Cyberspace: Jurnal Pendidikan Teknologi Informasi
Volume 2, Nomor 2, Oktober 2018, 109 - 134

MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS

Avijit Mallik
Department of Mechanical Engineering, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh
Email: avijitme13@gmail.com

Abstract

These days cyber-attack is a serious criminal offense and it is a hot debated issue moreover. A man-in-the-middle-attack is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users. A man-in-the-middle-attack as a protocol is subjected to an outsider inside the system, which can access, read and change secret information without keeping any tress of manipulation. This issue is intense, and most of the cryptographic systems without having a decent authentication security are threatened to be hacked by the malware named 'men-in-the-middle-attack' (MITM/MIM). This paper essentially includes the view of understanding the term of 'men-in-the-middle-attack'; the current work is mainly emphasized to accumulate related data/information in a single article so that it can be a reference to conduct research further on this topic at college/undergraduate level. This paper likewise audits most cited research and survey articles on 'man-in-the-middle-attack' recorded on 'Google Scholar'. The motivation behind this paper is to help the readers for understanding and familiarizing the topic 'man-in-the-middle attack'.

Keywords: *Men-In-The-Middle, Cryptography, Internet Security, Wireless Communication Security, Malware*

1. Introduction

In cryptography and PC security, a man-in-the-middle attack (MITM) is an attack where the attacker furtively transfers and perhaps changes the correspondence between two parties who trust they are straightforwardly communicating with each other. A man in the middle (MITM) attack is a general term for when a culprit positions himself in a discussion between a client and an application; either to listen stealthily or to imitate one of the parties, making it show up as though an ordinary trade of information is in progress (U. Meyer and S. Wetzel, 2004 [1]; L. B. Kish, 2006 [2]; K. Hypponen and K. M. Haataja, 2007 [3]; K. Ouafi *et al.* 2008 [4]). The objective of an attack is to take individual information, for example, login certifications, account points of interest and charge card numbers. Targets are normally the clients of financial applications, SaaS businesses, web-based business locales and other sites where logging in is required. Information obtained during an attack could be utilized for many, purposes, including fraud, unapproved support exchanges or an unlawful watchword change. Furthermore, it can be utilized to gain a decent footing inside an anchored edge during the infiltration phase of an Advanced Persistent Threat (APT) strike. Figure-01 portrays a schematic of 'men-in-the-middle-

attack' belief system. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM (K. Ouafi *et al.,* 2008 [4]; Y. Joshi *et al.,* 2009 [6]; A. S. Khader and D. Lai, 2016 [9]; Y.C. Tung *et al.,* 2016 [10]; B. M. Wallace and J. W. Miller, 2017 [11]; M. Conti *et al.,* 2016 [12])

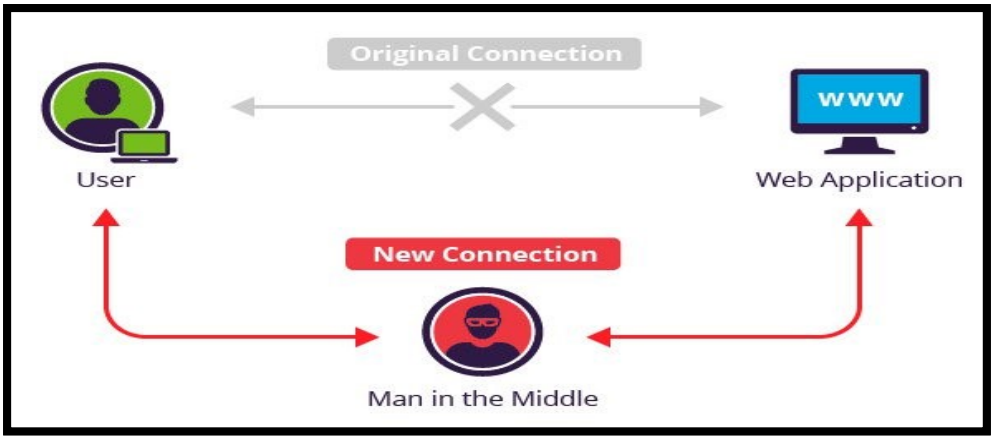

Figure 1. Men-in-the-middle attack ideology schematic

One case of man-in-the-middle attacks is dynamic eavesdropping, in which the attacker makes independent associations with the victims and transfers messages between them to influence them to trust they are talking straightforwardly to each other over a private association when in certainty the whole discussion is controlled by the attacker. The attacker must have the capacity to intercept every single significant message passing between the two casualties and inject new ones. This is direct in many conditions; for instance, an attacker within gathering scope of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle (F. Callegati *et al.,* 2009 [5]; Y. Desmedt, 2011 [7]). As an attack that goes for circumventing common authentication, or scarcity in that department, a man-in-the-middle attack can succeed just when the attacker can mimic every endpoint agreeable to them not surprisingly from the genuine closures. Comprehensively speaking, a MITM attack is what might as well be called a mailman opening your bank proclamation, writing down your record points of interest and after that resealing the envelope and delivering it to your entryway. Most cryptographic conventions include some type of endpoint authentication particularly to persist MITM attacks. For instance, TLS can authenticate one or the two parties using a commonly confided in endorsement expert (D. Sounthiraraj *et al.,* 2014 [8]; A. S. Khader and D. Lai, 2015 [9]; R. Rahim, 2017 [14]).

2. Literature Survey

MITM is named for a ball game where two people play catch while a third person in the middle attempts to intercept the ball. MITM is also known as a fire brigade attack, a term derived from the emergency process of passing water buckets to put out a fire. In the year 2004, U. Meyer and S. Wetzel presented a report on Universal Mobile Telecommunication System's (UITM) security protocol where they discussed about 'men-in-the-middle-attack' on mobile communication (U. Meyer and S. Wetzel, 2004 [1]). In 2006, L. B. Kish published his research in a master listed journal where he showed an encryption method of MITM using Kirchhoff-loop-Johnson (-like)-noise cipher (L. B. Kish, 2006 [2]). K. Hypponen and K. M. J. Haataja (2007), made a research on secure

Bluetooth communication and showed their developed system was capable of preventing MITM attack (K. Hypponen and K. M. Haataja, 2007 [3]). D. Sun *et al.,* 2018 and S. Saif *et al.,* 2018; made similar type of researches on updated version of Bluetooth networks security and discussed about new techniques to prevent MITM in two party's communication (D. Z. Sun *et al.,* 2018 [17]; S. Saif *et al.,* 2018 [21]). K. Ouafi *et al.,* 2008, F. Callegati *et al.,* 2009, Y. Joshi *et al.,* 2009, Y. Desmedt, 2011 and D. Sounthiraraj *et al.,* 2014 conducted researches about HTTP security and those researches found MITM as a very serious threat and those also discussed about the prevention techniques (K. Ouafi *et al.,* 2008 [4]; F. Callegati *et al.,* 2009 [5]; Y. Joshi *et al.,* 2009 [6]; Y. Desmedt, 2011 [7]; D. Sounthiraraj *et al.,* 2014 [8]). A. S. Khader et al. 2015 and Y. Tung et al. 2016 published their researches which mostly talks about different prevention methods of MITM (A. S. Khader & D. Lai, 2015 [9]; Y. Tung *et al.,* 2016 [10]). B. J. Wallace and J. W. Miller patented their research about endpoint based MITM where they tested multiple prevention methods for MITM (B. M. Wallace & J. W. Miller, 2017 [11]). M. Conti *et al.,* 2016; did a survey on MITM and its effects on the economy (M. Conti *et al.*, 2016 [12]). X. Li *et al.,* 2017; R. Rahim, 2017; C. Howell *et al.,* 2018 made identical researches on prevention of MITM mainly for internet communication and those papers discusses several unique and effective measures on prevention of MITM from on-net communication (X. Li *et al.,* 2017 [13]; R. Rahim, 2017 [14]; C. Howell et al., 2018 [16]). Y. Fei *et al.,* 2017; K. Usman *et al.,* 2018; M. R. Valluri, 2018 and E. Kuo *et al.* 2018 published their review reports on MITM which mostly discusses about WLAN security for 2-way communication.

3. Progression of 'Man-In-The-Middle-Attack'

Effective MITM execution has two distinct stages: interception and decryption; which involves being within physical closeness to the intended target, and another that exclusive involves malware, known as a man-in-the-browser (MITB) attack. With a conventional MITM attack, the attacker needs access to an unsecured, or ineffectively anchored Wi-Fi switch (X. Li *et al.,* 2017 [13]; R. Rahim, 2017 [14]; Y. Y. Fei *et al.,* 2018 [15]; C. Howell *et al.,* 2018 [16]; D. Z. Sun *et al.,* 2018 [17]). These sorts of associations are by and large found out in the open territories with free Wi-Fi hotspots, and even in a few people's homes. An attacker will check the switch using code looking for particular shortcomings, for example, default or poor secret key utilize, or security gaps because of the poor arrangement of the switch. Once the attacker has discovered the powerlessness, they will then insert their instruments in the middle of the clients' PC and the sites the client visits. A fresher variation of this attack has been gaining fame with cybercriminals because of its simplicity of execution. With a man-in-the-browser attack, every one of an attacker needs are an approach to inject malware into the PC, which will then install itself into the browser without the clients' learning and will then record the information that is being sent between the victim and particular focused on sites, for example, financial institutions, that are coded into the malware. Once the malware has gathered the particular information it was modified to gather, it then transmits that information back to the attacker.

3.1 Interception

The initial step intercepts client activity through the attacker's system before it achieves its intended destination. The most well-known (and easiest) method for doing this is an inactive attack in which an attacker makes free/open wifi hotspots; accessible to general society. Commonly named in a way that relates to their area, they aren't watchword secured. Once a casualty interfaces with such a hotspot, the attacker gains full permeability to any online information trade. Attackers wishing to adopt a more dynamic strategy to interception may dispatch one of the following attacks:

- *IP spoofing* involves an attacker disguising himself as an application by altering parcel headers in an ip address. Accordingly, clients attempting to get to a url associated with the application are sent to the attacker's site (‘man in the middle (mitm) attack’ (incapsula co.), 2016 [22])

- *ARP spoofing* is the way toward linking an attacker's mac address with the ip address of a legitimate user on a local area network using fake ARP messages. Subsequently, information sent by the client to the host ip deliver is instead transmitted to the attacker (U. Meyer And S. Wetzel, 2004 [1]; I. B. Kish, 2006 [2]; K. Hypponen and K. M. Haataja, 2007 [3]; K. Ouafi *et al.,* 2008 [4]; F. Callegati *et al.,* 2009 [5]; Y. Joshi *et al.,* 2009 [6]; Y. Desmedt, 2011 [7])

- *DNS spoofing*, otherwise called DNS store poisoning, involves infiltrating a DNS server and altering a site's address record. Accordingly, clients attempting to get to the site are sent by the adjusted dns record to the attacker's site (K. Ouafi *et al.,* 2008 [4]; Y. Joshi et al., 2009 [6]; Khader *et al.,* 2015 [9]; C. Howell *et al.,* 2018 [16]; D. Z. Sun *et al.,* 2018 [17]; K. Usman *et al.,* 2018 [18]; M. R. Valluri, 2018 [19]; C. Kuo *et al.,* 2018 [20]; S. Saif *et al.,* 2018 [21]; ‘man in the middle (mitm) attack’ (incapsula co.), 2016 [22]).

3.2. Decryption

After an interception, any two-way SSL movement should be unscrambled without alerting the client or application. Various strategies exist to accomplish this:

- *HTTPS spoofing* sends an imposter endorsement to the victim's browser once the initial association demand for a safe site is made (‘Man-in-the-middle attack’ (Wikipedia) [23]). It holds an advanced thumbprint related with the bargained application, which the browser confirms according to an existing rundown of confided in destinations. The attacker is then ready to get to any information entered by the casualty before it's passed to the application.

- *SSL BEAST* (browser abuse against SSL/TLS) focuses on a TLS variant 1.0 helplessness in SSL. Here, the casualty's PC is infected with pernicious JavaScript that intercepts scrambled treats sent by a web application. Then the application's figure square chaining (CBC) is endangered in order to decode its treats and authentication tokens (‘man-in-the-middle-attack-mitm’ (Techpedia) [25]; “man-in-the-middle-attack” (Rapid Web Ser.) [26]; ‘What is a Man In The Middle attack?’ (Symantec Corp.) [27], Norton Security Blog- ‘What is UMTS?’ (Tech Target Web), Blog Post [28])

- *SSL hijacking* happens when an attacker passes produced authentication keys to both the client and application during a TCP handshake. This sets up what seems, by all accounts, to be a safe association when, actually, the man in the middle controls the whole session (K. Ouafi *et al.,* 2008 [4]; Y. Desmedt, 2011 [7]; ‘Man-in-the-middle attack’ (Wikipedia) [23]; ‘Flaw in Windows DNS client exposed millions of users to hacking’ (SC Mag. UK), News Article [29])

- *SSL stripping* minimizes an HTTPS association with HTTP by intercepting the TLS authentication sent from the application to the client. The attacker sends a decoded form of the application's site to the client while maintaining the anchored session with the application. In the meantime, the client's whole session is noticeable to the attacker (M. Conti *et al.,* 2016 [12]; X. Li *et al.,* 2017 [13]; R. Rahim, 2017 [14]; Y. Y. Fei *et al.,* 2018 [15]; C. Howell *et al.,* 2018 [16]; D. Z. Sun *et al.,* 2018 [17]; K. Usman *et al.,* 2018 [18]; M. R. Valluri, 2018 [19])

4. MITM: What and How?

‘Man-in-the-middle-attack’ also known/abbreviated as MIM, MiM, MitM or MITMA is a type of cryptographic attack over a communication channel by a malicious third party where

he/she takes over a confidential/personal communication channel between two or legitimate communicative points or parties. In this cyber-attack, the attacker can control (read, modify, intercept, change or replace) the communication traffic between victims. But by using MITM protocol the unauthenticated attacker leaves no clues/traces of his interception of this cybercrime, in short words the attacker remains invisible to the victims.

It needs a communication channel to make a MITM attack. The most used communication channels of MITM attack are namely GSM, UMTS, Long-Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), Radio Frequency and Wi-Fi. The first recorded MITM attack was planned in the time of WW-II for intercepting German Military's radio communication and was done by the Royal British Intelligence (also known as MI-6) (W. Kozaczuk, 1984 [31]). In normal sense, there are three most possible compromises, namely Confidentiality, Integrity, and Availability; which is aimed at my MITM attack. Most of the MITM attacks now days are done in social media, because of the extensive use of human communication are done using social media (Facebook, Twitter, Yahoo Messenger and etc. (A. A. Z. Hudaib, 2014 [32]) Decoding a MITM attack is a long process, basically this is done using three ways, namely 1) Based on impersonation methods of cyber decoding, 2) Based on Telecommunication addressing techniques and lastly 3) Based on GPS locating method of attacker and victims both (M. Conti *et al.,* 2016 [33]).

5. Present Status of MITM Attacks

Nowadays, most of the MITM attacks are performed using communication layers. Open System Intercommunication (OSI) and GSM networks are the most affected communication channels by MITM attacks. Table-1 shows types of MITM attacks on different OSI and Cellular service networks ('Man-in-the-middle attack' (Wikipedia) [23]; 'man-middle-attack' (CA Tech) [24]; 'man-in-the-middle-attack-mitm' (Techpedia) [25]; "man-in-the-middle-attack" (Rapid Web Ser.) [26]; 'What is a Man In The Middle attack?' (Symantec Corp.), Norton Security Blog) [27]; 'What is UMTS?' (Tech Target Web), Blog Post [28]; 'Flaw in Windows DNS client exposed millions of users to hacking' (SC Mag. UK), News Article [29]; A. Fatima, 2011 [30]; W. Kozaczuk, 1984 [31]; A. A. Z. Hudaib, 2014 [32]; M. Conti *et al.,* 2016 [33]).

Table-1: MITM attacks on different communication channels

		MITM Types
OSI Layers	Data Links	ARP spoofing type
	Presentation	SSL decryption, CA decryption
	Transport and Networking	IP spoofing
	Applications	DHCP spoofing, BGP type, DNS spoofing
Cellular Networks	GSM	FBS type
	UTMS	

In Table-1, we list MITM attacks across OSI layers and cellular networks. Each layer enforces different approaches to provide security. Nevertheless, neither of them is free from MITM attacks. Ornaghi et al. 2003, at a European conference, was the first to present a security system-based tracking location of the attacker and victim (Ornaghi *et al.*, 2003 [34]). He classified MITM attacks in three distinct categories: a) LAN (Local Area Network) tracking, b) LAN to Remote Network tracking and c) Remote Network track. The authors also take into consideration that STP mangling is a closed type of MITM as the attacker can only manage to decode the unmanaged traffic between two clients.

5.1. Spoofing: Most Common MITM

Spoofing an impersonation technique which is originated from 'spying'. In the middle century, European spies used to hear secret conversation by impersonating him/her to the communicative party. The same method is applied in modern cryptographic spoofing, as the attacker intercepts a confidential/personal communication between two hosts and controls over transferring data, while the hosts are not being aware of the unauthenticated attacker. Some research papers ('Flaw in Windows DNS client exposed millions of users to hacking' (SC Mag. UK), News Article [18]; 'What is UMTS?' (Tech Target Web), Blog Post) [19]; 'What is a Man in The Middle attack?' (Symantec Corp.), Norton Security Blog [20]; "man-in-the-middle-attack" (Rapid Web Ser.), Blog Post [21]; 'man-in-the-middle-attack-mitm' (Techpedia) [22]; 'man-middle-attack' (CA Tech.) [23]; 'Man-in-the-middle attack' (Wikipedia) [24]; 'MAN IN THE MIDDLE (MITM) ATTACK' (Incapsula Co.) [25]; S. Saif *et al.,* 2018 [26]; E. C. Kuo *et al.,* 2018 [27]; M. R. Valluri, 2018 [28]; K. Usman *et al.,* 2018 [29]; D. Senie and P. Ferguson, 1998 [35]; T. E. Humphreys *et al.,* 2008 [36]; L. Scott, 2001 [37]; S. A. Schuckers, 2002 [38]) describe spoofing as the first step of executing MITM, not being the total of a MITM attack; while some other deliciated research papers claim spoofing as a whole MITM process. In this paper, we will consider it as a spoofing based MITM or spoofing attack. When a party wants to communicate with other parties over a cryptographic network then if their network is same with an unknown MAC address then the server broadcasts an address resolution protocol (also abbreviated as ARP) request to all hosts under the same network connection. The client with the announced Internet Protocol is only expected to make a reply including his/her MAC (Media Access Control) address. However, when ARP cache is managed in a dynamic mode, cache entries can be easily fabricated by forged ARP messages, since proper authentication mechanism is missing (M. Oh *et al.,* 2012 [39]). In the meantime, the communicating medium saves the IP to MAC entry in its local cache, so the next time communication can be speeded up, by avoiding the broadcasts.

Address Resolution Protocol has no states thus it provides very few securities to the caching system. Some top-notch researches referring from M. Ataullah and N. Chauhan, 2012 [40]; H. Altunbasak *et al.,* 2004 [41]; S. Subashini and V. Kavitha, 2011 [42]; S. Alabady, 2009 [43]; R. Caceres and V. N. Padmanabhan, 1998 [44]; M. Ford, 2005 [45]; D. Pansa and T. Chomsiri, 2008 [46]; T. Chomsiri, 2008 [47]; H. Salim *et al.,* 2012 [48]; T. Demuth and A. Leitner, 2005 [49] shows the state-of-art (SoA) of using those security weaknesses for conducting a perfect MITM attack. Suppose, we have next network: the attacker 'X' (IP = 10.0.x.x3, MAC = EE:EE:EE:EE:EE:X3), victim 'A' (IP = 10.0.x.x1, MAC = AA:AA:AA:AA:AA:X1), and victim 'B' (IP = 10.0.x.x2, MAC = BB:BB:BB:BB:BB:X2). The next steps for a perfect spoofing based on ARP are shown below:

1)'X' sends an ARP Reply message to 'A', which says that IP: 10.0.x.x3 has MAC address: EE:EE:EE:EE:EE:X3. This message will update 'A''s ARP table.
2)'X' also sends an ARP Reply message to 'B', which says that IP: 10.0.x.x2 has MAC address: EE:EE:EE:EE:EE:X3. This message will update 'B''s ARP table.
3)When 'A' wants to send a message to 'B', it will go to 'X''s MAC address EE:EE:EE:EE:EE:X3, instead of 'B''s BB:BB:BB:BB:BB:X2.
4) When 'B' wants to send a message to 'A', it will also go to 'X'.

Schematic regarding the example stated above is given in **Figure-2**.

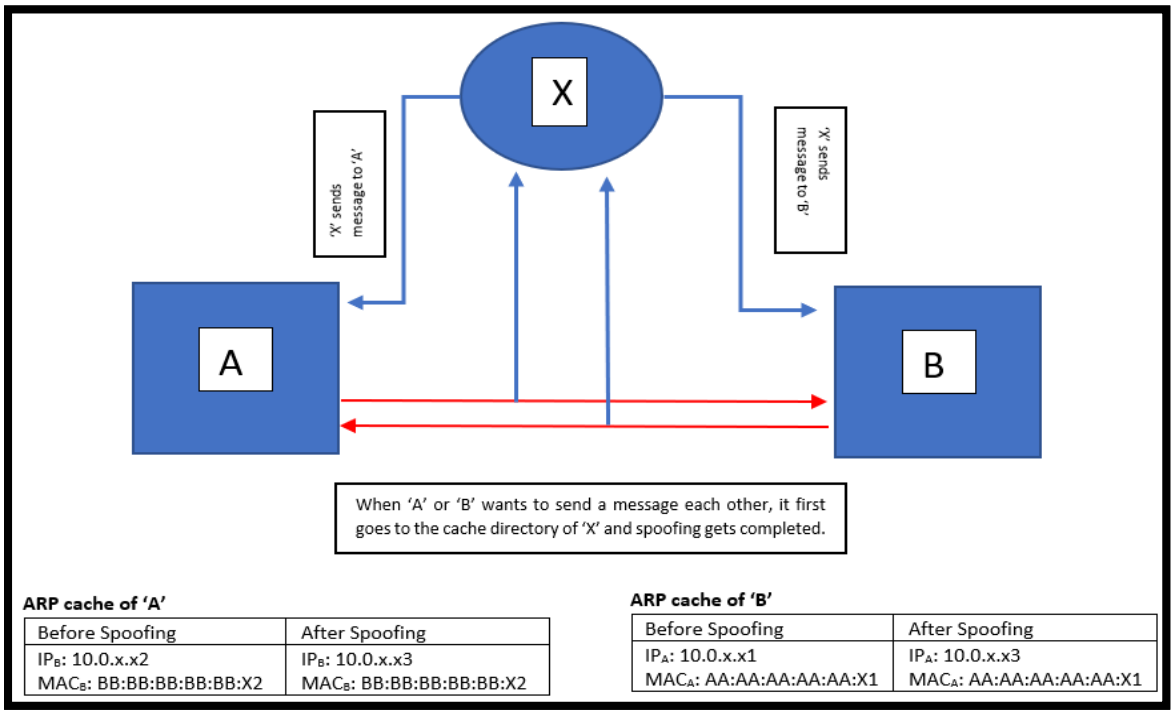

Figure-2: Spoofing method between two clients

There are many well-researched works of literature where spoofing defending system is discussed. Among them T. Demuth *et al.,* 2005, D. Pansa *et al.,* 2008, Z. Trabelsi *et al.,* 2007 and R. Philip *et al.,* 2007 are mostly considerable (D. Pansa and T. Chomsiri, 2008 [49]; T. Demuth and A. Leitner, 2005 [46]; Z. Trabelsi and W. El-Hajj, 2007 [50]; R. Philip *et al.,* 2007 [51]). They introduced various well-researched techniques to prevent spoofing and make secure communication over LAN. But those Literature doesn't concern about wireless methods of communications. The **Table-2** below shows a typical comparison between spoofing prevention techniques:

Table-2: Comparison of various types of spoofing prevention technologies

References	**Medium of Communication**	**Protocol**	**Concerns**
T. Demuth *et al.,* 2005 [49]	Server Based Communication	ARP	Can't work for wireless communications.
D. Pansa *et al.,* 2008 [46]	Server Based/ Host Based	ARP, DHCP	Compatible for DoS, DHCP but has a single point of failure.
Z. Trabelsi *et al.,* 2007 [50]	Host Based	ARP	Level of importance of each host is very difficult to decide.
R. Philip *et al.,* 2007 [51]	Host Based	ARP	Works only with Linksys routers. Static IP not supported.
M. Oh *et al.,* 2012 [52]	Cryptographic/ Host Based	UDP/ ARP	For UDP, authentication is a must need.

Komori *et al.,* 2002 [53]	SYMMETRIC/PRIVATE-KEY CRYPTOGRAPHY	DHCP	Legitimate hosts must register in advance, adds additional message flow, hard to manage for large number of hosts.
Ju *et al.,* 2007 [54]	SYMMETRIC/PRIVATE-KEY CRYPTOGRAPHY, RFC	DCHP, DHCP	The authors did not describe how the random value (the number, which used by the server and client to compute the session key) is determined.
Z. Duan *et al.,* 2006 [55]	Router Based	IP, ARP	Filtering-on-path method can't ensure a secure communication.
D. G. Andersen *et al.,* 2008 [56]	Router/ Host Based	IP, DHCP	This system is considered as the highest secured communication. But not so user friendly.

6. MITM On GSM: A Threat to Phone Communication Security

In the early 90's, the European Telecommunications Standards Institute introduced GSM as a second generation (2G) telecommunication standard. Today, according to the mobility report (SAMSUNG ELECTRONICS SUSTAINABILITY REPORT [57]), GSM covers more than 90% of the world population. There are two basic types of services offered through GSM: telephony and data bearer. The GSM architecture consists of Mobile Stations (MSs) and Base Terminal Stations (BTS), which communicate with each other through radio links. Each BTS connects to the Base Station Controller (BSC). BSC links to the Mobile Switching Center (MSC), which is responsible for routing signals to and from fixed networks (Z. Su *et al.,* 2018 [58]). Home Location Register (HLR) and the Visitor Location Register (VLR) are the two major databases for each mobile service provider in the GSM architecture. Figure-3 shows a schematic of GSM architecture. Each of GSM subscribers has the secret key, which is stored in the Subscriber Identity Module (SIM) card of the MS. The Authentication Center (AUC) has a secret key, which is shared with the subscriber and AUC**.** AUC generates a set of security parameters for execution of encryption and authentication.

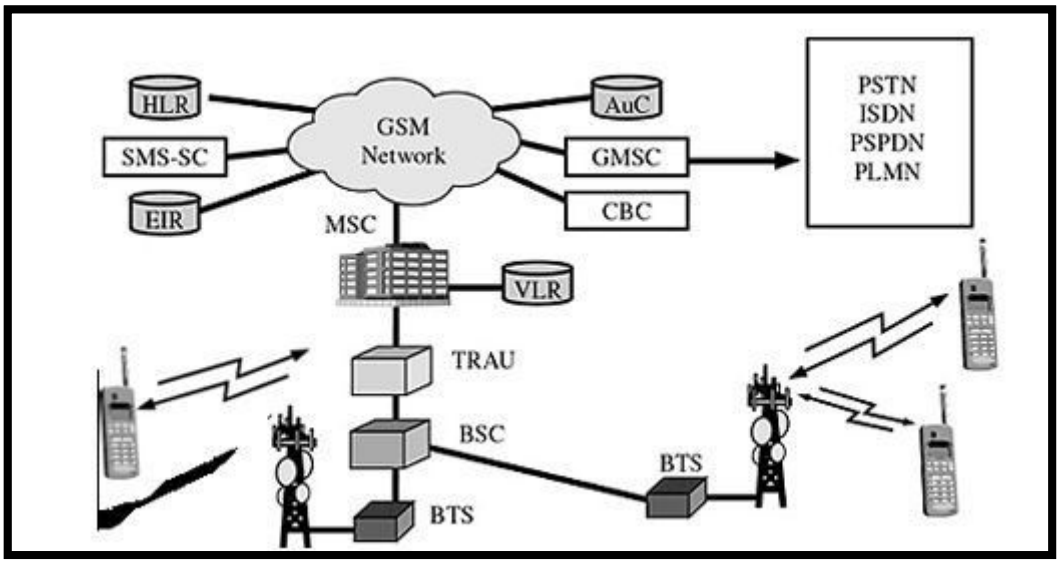

Figure-3: GSM Architecture (J. F. Kurose, 2005 [114])

The main idea behind the attack is to impersonate same mobile network code as the legitimate GSM network to false BTS (or IMSI Cather (N. V. Hardin, 2018 [59]) and convince the victim that this station is the valid one. Let us consider the next example: network consists of the Legitimate MS, Legitimate BTS, False BTS, and False MS. Attacker's network is a combination of the False BTS and False MS. While in standby mode the MS connects to the best received BTS. Therefore, False BTS should be more powerful than the original one, or closer to the target. If the victim is already connected, then the attacker requires to drawn any present real stations. The algorithm of the FBS-based MITM attack on GSM is the following:

1) Attacker sets-up connection between False BTS and Legitimate MS.

2) False MS impersonates the victim's MS to the real network by resending the identity information, which was received from the step 1.

3) Victim's MS sends its authentication information and cipher-suites to the False BTS.

4) Attacker forwards message from step 3 to the Legitimate BTS, with changed authentication abilities of the MS to do not support encryption (A5/0 algorithm (Su X. *et al.* 2018 [60]), or to weak encryption algorithm (e.g., A5/2).

5) Legitimate MS and Legitimate BTS exchange authentication challenge (RAND), and authentication response (SRES), attacker forwards them.

Figure-4 below shows a graphical representation of the example stated above.

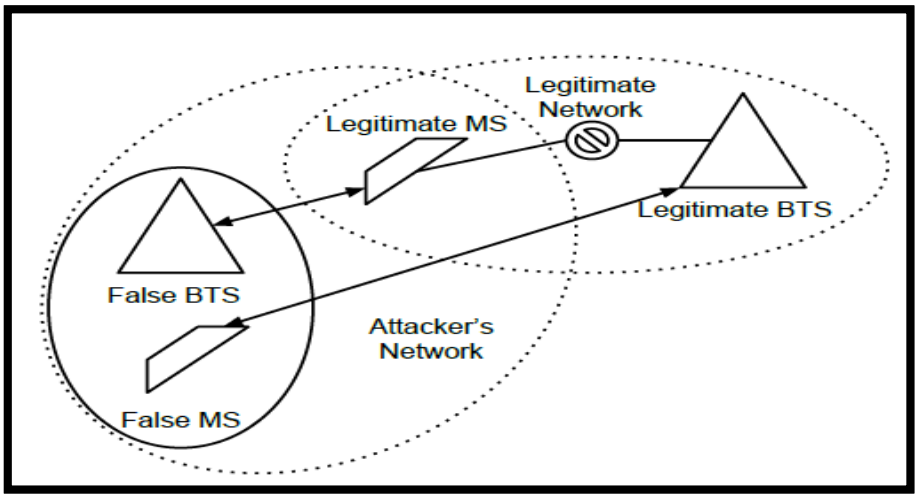

Figure-4: MITM in GSM network

Finally, the authentication is finished. All following messages between the victim and real network are going through attacker's entities, with encryption specified by an attacker, or no encryption at all. This manipulation is possible since GSM does not provide the data integrity (Z. Chen *et al.,* 2007 [61]), as a result, the attacker can catch, modify, and resend messages.

At the designing phase of the GSM protocol, FBS seemed impractical due to costly required equipment, but currently, this kind of attack is completely applicable since costs decreased (B. Feher *et al.,* 2018 [62]). Paik *et. al.,* 2010 (Paik *et. al.,* 2010 [63]); besides describing GSM security concerns, pointed out that nowadays attackers are better equipped. Among the reasons we can identify opensource projects (e.g., Open BTS (D. A. Burgess and H. S. Samra, 2008 [64])) and low-cost hardware (e.g., Ettus Research (A. N. I. C. Ettus Research. Ettus research - the leader in software-defined radio (SDR) [65])). In particular, an attacker can build its own false BTS for less than $1000. An algorithm of FBD based MITM attack on GSM network is given below in Figure-5.

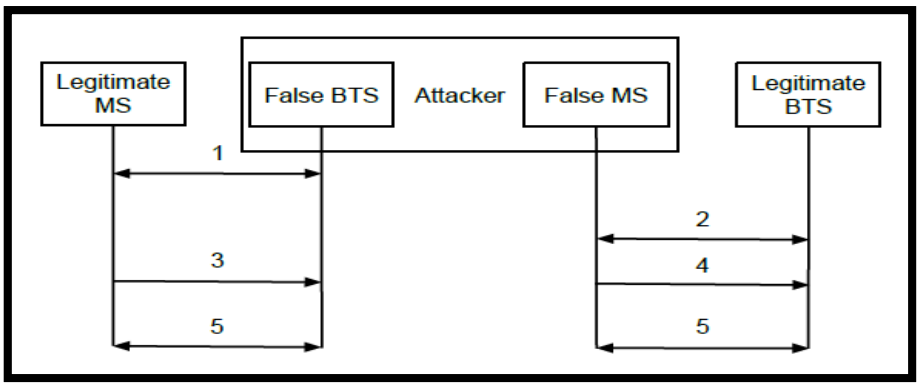

Figure-5: MITM on GSM network via FBS method

The Table-3 discusses various FBS based MITM attacks prevention approaches and different attacks with regarding references.

Table-3: FBS based MITM attacks preventions

Preventions	H. H. Ou *et al.*, 2010 [66]	Y. L. Huang *et al.*, 2011 [67]	T. Hwang *et al.*, 2014 [68]	N. Saxena and N. S. Chaudhari, 2014 [69]	N. Saxena and N. S. Chaudhari, 2014 [70]
MITM attacks	Yes	Yes	Yes	Yes	Yes
Replay attacks	Yes	Yes	Yes	Yes	Yes
Active attack in unauthorized network	Yes	Yes	Yes	Yes	Yes
Redirection	Yes	Yes	Yes	Yes	Partially
DoS attack	No	Partially	Yes	No	Yes

7. Statistical Analysis of MITM Attack

For statistical analysis of the MiM attacks, we refer to the usual finite lattice of security levels, $(\mathcal{S}, \sqsubseteq_{\mathcal{S}}, \sqcap_{\mathcal{S}}, \sqcup_{\mathcal{S}}, \top_{\mathcal{S}}, \bot_{\mathcal{S}})$ and based on it define $\zeta: \mathbb{N} \to \mathcal{S}$ as a mapping from names to their security levels. Now, we can define the *name integrity* property as follows.

Property [Name integrity]

We say that a name, x, has the integrity property with respect to a ϕ_A environment if

$$\forall n \in value_{of(\phi_A(x))}: \zeta(x) \sqsubseteq \zeta(n)$$

The predicate integrity (x, ϕ_A) indicates that x upholds the above property with respect to ϕ_A. A MITM attack is defined as an attack in which the intruder is capable of breaching the integrity of names of two processes.

Property [Man-in-the-Middle Attack]

A context, C (a process with a hole) succeeds in launching a MiM attack on two processes, P and Q, if the result of the abstract interpretation, $A(|C(P|Q|)\{||\}\ \bot_{D_\bot} = \phi_A$ proves that$\exists_x \in bn(P), y \in bn(Q): \neg(integrity(x, \phi_A) \vee integrity(y, \phi_A))$.

8. Preveenting 'MITM'

Blocking MITM attacks requires a few down to earth ventures with respect to clients, and additionally a combination of encryption and check techniques for applications. For clients, this implies:

- Avoiding WiFi associations that aren't password encrypted.
- Paying consideration regarding browser warnings reporting a site as being unsecured.
- Immediately logging out of a protected application when it's not in utilize.
- Not using open systems (e.g., cafés, lodgings) when conducting sensitive financial exchanges.

For site administrators, secure correspondence conventions, including TLS and HTTPS, help relieve spoofing attacks by vigorously encrypting and authenticating transmitted information (A. Fatima, 2011 [30]). Doing so keeps the interception of site activity and hinders

the decoding of delicate information, for example, authentication tokens. It is viewed as best practice for applications to utilize SSL/TLS to anchor each page of their site and not only the pages that expect clients to sign in. Doing so helps diminishes the possibility of an attacker stealing session treats from a client browsing on an unsecured segment of a site while signed in.

To counter MITM, Antivirus frameworks furnishes its clients with a streamlined end-to-end SSL/TLS encryption, as a component of its suite of security administrations (‘Man-in-the-middle attack’ (Wikipedia) [23]; ‘man-middle-attack’ (CA Tech.) [24]; ‘man-in-the-middle-attack-mitm’ (Techpedia) [25]; “man-in-the-middle-attack” (Rapid Web Ser.), Blog Post [26]; ‘What is a Man In The Middle attack?’ (Symantec Corp.), Norton Security Blog [27]; ‘What is UMTS?’ (Tech Target Web), Blog Post [28]; ‘Flaw in Windows DNS client exposed millions of users to hacking’ (SC Mag. UK), News Article [29]). Facilitated on well-known Anti-spam administrations content conveyance arrange (CDN), the authentications are ideally executed to forestall SSL/TLS compromising attacks, for example, minimize attacks (e.g. SSL stripping), and to guarantee compliance with most recent PCI DSS demands. Offered as a managed benefit, SSL/TLS arrangement is stayed up with the latest maintained by an expert security, both to stay aware of compliance demands and to counter emerging dangers (e.g. Heartbleed) (‘What is a Man In The Middle attack?’ (Symantec Corp.), Norton Security Blog [27]). Finally, with Antivirus dashboards, the client can likewise design HTTP Strict Transport Security (HSTS) arrangements to implement the utilization of SSL/TLS security over different subdomains. This furthers secure site and web application from convention minimize attacks and treat hijacking endeavours. **Table-4** gives a typical review of different types of prevention methodologies.

Table-4: Various MITM prevention Mechanisms studied from literatures

		Approaches				
		Detection	**Cryptography**	**Voting**	**Hardware**	**Other**
OSI	**Application**	***BGP:*** (Mayer and Susanne, 2014[1]; Hypponen and Keijo, 2007[2]; Ouafi *et al.,* 2008[3]; Callegati *et al.,* 2009[4]; Joshi *et al.,* 2009[5]; Yvo Desmedt, 2011[6]; D. Sounthiraraj *et al.,* 2014[7]; A. S. Khader and D. Lai, 2015[8]; Yu-Chih Tung *et al.,* 2016[9]; B. M. Wallace and J. W. Miller, 2017[10]; M. Conti *et al.,* 2016[11]; X. Li *et al.,* 2017[12]; R. Rahim, 2017[13]; Yang-Yang Fei *et al.,* 2018[14]; C. Howell *et al.,* 2018[15]; Da-Zhi Sun *et al.,* 2018[16]; K. Usman *et al.,* 2018[17]; M. R. Valluri 2018[18]; En-Chun Kuo *et al.,* 2018[19]; S. Saif *et al.,* 2018[20]), (T. Stiansen, 2018[78]; V. Chaz and Kim-Kwang Raymond Choo, 2018[79]; T. Stiansen *et al.,* 2018[80]) **DNS:** (Yong Wan Ju *et al.,* 2007[71]; A. Chopra and MichaelKaufman, 2014[72]; T. Naqash et al. 2012[73]; D.	***BGP:***(A. Mitseva *et al.,* 2018[81]; Preneel and Frederik Vercauteren, 2015[82]; Haya Shulman, 2018[83]; M. Flores *et al.,* 2018[84]) ***DCHP:*** (H. H. Ou *et al.,* 2010[66]; Y. L. Huang *et al.,* 2017[67]; T. Hwang and Prosanta Gope, 2014[68]; N. Saxena and N. S. Chaudhari, 2014 (1 & 2) [68 and 69])	***DNS:***('man-in-the-middle-attack'(CA.Tech.) [24]), (Z. Duan *et al.,* 2006[55]; D. G. Andersen *et al.,* 2008[56]; SAMSUNG ELECTRONICS SUSTAINABILITY REPORT, 2017[57]; Z. Su *et al.,*2018[58]; N. V. Hardin 2018[59]; Su Xin *et al.,* 2005[62]), (M. Flores *et al.,* 2018[86]; R. Fernàndez-València *et al.,* 2018[88]; D. Hanna *et al.,* 2018[89])	***DCHP:*** (A. N. I. C. Ettus Research. Ettus research[65]; H. H. Ou et al. 2010[66]; Y. L. Huang *et al.,* 2011[67]; T. Hwang *et al.,* 2014[68]; N. Saxena And N.S. Chaudhari 2014[69]), (M. Xie *et al.,* 2018[87], A. Karina *et al.,* 2018[89])	***BGP:*** (T. Naqash *et al.,* 2012[73]; D. Kaminsky, 2008[77]; Y. Lindell, 2018; L. Xiang, 2018[86]; D. Zhang, 2018[113]) ***DNS:*** (T. Stiansen *et al.,* 2018[93]; A. Mitseva *et al.,* 2018[102]; B. Preneel and Frederik Vercauteren, 2015[106])

		Kaminsky, 2008[74]; Y. Lindell 2018[75]; Li Xiang *et al.,* 2018[76]; D. Zhang, Yuezhi Zhou and Yaoxue Zhang, 2018[77])				
	Presentation	***SSL/TLS:*** (M. Ulrike and Susanne Wetzel, 2004[1]; B. Laszlo and Kish, 2006[2]; K. Hypponen and M. J. Haataja, 2007[3]; K. Ouafi *et al.,* 2008[4]; F. Callegati *et al.,* 2009[5]; Y. Joshi *et al.,* 2009[6]; Yvo Desmedt, 2011[7]; D. Sounthiraraj *et al.,* 2014[8]; A. S. Khader and David Lai, 2015[9]; Yu-Chih Tung *et al.,* 2016[10]; B. M. Wallace and W. S. Miller, 2018[11]; M. Conti *et al.,* 2016[11]; Xiaohong Li *et al.,* 2017[12]), (Logan Scott, 2001[37])	***SSL/TLS:*** (B. M. Wallace and W. S. Miller, 2016[33]; M. Conti *et al.,* 2016[34]; T. Stiansen, 2018[35]; V. Chaz and Kim-Kwang Raymond Choo, 2018[36]; T. Stiansen *et al.,* 2018[37]; X. Li *et al.,* 2017[39]), (A. Karina *et al.,* 2015[88]; U. Nath *et al.,* 2018[89]; M. S. Hossain *et al.,* 2018[90]; D. Sinor, 2018[91])	***SSL/TLS:*** (L. Scott, 2001[37]; M. Oh *et al.,* 2012[39])	-	***SSL/TLS:*** (D. Sinor, 2018[92]; D. Gunawan, 2018[93])
	Transport	-	***IP:*** (Ulrike Meyer and Susanne Wetzel, 2004[1]; Laszlo B. Kish, 2006[3]; K. Hypponen and Keijo MJ Haataja, 2007[4]; K. Ouafi *et al.,* 2008[5]; F. Callegati *et al.,* 2009[6]; Y. Joshi *et al.,* 2009[7]; Yvo	-	-	***IP:*** (L. W. Huang *et al.,* 2018[96]; J. L. Goodman *et al.,* 2018[97]; X. Wang *et al.,* 2018[98])

			Desmedt, 2011[8]; D. Sounthiraraj *et al.,* 2014[9]; A. S. Khader and David Lai, 2015[10]; Yu-Chih Tung *et al.,* 2016[11]; B. M. Wallace and W. S. Miller, 2016[12]; M. Conti *et al.,* 2016[13]; X. Li *et al.,* 2017[14]; R. Rahim, 2017[15]; Yang-Yang Fei *et al.,* 2018[16]; C. Howell *et al.,* 2018[17]; Da-Zhi Sun *et al.,* 2018[18]; K. Usman *et al.,* 2018[19]; M. R. Valluri, 2018[20]; En-Chun Kuo et al 2018[21]; S. Saif *et al.,* 2018[22]; 'MAN IN THE MIDDLE (MITM) ATTACK' (Incapsula Co.)[33]; 'Man-in-the-middle attack' (Wikipedia); 'man-middle-attack' (CA Tech.)[34]), (M. I. Gramegna *et al.,* 2018[94]; M. F. Anagreh *et al.,* 2018[95]; L. W. Huang *et al.,* 2018[96])			
	Network	-	||	-	-	||
	Data Link	***ARP:*** (H. H. Ou *et al.,* 2018[60]; M. I. Gramegna	***ARP:*** (Mayer and Susanne, 2014[1];	***ARP:*** (Humphreys *et al.,* 2008[38]; L. Scott, 2001[39]; S.	***ARP:*** (L. W. Huang et al. 2018[96];	***ARP:*** (Z. Duan *et al.,* 2006[55]; D. G. Andersen *et al.,*

		et al., 2018[61]; M. F. Anagreh *et al.,* 2018[62]; L. W. Huang *et al.,* 2018[63]; R. Rahim, 2017[64]; Yang-Yang Fei *et al.,* 2018[65]; C. Howell *et al.,* 2018[66]; Da-Zhi Sun *et al.,* 2018[67]; K. Usman *et al.,* 2018[68]; M. R. Valluri, 2018[69]; En-Chun Kuo *et al.,* 2018[70]; S. Saif *et al.* 2018[71]; 'MAN IN THE MIDDLE (MITM) ATTACK' (Incapsula Co.)[72]; 'Man-in-the-middle attack' (Wikipedia); 'man-middle-attack' (CA Tech.) [73])	Hypponen and Keijo, 2007[2]; Ouafi *et al.,* 2008[3]; Callegati *et al.,* 2009[4]; Joshi *et al.,* 2009[5]; Yvo Desmedt, 2011[6]; D. Sounthiraraj *et al.,* 2014[7]; A. S. Khader and D. Lai, 2015[8]; Yu-Chih Tung *et al.,* 2016[9]; B. M. Wallace and J. W. Miller, 2017[10]; M. Conti *et al.,* 2016[11]; X. Li *et al.,* 2017[12]; R. Rahim, 2017[13]; Yang-Yang Fei *et al.,* 2018[14]; C. Howell *et al.,* 2018[15]; Da-Zhi Sun *et al.,* 2018[16]; K. Usman *et al.,* 2018[17]; M. R. Valluri, 2018[18]; En-Chun Kuo *et al.,* 2018[19]; S. Saif *et al.,* 2018[20]; T. Stiansen, 2008[23])	A. C. Schuckers, 2002[80]; Myeongjin Oh, 2012[81])	Goodman *et al.,* 2018[97]; X. Wang *et al.,* 2018[98]; Y. Li *et al.,* 2018[99]; D. MAHESWARI *et al.,* 2015[100]; M.Truedsson *et al.,* 2018[101])	2008[56]; W. Timmermans,2018[57])
Modular Networks	***GSM***	-	(Z. Trabelsi and W. El-Hajj, 2007[78]; R. Philip, 2007[79]; M. Oh, 2012[80]; T. Komori and T. Saito, 2002[81]; H. Ju and J. Han, 2012[82]; Z. Duan, X. Yuan, and J. Chandrasheka	-	-	-

			r, 2006[83]; D. G. Andersen *et al.,* 2005[84]), (M. Siergiejczyk and Adam Rosiński, 2018[102]; N. Nayak and Rohit Sharma, 2018[103]; G. Firdous *et al.,* 2018[106])			
	UMTS	-	(T. Stiansen, 2018(a)[78]; C. Vidal and Kim-Kwang Raymond Choo, 2017[79];T. Stiansen, 2018(b)[80]); (M.S. M.M. Jadhao *et al.,*2018[107]; Firdous, G. Shaheen, and R.Sandeep Kumar, 2018[108]; N. Nayak and Rohit Sharma. 2018[109]; M. Siergiejczyk and Adam Rosiński, 2018[110]; M. Truedsson and Viktor Hjelm, 2018[111])	-	-	-

9. Conclusion

The MITMs interrupt interchanges between two frameworks, and this phenomenon takes place when the attacker is responsible for a switch along typical point of movement. The attacker in all cases is situated on a similar communicated domain as the victim stands. Indeed, in a HTTP exchange, a TCP protocol exists among the customer and the server. The attacker divides the TCP protocol into two connections – one between the victim and the attacker and the other between the attacker and the server. On intercepting the TCP protocol, the attacker goes about as an intermediary reading, altering and inserting information in intercepted correspondence. In an unsecured connection (e.g. HTTP protocol), the communication of two users can be hacked by an intruder without any difficulties. In a HTTPS connection, a single TCP protocol is attained by building two independent SSL connections. A MITM attack exploits the shortcoming in arrange correspondence convention, convincing the casualty to course movement through the attacker instead of ordinary switch and is by and large alluded to as ARP spoofing. This unethical

phenomenon can affect a country's economy and may be a reason of instability between nations by stealing/modifying classified/secret defence sector data/information. So, this unethical phenomenon has to be prevented, and the necessary measures should be taken for ending. Although the paper did not focus on extensive analysis for future research directions of MITM, but a good understanding about MITM and the technologies for preventing MITM like Li-Fi were discussed briefly.

Author Contributions

This article has been made under a part of the undergraduate thesis of the first author and the second author made the literature review along with necessary computing and communication reviews. The total reporting was directly supervised by the 3rd author.

References

[1] Meyer, Ulrike, and Susanne Wetzel. "A man-in-the-middle attack on UMTS." In *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 90-97. ACM, 2004.

[2] Kish, Laszlo B. "Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security." *Fluctuation and Noise Letters* 6, no. 01 (2006): L57-L63.

[3] Hypponen, Konstantin, and Keijo MJ Haataja. ""Nino" man-in-the-middle attack on bluetooth secure simple pairing." In *Internet, 2007. ICI 2007. 3rd IEEE/IFIP International Conference in Central Asia on*, pp. 1-5. IEEE, 2007.

[4] Ouafi, Khaled, Raphael Overbeck, and Serge Vaudenay. "On the security of HB# against a man-in-the-middle attack." In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 108-124. Springer, Berlin, Heidelberg, 2008.

[5] Callegati, Franco, Walter Cerroni, and Marco Ramilli. "Man-in-the-Middle Attack to the HTTPS Protocol." *IEEE Security & Privacy* 7, no. 1 (2009): 78-81.

[6] Joshi, Yogesh, Debabrata Das, and Subir Saha. "Mitigating man in the middle attack over secure sockets layer." In *Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on*, pp. 1-5. IEEE, 2009.

[7] Desmedt, Yvo. "Man-in-the-middle attack." In *Encyclopedia of cryptography and security*, pp. 759-759. Springer, Boston, MA, 2011.

[8] Sounthiraraj, David, Justin Sahs, Garret Greenwood, Zhiqiang Lin, and Latifur Khan. "Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps." In *In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14*. 2014.

[9] Khader, Aqeel Sahi, and David Lai. "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol." In *22nd International Conference on Telecommunications: ICT 2015*, p. 204. Engineers Australia, 2015.

[10] Tung, Yu-Chih, Kang G. Shin, and Kyu-Han Kim. "Analog man-in-the-middle attack against link-based packet source identification." In *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 331-340. ACM, 2016.

[11] Wallace, Brian Michael, and Jonathan Wesley Miller. "Endpoint-based man in the middle attack detection using multiple types of detection tests." U.S. Patent 9,680,860, issued June 13, 2017.

[12] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A survey of man in the middle attacks." *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 2027-2051.

[13] Li, Xiaohong, Shuxin Li, Jianye Hao, Zhiyong Feng, and Bo An. "Optimal Personalized Defense Strategy Against Man-In-The-Middle Attack." In *AAAI*, pp. 593-599. 2017.

[14] Rahim, Robbi. "Man-in-the-middle-attack prevention using interlock protocol method." *ARPN J. Eng. Appl. Sci* 12, no. 22 (2017): 6483-6487.

[15] Fei, Yang-Yang, Xiang-Dong Meng, Ming Gao, Hong Wang, and Zhi Ma. "Quantum man-in-the-middle attack on the calibration process of quantum key distribution." *Scientific reports* 8, no. 1 (2018): 4283.

[16] Howell, Christopher, Robert Statica, and Kara Lynn Coppa. "In-band identity verification and man-in-the-middle defense." U.S. Patent 9,906,506, issued February 27, 2018.

[17] Sun, Da-Zhi, Yi Mu, and Willy Susilo. "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure." *Personal and Ubiquitous Computing*22, no. 1 (2018): 55-67.

[18] Usman, Karim, Awuhe T. Richard, Aboho D. Moses, and Ugba T. Pius. "A Novel Approach to Enhance the Security of Keys Shared by Users in WLAN Environments Using 3DES Algorithm." *International Journal of Advanced Studies in Computers, Science and Engineering* 7, no. 2 (2018): 1-7.

[19] Valluri, Maheswara Rao. "Cryptanalysis of Xinyu et al.'s NTRU-lattice based key exchange protocol." *Journal of Information and Optimization Sciences* 39, no. 2 (2018): 475-479.

[20] Kuo, En-Chun, Ming-Sang Chang, and Da-Yu Kao. "User-side evil twin attack detection using time-delay statistics of TCP connection termination." In *Advanced Communication Technology (ICACT), 2018 20th International Conference on*, pp. 211-216. IEEE, 2018.

[21] Saif, Sohail, Rajni Gupta, and Suparna Biswas. "Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring." In *Advanced Computational and Communication Paradigms*, pp. 665-674. Springer, Singapore, 2018.

[22] 'MAN IN THE MIDDLE (MITM) ATTACK' (Incapsula Co.), 2016, Retrieved from: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

[23] 'Man-in-the-middle attack' (Wikipedia), 2018, Retrieved from: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[24] 'man-middle-attack' (CA Tech.), 2018, Retrieved from: https://www.veracode.com/security/man-middle-attack

[25] 'man-in-the-middle-attack-mitm' (Techpedia), 2018, Retrieved from: https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm

[26] "man-in-the-middle-attack" (Rapid Web Ser.), Blog Post, 2017, Retrieved from: https://www.thesslstore.com/blog/man-in-the-middle-attack/

[27] 'What is a Man In The Middle attack?' (Symantec Corp.), Norton Security Blog, 2018, Retrieved from: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[28] 'What is UMTS?' (Tech Target Web), Blog Post, 2018, Retrieved from: https://searchmobilecomputing.techtarget.com/definition/UMTS

[29] 'Flaw in Windows DNS client exposed millions of users to hacking' (SC Mag. UK), News Article, 2017, Retrieved from: https://www.scmagazineuk.com/flaw-in-windows-dns-client-exposed-millions-of-users-to-hacking/article/699416/

[30] Fatima, Amtul. "E-Banking Security Issues-Is There A Solution in Biometrics?." *Journal of Internet Banking and Commerce*16, no. 2 (2011): 1.

[31] Kozaczuk, Wladyslaw. Enigma: How the German Machine Cipher was Broken, and How it was Read by the Allies in World War Two (Foreign Intelligence Book Series). Lanham, MD: University Publications of America, 1984.

[32] Hudaib, Adam Ali Zare. "Comprehensive Social Media Security Analysis & XKeyscore Espionage Technology." International Journal of Computer Science and Security (IJCSS) 8, no. 4 (2014): 97.

[33] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A survey of man in the middle attacks." *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 2027-2051.

[34] A. Ornaghi and M. Valleri, "Man in the middle attacks," in Blackhat Conference Europe, 2003.

[35] Senie, D., and P. Ferguson. "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing." *Network* (1998).

[36] Humphreys, Todd E., Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer." In *Radionavigation Laboratory Conference Proceedings*. 2008.

[37] Scott, Logan. "Anti-spoofing & authenticated signal architectures for civil navigation systems." In *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pp. 1543-1552. 2001.

[38] Schuckers, Stephanie AC. "Spoofing and anti-spoofing measures." *Information Security technical report* 7, no. 4 (2002): 56-62.

[39] Oh, Myeongjin, Y-G. Kim, Seungpyo Hong, and S. Cha. "ASA: agent-based secure ARP cache management." *IET communications* 6, no. 7 (2012): 685-693.

[40] Ataullah, Md, and Naveen Chauhan. "ES-ARP: an efficient and secure address resolution protocol." In *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, pp. 1-5. IEEE, 2012.

[41] Altunbasak, Hayriye, Sven Krasser, Henry Owen, Joachim Sokol, and Jochen Grimminger. "Addressing the weak link between layer 2 and layer 3 in the Internet architecture." In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pp. 417-418. IEEE, 2004.

[42] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[43] Alabady, Salah. "Design and Implementation of a Network Security Model for Cooperative Network." *Int. Arab J. e-Technol.* 1, no. 2 (2009): 26-36.

[44] Caceres, Ramon, and Venkata N. Padmanabhan. "Fast and scalable wireless handoffs in support of mobile Internet audio." *Mobile Networks and Applications* 3, no. 4 (1998): 351-363.

[45] Ford, Mat. "New internet security and privacy models enabled by ipv6." In *Applications and the Internet Workshops, 2005. Saint Workshops 2005. The 2005 Symposium on*, pp. 2-5. IEEE, 2005.

[46] Pansa, Detchasit, and Thawatchai Chomsiri. "Architecture and protocols for secure LAN by using a software-level certificate and cancellation of ARP protocol." In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2, pp. 21-26. IEEE, 2008.

[47] Chomsiri, Thawatchai. "Sniffing packets on LAN without ARP spoofing." In *Third 2008 International Conference on Convergence and Hybrid Information Technology*, pp. 472-477. IEEE, 2008.

[48] Salim, Haider, Zhitang Li, Hao Tu, and Zhengbiao Guo. "Preventing ARP spoofing attacks through gratuitous decision packet." In *Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2012 11th International Symposium on*, pp. 295-300. IEEE, 2012.

[49] T. Demuth and A. Leitner, “Arp spoofing and poisoning: Traffic tricks,” Linux magazine, vol. 56, pp. 26–31, 2005.

[50] Z. Trabelsi and W. El-Hajj, “Preventing arp attacks using a fuzzy-based stateful arp cache,” in IEEE International Conference on Communications (ICC’07). IEEE, 2007, pp. 1355–1360.

[51] R. Philip, “Securing wireless networks from arp cache poisoning,” Masters Thesis, San Jose State University, 2007.

[52] M. Oh, Y.-G. Kim, S. Hong, and S. Cha, “Asa: agent-based secure arp cache management,” IET communications, vol. 6, no. 7, pp. 685–693, 2012.

[53] T. Komori and T. Saito, “The secure dhcp system with user authentication,” in 27th Annual IEEE Conference on Local Computer Networks (LCN). IEEE, 2002, pp. 123–131.

[54] H. Ju and J. Han, “Dhcp message authentication with an effective key management,” World Academy of Science, Engineering and Technology, vol. 8, pp. 570–574, 2007

[55] Z. Duan, X. Yuan, and J. Chandrashekar, “Constructing inter-domain packet filters to control ip spoofing based on bgp updates.” in INFOCOM, 2006.

[56] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, “Accountable internet protocol (aip),” in ACM SIGCOMM Computer Communication Review, vol. 38, no. 4. ACM, 2008, pp. 339–350.

[57] SAMSUNG ELECTRONICS SUSTAINABILITY REPORT 2017 (https://images.samsung.com/is/content/samsung/p5/global/ir/docs/Samsung_Electronics_Sustainability_Report_2017.pdf)

[58] Su, Z., W. Timmermans, Y. Zeng, J. Schulz, V. O. John, R. A. Roebeling, P. Poli et al. "An overview of European efforts in generating climate data records." Bulletin of the American Meteorological Society 99, no. 2 (2018): 349-359.

[59] Hardin, Nicole Valdes. "UNCOVERING THE SECRECY OF STINGRAYS: What Every Practitioner Needs to Know." Criminal Justice 32, no. 4 (2018): 20-24.

[60] Su, Xin, Ziyu Wang, Xiaofeng Liu, Chang Choi, and Dongmin Choi. "Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures." Security and Communication Networks 2018 (2018).

[61] Z. Chen, S. Guo, K. Zheng, and Y. Yang, “Modeling of man-in-the middle attack in the wireless networks,” in Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2255–2258.

[62] Feher, Ben, Lior Sidi, Asaf Shabtai, Rami Puzis, and Leonardas Marozas. "WebRTC security measures and weaknesses." International Journal of Internet Technology and Secured Transactions 8, no. 1 (2018): 78-102.

[63] M. Paik, “Stragglers of the herd get eaten: Security concerns for gsm mobile banking applications,” in 11th Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 54–59.

[64] OpenBTS.org. Openbts — open source cellular infrastruture. [Online]. Available: http://openbts.org

[65] A. N. I. C. Ettus Research. Ettus research - the leader in software defined radio (sdr). [Online]. Available: http://www.ettus.com

[66] H. H. Ou, M. S. Hwang, and J. K. Jan, "A cocktail protocol with the authentication and key agreement on the umts," Journal of Systems and Software, vol. 83, no. 2, pp. 316–325, 2010.

[67] Y. L. Huang, C. Y. Shen, and S. W. Shieh, "S-aka: a provable and secure authentication key agreement protocol for umts networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 9, pp. 4509–4519,2011.

[68] Hwang, Tzonelih, and Prosanta Gope. "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets." *Wireless personal communications* 77, no. 1 (2014): 197-224.

[69] Saxena, Neetesh, and Narendra S. Chaudhari. "NS-AKA: An improved and efficient AKA protocol for 3G (UMTS) networks." In *International conference on advances in computer science and electronics engineering (CSEE'14), Kuala Lampur, Malaysia*, pp. 220-224. 2014.

[70] Saxena, Neetesh, and Narendra S. Chaudhari. "Secure-AKA: An efficient AKA protocol for UMTS networks." *Wireless personal communications* 78, no. 2 (2014): 1345-1373.

[71] Ju, Yong Wan, Kwan Ho Song, Eung Jae Lee, and Yong Tae Shin. "Cache poisoning detection method for improving security of recursive DNS." In *Advanced Communication Technology, The 9th International Conference on*, vol. 3, pp. 1961-1965. IEEE, 2007.

[72] Chopra, Alexander, and Michael Kaufman. "Man In the Middle (MITM) DNS Spoofing Explained." (2014).

[73] Naqash, Talha, Faisal Bin Ubaid, and Abubakar Ishfaq. "Protecting DNS from cache poisoning attack by using secure proxy." In *Emerging Technologies (ICET), 2012 International Conference on*, pp. 1-5. IEEE, 2012.

[74] Kaminsky, Dan. "Black ops 2008: It's the end of the cache as we know it." *Black Hat USA* (2008).

[75] Lindell, Yehuda. "The Security of Intel SGX for Key Protection and Data Privacy Applications." (2018).

[76] Xiang, Lin, Derrick Wing Kwan Ng, Robert Schober, and Vincent WS Wong. "Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks." *IEEE Transactions on Wireless Communications* 17, no. 2 (2018): 736-751.

[77] Zhang, Di, Yuezhi Zhou, and Yaoxue Zhang. "A Multi-Level Cache Framework for Remote Resource Access in Transparent Computing." *IEEE Network* 32, no. 1 (2018): 140-145.

[78] Stiansen, Tommy. "Systems and platforms for intelligently monitoring risky network activities." U.S. Patent 9,923,914, issued March 20, 2018.

[79] Vidal, Chaz, and Kim-Kwang Raymond Choo. "Situational Crime Prevention and the Mitigation of Cloud Computing Threats." In *Security and Privacy in Communication*

Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13, pp. 218-233. Springer International Publishing, 2018.

[80] Stiansen, Tommy, Alfred Perlstein, and Sheldon Foss. "Network appliance for dynamic protection from risky network activities." U.S. Patent 9,942,250, issued April 10, 2018.

[81] Mitseva, Asya, Andriy Panchenko, and Thomas Engel. "The State of Affairs in BGP Security: A Survey of Attacks and Defenses." *Computer Communications* (2018).

[82] Preneel, Bart, and Frederik Vercauteren. "Applied Cryptography and Network Security."

[83] Shulman, Haya. "Implications of Vulnerable Internet Infrastructure." In *Digital Marketplaces Unleashed*, pp. 921-935. Springer, Berlin, Heidelberg, 2018.

[84] Flores, Marcel, Alexander Wenzel, Kevin Chen, and Aleksandar Kuzmanovic. "Fury Route: Leveraging CDNs to Remotely Measure Network Distance." In *International Conference on Passive and Active Network Measurement*, pp. 87-99. Springer, Cham, 2018.

[85] Fernàndez-València, Ramsès, Juan Caubet, and Aleix Vila. "Cryptography Working Group Introduction to Blockchain Technology." (2018).

[86] Hanna, Dalal, Prakash Veeraraghavan, and Eric Pardede. "PrECast: An Efficient Crypto-Free Solution for Broadcast-Based Attacks in IPv4 Networks." *Electronics* 7, no. 5 (2018): 65.

[87] Xie, Michael, Robert A. May, and Jinhai Yang. "Automated configuration of endpoint security management." U.S. Patent 9,894,034, issued February 13, 2018.

[88] Karina, Arellano, Diego Avila-Pesántez, Leticia Vaca-Cárdenas, Alberto Arellano, and Carmen Mantilla. "Towards a Security Model against Denial of Service Attacks for SIP Traffic." *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*12, no. 1: 82-87.

[89] Nath, Ujjual, Gaurav Sharma, and William Fletcher. "User interface for control of personal information privacy." U.S. Patent 9,992,192, issued June 5, 2018.

[90] Hossain, Md Shohrab, Arnob Paul, Md Hasanul Islam, and Mohammed Atiquzzaman. "Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks." *Network Protocols and Algorithms* 10, no. 1 (2018): 83-108.

[91] Sinor, Dale. "Field level data protection for cloud services using asymmetric cryptography." U.S. Patent 9,965,645, issued May 8, 2018.

[92] Weiser, Samuel, Raphael Spreitzer, and Lukas Bodner. "Single Trace Attack Against RSA Key Generation in Intel SGX SSL." In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 575-586. ACM, 2018.

[93] Gunawan, D., E. H. Sitorus, R. F. Rahmat, and A. Hizriadi. "SSL/TLS Vulnerability Detection Using Black Box Approach." In *Journal of Physics: Conference Series*, vol. 978, no. 1, p. 012121. IOP Publishing, 2018.

[94] Gramegna, M., I. Ruo Berchera, S. Kueck, G. Porrovecchio, C. J. Chunnilall, I. P. Degiovanni, M. Lopez et al. "European coordinated metrological effort for quantum cryptography." In *Quantum Technologies 2018*, vol. 10674, p. 106741K. International Society for Optics and Photonics, 2018.

[95] Anagreh, Mohammad Fawaz, Anwer Mustafa Hilal, and Tarig Mohamed Ahmed. "Encrypted Fingerprint into VoIP Systems using Cryptographic Key Generated by Minutiae Points." *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS* 9, no. 1 (2018): 151-154.

[96] Huang, Ling Wei, Hsuan Ling Hsu, and Hsiu Ting Kao. "Method and system for providing tokenless secure login by visual cryptography." U.S. Patent 9,984,225, issued May 29, 2018.

[97] Goodman, Jonathan Lloyd, Hampton Boone Maher, Ravi Komanduri, and Rashmi Kumar Raj. "Multi-processor system and operations to drive display and lighting functions of a software configurable luminaire." U.S. Patent Application 15/211,272, filed January 18, 2018.

[98] Wang, Xiaofeng, Huan Zhou, Jinshu Su, Baosheng Wang, Qianqian Xing, and Pengkun Li. "T-IP: A self-trustworthy and secure Internet protocol." *China Communications* 15, no. 2 (2018): 1-14.

[99] Li, Y., D. Eastlake 3rd, L. Dunbar, R. Perlman, and M. Umair. *Transparent Interconnection of Lots of Links (TRILL): ARP and Neighbor Discovery (ND) Optimization*. No. RFC 8302. 2018.

[100] MAHESWARI, D., A. KAUSHIKA, and A. JENIFER. "A STUDY ON DATA ENCRYPTION AND DECRYPTION USING HILL CIPHER ALGORITHM."

[101] Truedsson, Marc, and Viktor Hjelm. "Situation-aware Adaptive Cryptography." (2018).

[102] Siergiejczyk, Mirosław, and Adam Rosiński. "Analysis of Information Transmission Security in the Digital Railway Radio Communication System." In *International Conference on Dependability and Complex Systems*, pp. 420-429. Springer, Cham, 2018.

[103] Nayak, Nayaneeka, and Rohit Sharma. "Designing security and Surveillance System Using GSM Technology." *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org* 8, no. 4 (2018).

[104] Firdous, G. Shaheen, and R. Sandeep Kumar. "SUPPORT DATA ACCESS ORGANIZE MECHANISM OF RELEASE ENCRYPTION PRIVACY AND SECURITY PROTECTION." *IJITR* 6, no. 2 (2018): 7937-7939.

[105] Hasan, Shiza, Muhammad Awais, and Munam Ali Shah. "Full Disk Encryption: A Comparison on Data Management Attributes." In *Proceedings of the 2nd International Conference on Information System and Data Mining*, pp. 39-43. ACM, 2018.

[106] Jadhao, Ms MM, Mrs SM Gothe, and Mrs SV Nimkarde. "Specific Location Based Privacy protecting Access Control System."

[107] Klink, Jerod, and Herb Little. "Secure access to physical resources using asymmetric cryptography." U.S. Patent Application 15/332,057, filed April 26, 2018.

[108] Lan, Pang-Chang, Tze-Ping Low, and Jangwook Moon. "Precoding-codebook-based secure uplink in LTE." U.S. Patent 9,876,655, issued January 23, 2018.

[109] Rupprecht, David, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Pöpper. "On Security Research towards Future Mobile Network Generations." *IEEE Communications Surveys & Tutorials* (2018).

[110] Mallem, Saliha, and Chafia Yahiaoui. "A Secure, Green and Optimized Authentication and Key Agreement Protocol for IMS Network." In *World Conference on Information Systems and Technologies*, pp. 1108-1118. Springer, Cham, 2018.

[111] Mallem, Saliha, and Chafia Yahiaoui. "A Secure, Green and Optimized Authentication and Key Agreement Protocol for IMS Network." In *World Conference on Information Systems and Technologies*, pp. 1108-1118. Springer, Cham, 2018.

[112] Parne, Balu L., Shubham Gupta, and Narendra S. Chaudhari. "ESAP: Efficient and secure authentication protocol for roaming user in mobile communication networks." *Sādhanā*43, no. 6 (2018): 89.

[113] Hiltunen, Matti A., Emiliano Miluzzo, and Abhinav Srivastava. "Secure multi-party device pairing using sensor data." U.S. Patent Application 15/729,821, filed February 15, 2018.

[114] Kurose, James F. *Computer networking: A top-down approach featuring the internet, 3/E*. Pearson Education India, 2005.