYER SECURITY BASED MITM ATTACK

The guaranteed security offered by SSL/TLS rely on the certificate validation. Therefore, the attacker's main objective is to hijack the website, or to falsify the certificate. The following are the categorization of the SSL/TLS based MITM attacks:

MITM and certificate:
(i)Attacker holds a valid certificate to the target web server. This case is possible if the attacker compromises a CA, or is able to force it to issue such certificate.
(ii)Attacker holds an invalid certificate. In this scenario the attacker may succeed if the victim will ignore the security warnings, which is a common phenomenon.

MITM and key: attacker has a private key to legitimate server.

A. *Secure Socket Layers*

One needs to provide security while communicating with network devices which can be obtained with the help of Secure Socket Layers (SSL) or Transport Layer Security (TLS) by using encryption methodology. One uses this protocol with other protocols for secure implementation of the services that the protocol provides. HTTPS is the most commonly used protocol and most of the online banking services and email services use it to ensure security between their servers and your web browser.

In order to understand how exactly this protocol works consider the following example. Suppose the host PC wants to connect to yahoo mail account then the communication process starts as stated below:

1. Using HTTP port 80, the client web browser will connect to http://mail.yahoo.com.

2. The web server performs the requested process and forwards the client browser to the HTTP version of the particular website using HTTP code.

3. Now the client is connected to the "https://mail.yahoo.com" using port number 443.

4. The server provides authenticated certificate to the host device to verify the identification of the website using the digital signature.

5. The host PC will now verify this certificate with the list of certificates it has.

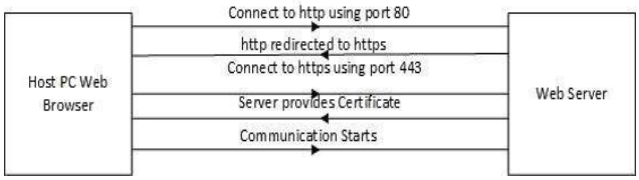

Fig 7.SSL/TLS based MITM attack

B. *SSL protocol communication*

If the certificate doesn't match with the list of certificates of the host PC then we say that the website has failed to verify its identity so the host PC will get a certificate validation error. Even after we get this error we can proceed to connect to the website but it might be risky because we won't know whether it is the actual website we need to connect to.

V. BORDER GATEWAY PROTOCOL(BGP) BASED MITM ATTACK

BGP protocol used to exchange routing information among networks on the Internet. It determines the most effective way to route data packets between independent working networks, or Autonomous Systems. BGP finds path to route data packets from one ISP to another ISP. It is vital to say that BGP protocol not only transfers data but also finds Any Protocols of TCP/IP model can be used to accomplish the transfer. Technically, a gathering of IP prefixes operated by the same entity is referred to as an **Autonomous System**. Each and every autonomous systems are given an Autonomous System Number (ASN) by the Internet Assigned Numbers Authority (IANA).

As BGP determines how data travels from its

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

source to its destination, security is an issue to be taken care of. By handling BGP, data can be rerouted in an attacker's favour allowing them to intercept or modify traffic in internet level.

BGP hijacking is performed by configuring an edge router to announce prefixes that have not been assigned to it. If the malicious announcement is more specific than the legitimate one or claims to offer a shorter path the traffic may be directed to the attacker. Attackers will frequently target unused prefixes for hijacking to avoid attention from the legitimate owner.by broadcasting false prefix announcements the compromised router may poison the routing information base (RIB) of its peers, as shown in the Fig 8. After poisoning one peer, the malicious routing information could propagate to other peers to other autonomous systems, and on to the broader internet.

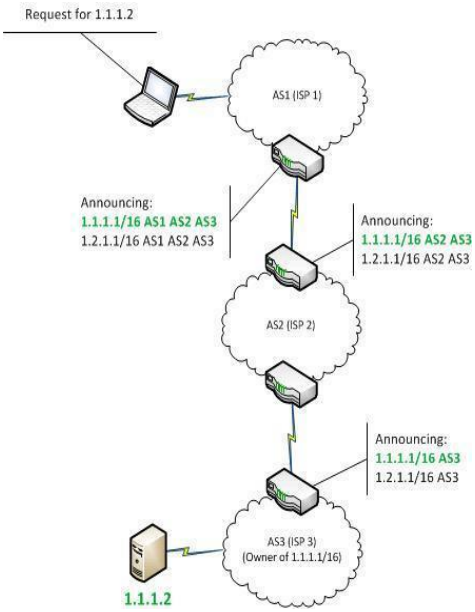

Fig 8.BGP based MITM attack

VI. LITERATURE SURVEY

ARP Spoofing based MITM attack Detection & Prevention Mechanisms are given in Table 1 & 2.

Author	Mechanism	Drawbacks
Carnut et.al	Architecture based on Switched networks	Attackers hide behind the volume traffic and undetected for long period.
Online	ARP Guard, ARP Defender system	Used in LAN and SNMP
Online	ARPwatch	Monitor Ethernet traffic, maintains database of IP& MAC Pairing. Difficult to differentiate between non-malicious and ARP Spoofing attacks.
Hou et.al	ARP Watch	IDS Snort.
Belenguer et.al	Low-cost IDS Prototype	Detect and prevent ARP Spoofing but required to be Plugged in to hub or switch.
Ramachandran et.al	Active IDS	ARP Spoofing detected by mismatch of ARP Request/Response and (IP, MAC) pairing. ARP DoS attacks generated to probe the networks create heavy traffic on LAN.
Trabelsi et.al	Improvised switched network architecture	Detection has 2 phases: Enabling IP Packet Routing for finding the suspicious packets and Target host traffic is tested for ARP Spoofing.
Kalajdzie&Patel	Reverse ARP Poisoning with active IP Probing and IP Probing with CAM table Poisoning	Instead of using test host, every host detects by itself. But certain MITM attacks are not detected and accuracy depends on the size of probing.
Barbhuiya et.al	Digital Signature	ARP requests and ARP Replies are verified by using the digital signature to identify the ARP Origin.
Song et.al	DS-ARP	Routing trace, cache table is been under surveillance and if IP, MAC pair in the cache table changes spoofing is detected. ARP Spoofing attacks is prevented changing the link type from dynamic state to a static state.

Table 1.ARP Spoofing Detection Mechanisms

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

Authors	Mechanisms	Drawbacks
D.Bruschi,A.Ornaghi & E.Rosti	S-ARP Public Key cryptography	By Exchanging the AKD when transmitting the ARP replies it is authenticated by AKD to prevent ARP Spoofing
Gouda et.al	Installed Security Server which has 2 protocols Invite-accept, request -reply	Security is enhanced, single point of failure obvious target of DoS attacks
Goyal et. al	Enhanced S-ARP with low computational costs. Combination of digital signatures , OTP and hash chain.	To avoid additional computations same digital signatures used for many ARP replies. To connect client with untrusted server OTP is shared for security and still uses AKD because it has single point of failure.
Lottah et.al	T-ARP	used for reducing computational cost of S-ARP by generating tickets for each (IP, MAC) Pair. LTA (Local Ticket Agent) and key management server (KMS) to issue public key. Performance overhead, replay attacks.
Y.I.Jerschow, C.Lochert, B.ScheuRmann	Cryptographic Link Layer(CLL) in law used public key cryptography	Host authenticate each other by exchanging the cryptographic parameters
P.Limmaneewic Hid & W.Lilakiatsakun	P-ARP, nonce, hash function HMAC	over all network throughput to an DoS, Slows down the acceptable level

Table 2.ARP Spoofing Prevention Mechanisms

Authors	Mechanisms	Drawbacks
	Ingress Filtering Egress Filtering	Filtering on path using ACL(Access control List) and uRPF(unicast Reverse Path Forwarding). Ingress Filtering & Egress Filtering is deployed at router level.
Yao et.al Z.Duan,X.Yuan & J.Chandrashekar	DPF(Distributed Packet Filtering) IDPF(Inter Domain Packet Filter Extension of DPF	If packets are transmitted in unexpected route they are dropped Builds inter domain filtering rules based on the valley free feature of inter domain routing and BGP announcement filtering rules.
A.Bremler-Barr & H.Levy	Spoofing Prevention Method	Autonomous systems tag is inserted with the data packet specifying the key(S, D).up on receiving in the destination key is verified and removed.
X.Liu,A.Li, A.Yang & D.Wetherall	Packet Passport System	Symmetric Cryptography & hash algorithms. Does not provide protection against spoofing.
H.Wang,C.Jin,and K.G.Shin	HFC(Hop Count Filtering) HOST based solutions	Checks the validation of the source prefix based on the binding between prefix and hop count value. Produces false negatives.HCF bypassed by Attackers.
A.Yaar,A.Perrig and D.Song	Stack Path identifier (Pi) (Host and Router based Solution	Each router uses IP identification field for marking. Packets travelling on the same path has same markings. even if the pi mark receive attack packets it is forced to drop valid packets

Table 3. IP Spoofing Defence Mechanisms

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

VII MITIGATION STRATEGIES

- Avoiding WIFI connections that are not password protected.
- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it is not in use.
- Not using Public networks (Eg. Coffee shops, hotels when conducting sensitive transactions).
- There are two kinds of attack vectors: attack over communication channels, physical on devices.
- Ever trust the communication channel.
- Always use encryption and authentication.

VIII CI TECHNIQUES USED FOR MACHINE TO MAHINE COMMUNICATIONS.

Existing CI techniques which are used in machine to machine communications are Reinforcement Learning, Swarm Intelligence and Mobile Agents, Heuristic methods.
RL is well suited for distributed problems, like routing. It has medium requirements for memory and computation at the individual nodes, arising from the need of keeping many different possible actions and their values. It needs some time to converge, but is easy to implement, highly flexible to topology changes and achieves optimal results.

Swarm intelligence is well suited for distributed network scenarios, where mobility and topology changes are of greatest importance, but energy is not restricted, like MANETs. Like Reinforcement Learning, Swarm Intelligence techniques need some reasonable amount of memory and computational resources on the network nodes and is very adaptable to topology changes. The results under perfect network properties are optimal. Swarm intelligence, for example, causes higher communication overhead by the sending back and forth many learning agents (ants), but achieves optimal results also in a highly mobile environment. Thus, this technique could be considered the first choice when acting in a MANET, where high mobility is present but energy is not restricted.
Reinforcement learning, on the other hand, does not require higher communication costs in the usual case where routing information is sent together with the data packets. However, this means also that routing information is disseminated at most at the same speed as data is forwarded in the network. In case of low data workload, routing information will get either old or will be disseminated only *after* data is sent. This is not well suited for scenarios with high required quality of service,
like multimedia applications. Another possibility, not found in any of the existing protocols, will be to separate the data from the control packets and to achieve better flexibility through constantly exploring the network. However, this resembles already too much a swarm intelligence approach.

Mobile agents refer to the usage of simple, small entities (packets), which traverse the system (in our case the network) and deliver fresh information to the system's nodes without any communication with the environment or each other. In the case of routing (Smart Agents, Ant-AODV), for example, the agents update paths or next hops information on the nodes. They represent a good optimization to traditional routing approaches in mobile scenarios, but increase the communication overhead.
Real Time Heuristic Search methods operate in two steps: planning and plan execution. For example, working with a search tree, they will first calculate the value function (the goodness) of all nodes and then take the best possible path through the tree. This approach cannot be applied in real time scenarios, where agents traverse the search space and have to take their decisions based on locally available data only. Real time heuristic search methods are very well suited for wireless ad-hoc scenarios and have been already applied to routing in ad-hoc networks with good results.

IX CONCLUSION

Most of the cyber-attacks encountered in machine to machine communications are discussed. The major threat against network security in machine to machine communications is MITM.it is important to note that MITM attacks has been launched in critical network infrastructures. Routers and Switches are also spoofed to create high security impact and firewalls can be spoofed to route a legitimate traffic to an attacker machine. We have analysed MITM attacks based on impersonation techniques, communication channels, and based on the location of the attacker. MITM is really difficult to tackle and it should taken serious by the cyber expert's team. It results in stealing the data theft causing rigorous reputational and monetary losses to the private sectors.As an outcome having correctly defined security perimeter defense design, implementing robust management system and following best security practices in server can help to fix MITM attacks. Since the attack is invisible, being vigilant in terms of performance of the network and network problems helps to detect it, before a data theft can occur. Few authors have suggested some detection and prevention mechanisms .so we can conclude that 95% of HTTPS are vulnerable to MITM attacks.

REFERENCES

[1] R. Wagner, "Address resolution protocol spoofing and man-in-the-middle attacks," The SANS Institute, Bethesda, Maryland, USA,2001.Available:https://www.ida.liu.se/~TDDC03/literature/dnscache. pdf
[2] A. Ornaghi and M. Valleri, "Man in the middle attacks," in *Proc. Blackhat Conf. Eur., 2003 [Online]. Available: http://www.blackhat.* com/presentations/bh-Europe-03/bh-Europe-03-valleri.pdf
[3] V. Ramachandran and S. Nandi, "Detecting ARP spoofing: An active technique," in *Information Systems Security. New York, NY, USA:* Springer, 2005, pp. 239–250
[4] M. Carnut and J. Gondim, "ARP spoofing detection on switched Ethernet networks: A feasibility study," in *Proc. 5th Symp. Seguranca Inf., 2003[Online].Available:ftp://www.linorg.cirp.usp.br/pub1/SSI/* 2003/A25.pdf
[5] V. Goyal and R. Tripathy, "An efficient solution to the ARP cache poisoning problem," in *Information Security and Privacy. New York, NY,* USA: Springer, 2005, pp. 40–51.
[6] W. Lootah, W. Enck, and P. McDaniel, "TARP: Ticket-based address resolution protocol, "*Comput. Netw., vol. 51, no. 15, pp. 4322–4337,* 2007.
[7] A. P. Ortega, X. E. Marcos, L. D. Chiang, and C. L. Abad, "Preventing ARP cache poisoning attacks: A proof of concept using

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

OpenWrt," in *Proc. Int. Conf. Latin Amer. Netw. Oper. Manage. Symp. (LANOMS)*,2009, pp. 1–9. [26]

[8] S. Y. Nam, S. Djuraev, and M. Park, "Collaborative approach to mitigating ARP poisoning-based man-in-the-middle attacks," *Comput. Netw.*, vol. 57, no. 18, pp. 3866–3884, 2013.

[9] M. G. Gouda and C.-T. Huang, "A secure address resolution protocol," *Comput. Netw., vol. 41, no. 1, pp. 57–71, 2003.*

[10] Y. I. Jerschow, C. Lochert, B. Scheuermann, and M. Mauve, "CLL: A cryptographic link layer for local area networks," in *Security and Cryptography for Networks. New York, NY, USA: Springer, 2008,* pp. 21–38.

[11] P. Limmaneewichid and W. Lilakiatsakun, "P-ARP: A novel enhanced authentication scheme for securing ARP," in *Proc. Int. Conf.Comput.Commun. Manage. (ICCCM'11), 2011, pp.83–87.*

[12] W. Xing, Y. Zhao, and T. Li, "Research on the defense against ARP spoofing attacks used on Winpcap," in *Proc. 2nd Int. Workshop Educ. Technol. Comput. Sci. (ETCS), 2010, vol. 1, pp. 762–765*

[13] X. Hou, Z. Jiang, and X. Tian, "The detection and prevention for ARP spoofing based on snort," in *Proc. Int. Conf. Comput. Appl. Syst. Model. (ICCASM), 2010, vol. 5, pp. V5–137.*

[14] 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. SecureWare Emerging Secure. Inf. Syst. Technol., 2007,* pp. 122–127

[15] F. Barbhuiya *et al., "An active host-based detection mechanism for* ARP-related attacks," in *Advances in Networks and Communications.* New York, NY, USA: Springer, 2011, pp. 432–443.

[16] M. S. Song, J. D. Lee, Y.-S. Jeong, H.-Y. Jeong, and J. H. Park, "DS-ARP: A new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments," *Sci. World J., vol. 2014, 2014, Art. no. 264654, 7 pp. [Online].Available:* http://www.hindawi.com/journals/tswj/2014/264654/

[17] M. Tanase. (1674). *IP Spoofing: An Introduction [Online]. Available:* http://www.securityfocus.com/infocus

[18] B. Liu, J. Bi, and A. V. Vasilakos, "Toward incentivizing anti-spoofing deployment," *IEEE Trans. Inf. Forensics Secur., vol. 9, no. 3, pp. 436–* 450, Mar. 2014.

[19] P. Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing," RFC2827, 2000.

[20] *intrusion detection system for LAN* specific attacks," in *Advances in Computer Science and Information Technology. New York, NY, USA: Springer, 2010, pp. 129–142.*

[21] K. Kalajdzic and A. Patel, "Active detection and prevention of sophisticated ARP-poisoning man-in-the-middle attacks on switched Ethernet LANs,"

AUTHOR'S BIODATA WITH PHOTOGRAPH

Sabitha Banu. A., she received her MCA in 2007 from Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She is currently pursuing her Ph.D. at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. Her areas of interest are Network Security, Cryptography and Wireless Communications.

G. Padmavathi, she is the Professor in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has 29 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Wireless Communication, Network Security and Cryptography. She has significant number of publications in peer reviewed International and National Journals. Life member of CSI, ISTE, WSEAS, AACE and ACRS.