DESIGN AND DEVELOPMENT OF AUTHENTICATION PROTOCOL FOR D2D COMMUNICATION

DISSERTATION-II

Submitted in partial fulfillment of
the Requirement for the award of the
Degree of

MASTER OF TECHNOLOGY

IN

Electronics and Communication Engineering

By

Charanpreet Kaur

(11608625)

Under the Guidance of

Gurjot Singh Gaba

Assistant Professor, L.P.U

School of Electronics and Electrical Engineering
Lovely Professional University
Phagwara, Punjab

December, 2017

TOPIC APPROVAL PERFORMA

School of Electronics and Electrical Engineering

Program : P175::M.Tech. (Electronics and Communication Engineering) [Full Time]

COURSE CODE : ECE620 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** EEERGD0278

Supervisor Name : Gurjot Singh **UID :** 17023 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Charanpreet Kaur	11608625	2016	E1622	8264981509

SPECIALIZATION AREA : Wireless Communication **Supervisor Signature:** _____

PROPOSED TOPIC : Design and development of Authentication protocol for Internet of Things.

	Qualitative Assessment of Proposed Topic by PAC	
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	7.67
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.67
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.67
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	8.33
5	Social Applicability: Project work intends to solve a practical problem.	8.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	8.00

PAC Committee Members		
PAC Member 1 Name: Rajeev Kumar Patial	UID: 12301	Recommended (Y/N): Yes
PAC Member 2 Name: Gurjot Singh	UID: 17023	Recommended (Y/N): Yes
PAC Member 3 Name: Jaspinder Singh	UID: 19601	Recommended (Y/N): Yes
DAA Nominee Name: Amanjot Singh	UID: 15848	Recommended (Y/N): NA

Final Topic Approved by PAC: **Design and development of Authentication protocol for Internet of Things.**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11106::Dr. Gaurav Sethi **Approval Date:** 14 Nov 2017

CERTIFICATE

This is to certify that Charanpreet kaur bearing Registration no. 11608625 have completed objective formulation/Base Paper implementation of the thesis titled, **"DESIGN AND DEVELOPMENT OF AUTHENTICATION PROTOCOL FOR D2D COMMUNICATION"** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of thesis has ever been submitted for any other degree at any university.

Mr. Gurjot Singh Gaba
Assistant professor
School of Electronics and Communication
Lovely Professional University
Phagwara, Punjab

Date:

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude and appreciation to my guide Mr. Gurjot Singh Gaba**,** for his whole-hearted and invaluable guidance, inspiring discussions, encouragement, and support throughout my work. I found him always sincere in helping me even during his busiest hours of the day. His ardor and earnestness for studies are respected and will never be forgotten. Without his sustained and sincere effort, this report would not have taken this shape.

We are also indebted to all authors of the research papers and books referred to, which have helped us in carrying out the research work.

Charanpreet kaur
Date:

DECLARATION

I, Charanpreet Kaur, student of M. Tech under Department of Electronics and Communication of Lovely Professional University, Punjab, hereby declare that all the information furnished in this Dissertation-II report is based on my own intensive research and is genuine.

This report does not, to the best of our knowledge, contain part of my work which has been submitted for the award of my degree either of this University or any other University without proper citation.

Charanpreet Kaur
Date:

ABSTRACT

The Design and Development of Authentication Protocol for D2D Communication is describe the Peer-to-Peer authentication in which it includes client and server. The peer to peer is having the application Device to Device. In which D2D is connect the mobile phones without having the Access Point. The Wi-FI direct is operate on the two techniques if we talk about the Authentication. The techniques are SAS and the Diffie - Hellman in berief it explained in the report.

LIST OF ABBREVIATION

i. **D2D = Device to Device**

ii. **D-H = Diffie –Hellman**

iii. **MITMA = Man In The Middle Attack**

iv. **SAS =Short Authentication String**

v. **C= Commitment Scheme**

vi. **P2P= Peer to Peer**

TABLE OF CONTENTS

Title Page	Page No
PAC	**i**
CERTIFICATE	**ii**
ACKNOWLEDGEMENT	**iii**
DECLARATION	**iv**
ABSTRACT	**v**
LIST OF ABBREVIATIONS	**vi**
LIST OF FIGURES	ix
CHAPTER 1: INTODUCTION	**1-25**
1.1 Peer-To- Peer	1
1.2 Peer-To- Peer Authentication	1
1.3 Challenges in Peer-To-Peer authentication	2
1.4 Peer-To-Peer Authentication application	4
1.5 Need of Security	4
1.6 Model for Network Security	5
1.7 Attacks in security	6
1.7.1Passive Attack	6
1.7.2 Active Attack	8
1.8 Security Measures	12
1.9 Wi - Fi Direct Authentication Communication	12
1.10 Characteristics of Wi-Fi Direct Authentication	13
1.10.3 Diffie-Helman Key Exchange	15
1.10.4 SAS (Short Authentication String)	17
1.10.5 HASH Function	20

1.10.6 Security Concern in peer-to-peer authentication 22
CHAPTER 2: REVIEW OF LITERATURE 26-39
CHAPTER 3: PROBLEM FORMULATION 40
CHAPTER 4: OBJECTIVES 41
CHAPTER 5: RESEARCH METHODOLOGY 42-49
5.1 Diffie hellman algorithm 43
5.2 Diffie hellman man in the middle attack 44
5.3 Short Authentication String 46
5.4 Short Authentication String Man in the Attack 48
CHAPTER 6: RESULT AND DISCUSSION 50-54
CHAPTER 7: CONCLUSION AND FUTURE SCOPE 55
REFERENCES 56-57

LIST OF FIGURES

Figure no.	Figure Name	Page no.
1.1	Peer-To-Peer Communication	1
1.2	Peer-to-Peer Authentication	2
1.3	HandOver	3
1.4	Security Requirement Triad	5
1.5	Model of Network Security	6
1.6	Passive Attack	7
1.7	Eaves Dropping Attack	7
1.8	Traffic Attack	8
1.9	Active Attack	8
1.10	Masquerade Attack	9
1.11	Modification of Message	9
1.12	Replay Attack	10
1.13	Denial of Service	10
1.14	Message Modification Attack	11
1.15	Man In The Middle Attack	11
1.16	SAS based Protocol	14
1.17	Diffie Hellman key Exchnge	15
1.18	Diffie Hellmanperform MITMA key exchnge	17
6.1	Secure Wi-Fi Direct Protocol	49

CHAPTER-1

INTRODUCTION

1. P2P is that network in which IP phones, Inter devices, Management of the Network and it deals only with the wireless network. P2P in fig 1.1 it shows that have many distinguished or different characteristics that is again different from server and client system, which includes the authentication web.

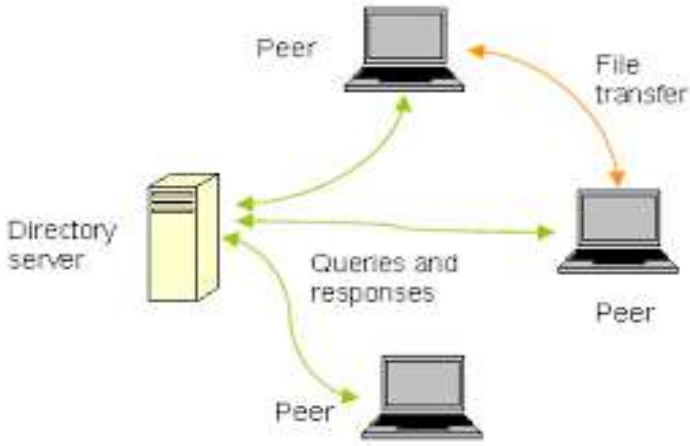

Fig.1.1 peer-to-peer communication [17]

1.2 Peer-To- Peer Authentication:

The latest version of Peer-to-Peer system, which is, manages all the mobility functions in which it involved such function like handover process and the updating of the location. It is the network, which are not mobile client communication. Fig 1.2 is the mobile client or user, which relay on the commands upcoming and the access point recommend it. It can control by the centralized network of the mobile user. If we are talk about the use of this approach it deals with the reduction of complexity in the system and the power contain by the processor of the mobile user. The disadvantage of the client is handover the handover deals with the hard handoff as well as the soft handoff it is cross technology the reason behind the cross technology because the main reason it is not negotiate the handover within the network between client server.

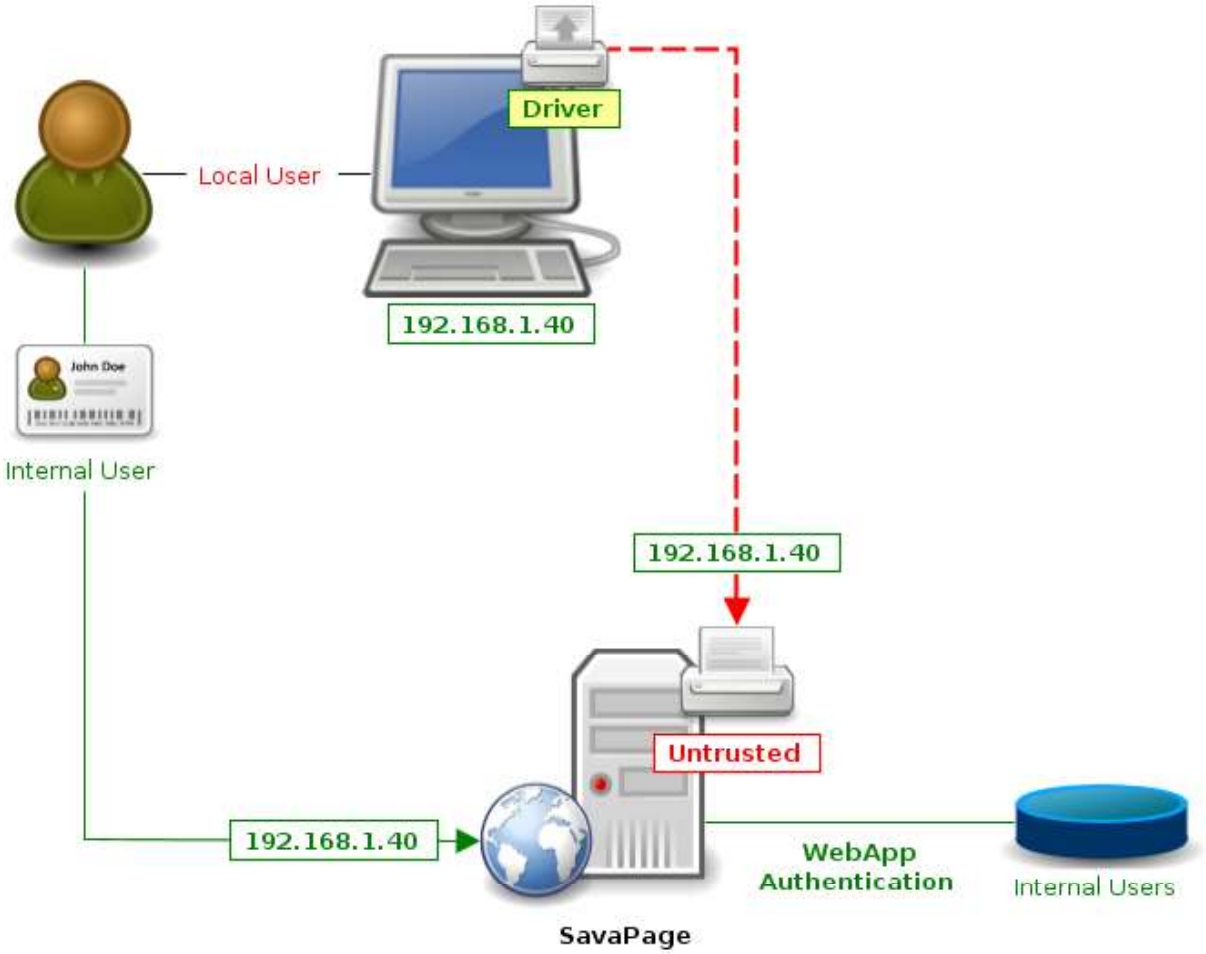

Fig. 1.2 Peer-to-Peer Authentication [17]

The protocol are the client and server member which is additional server for than each peer. There are some different technologies i) Access technology and ii) MAC technologies or client technology initiate from the mobile client have the layer of MAC for technology for the mobile is use. The module of radio is not capable for the working of each and every technology at a time but it can do the 2-3 technologies are work together at the same time. The technologies can be perform soft handoff process from the one access point to the another access point.

The important features of the network is to providing the access information which should be shared with the storage devices. A network is referring to as an efficient [8]network if the data is exchanged reliably, which further means that the intended receiver within the desired time span retaining its authenticity receives the data.

1.1 Challenges in Peer-To-Peer authentication:

The communication sector faces many challenges, which as summarized as:

1) **Handover:** As long as the access network provides an IP Pipe with a unique IP address to each peer, peers can easily perform the handover. For example, let us assume that our peers Peer-A and Peer-B are in a call, and let Peer-B start moving from the UMTS coverage area to WLAN coverage shown in fig.1.3. The mobile client maintains more than one IP addresses (one for each IP stack), and the P2P Mobility Layer sees each one of these IP stacks as one IP Pipe [3]. The mobile client maintains more than one IP addresses (one for each IP stack), and the P2P Mobility Layer sees each one of these IP stacks as one IP Pipe.

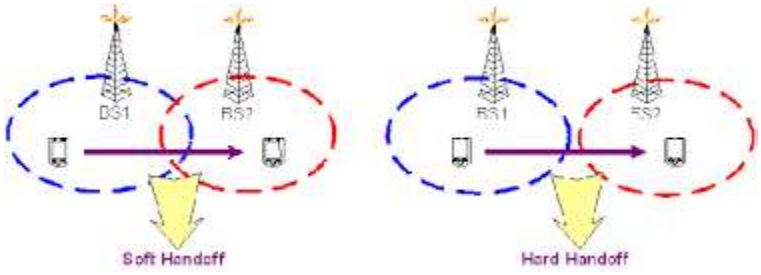

Fig1.3Hand over [18]

2) **Finding the IP Address:** In order to find another peer, there has to be a piece of shared knowledge between these peers: a fixed IP address that belongs to a Lookup Server on the Internet. For example, when Peer-A wants to initiate a call to Peer-B, it should first contact the Lookup Server and ask for Peer-B's current IP address. Of course, Peer-B should be updating the Lookup Server with its new IP address every time it moves to a new IP Pipe. In addition, during the handover, Peer-B should update the Lookup Server with both IP addresses that Peer-B is currently [13] using, so that any peer trying to setup a connection to Peer-B will be able to find Peer-B.

3) **Security:** The primary task of utilities is to maintain high levels of security. Any enhancement to this infrastructure therefore made with reliability uppermost in mind. The security here is a broad term, which includes integrity, confidentiality and authentication.

1.2 Peer-To-Peer Authentication application

Peer to peer networks are of two types depending upon the type of links between the devices: wired or wireless. P2P Networks find their application in various areas. Applications of wireless communication involve security systems, Wi-Fi, Wi-Fi DIRECT, mobile communication (Device to Device (D2D)), microwave communication, infra red communication, wireless power transfer, computer interface devices, satellite communication and radio broadcasting. Wired communication includes optical fiber communication, Local Area Network, Ethernet etc.

Each peer is nothing but a mobile client with a few additional members in its protocol stack. First, the mobile client should have one MAC layer for each different access technology that this mobile is going to use. Likewise, the radio module in the device has to be not only capable of working with each technology, but also capable of working with two or more of these technologies at the same time so that we can perform a soft-handover from one technology to another. One way of solving this problem is having an individual radio circuitry for each technology. Another solution, which is preferable when we have a large number of access technologies, is using software-defined radios (SDR). The number of SDRs required is equal to the maximum number of legs we want to maintain during a soft-handover.

Secondly, the mobile should also have a separate TCP/IP protocol stack for each MAC layer so that we can maintain multiple IP addresses simultaneously. A new protocol layer, called P2P Mobility Layer, is placed at the session layer, above the TCP/IP layers. All mobility functions are negotiated and executed by the P2P Mobility Layers in the peers.

1.1.1Need of Security:

Security of the data becomes most important concern in order to avoid an unauthorized or unintended access. It includes physical security to prevent theft to the network equipment's from the opponent and information security to prevent any sort of data theft. The three trails are shown in fig.1.4. There are mainly three objectives in security provisioning:

● **Confidentiality**: It assures that the private information transmitted by the source is not disclosed to any unauthorized individuals. It also ensures privacy that the specific user will influence or collect only the data that are relate to him.

● **Integrity:** It assures that the information at the receiver is change only according to the authorized access. It ensures that the data have not being altered; the final output at the receiver end is changing according to the specified algorithm or by an authorized party.

● **Availability**: It assures that the system is working properly and service to the authorized user have not been denied.

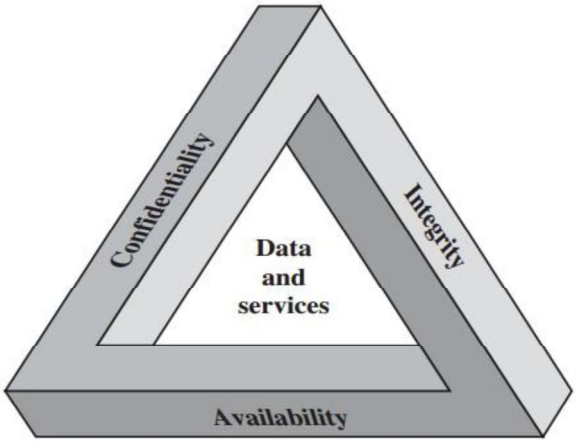

Figure 1.4 Security Requirements Triad

1.1.2 Model for Network Security:

A message is transmitted by a source on a wired or wireless channel towards the destination. Routing process has been taken care of by using certain routing protocols depending on the constraints with respect to the environment in which the network fig1.5 has been established (e.g. TCP/IP). Security comes into role when it becomes necessary to protect data from the intruders. This can be done by various methods such as by encrypting a message or by adding additional code into the original message or by assigning different secret keys to both sender and receiver. By doing this attacker or any other third party is unable to decrypt the original message content [1].

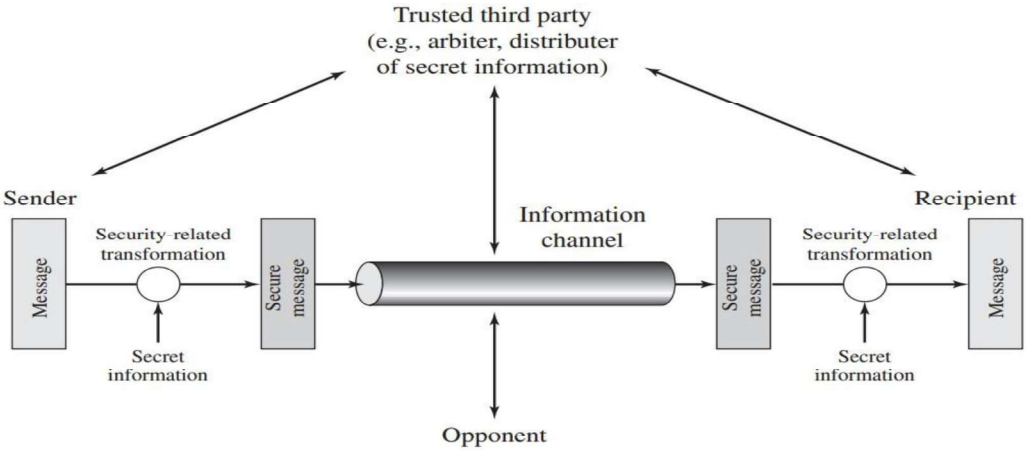

Figure 1.5 Model for Network Security

This model performs following tasks:

(i) Design such algorithm for security related transformation, which is complex, so that the intruder is unable to break it.

(ii) Generate some secret information and also add it to the original message.

(iii) Develop efficient methods for sharing and distribution of secret data.

Security against various attacks is required to ensure reliability. Attacks are classified into two categories:

1.2.1Attacks in security

1.2.1(A) Passive Attacks:

In passive attacks, an opponent or an unauthorized member can monitor and listen to the communication between authorized members, passive attacks fig.1.6 are basically attacks against the privacy of the data, and it does not affect the system resources. This monitoring and listening to the transmissions by opponent can cause insecurity to data or even entire network, because by continuously monitoring opponent can easily examine many other factors like topology of network and position of the authorized members[2].

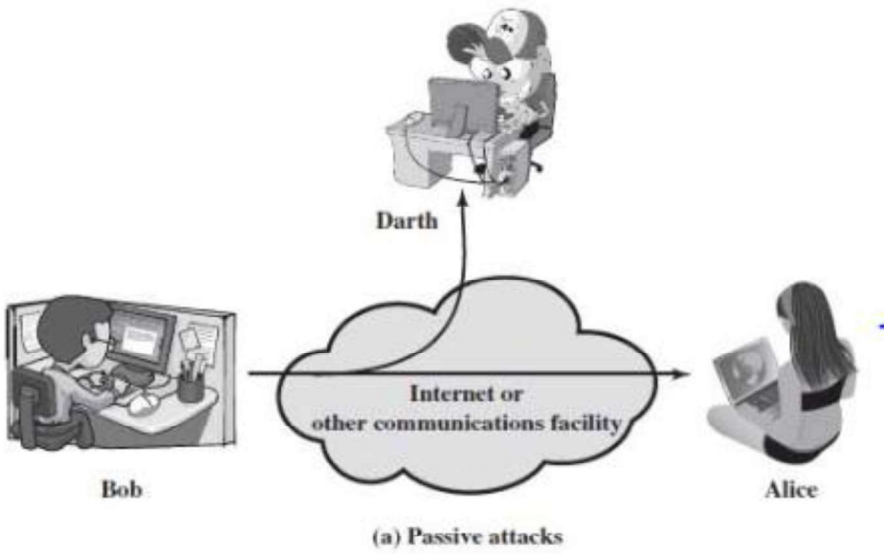

Fig. 1.6 Passive Attack[17]

Different types of passive attacks are as follows:

(a)Eavesdropping: In this type of attack the opponent continuously investigates the communication occurring between various members of the given network, fig. 1.7opponent can easily find out data contents, by secretly listening to the conversation going on between various authorized members, opponent can easily get much information about the entire network, and it can effect privacy protection [10].

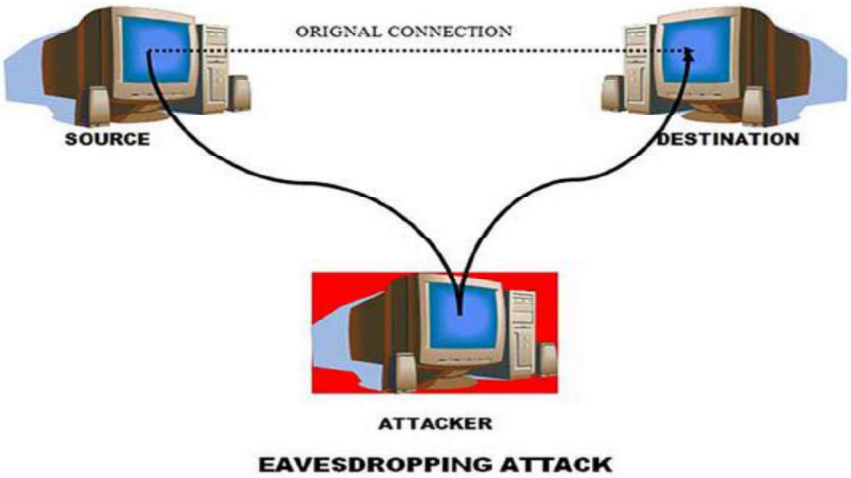

Fig.1.7 Eaves dropping attack [17]

(b)Traffic Analysis: When data is transfer from one member to another,fig.1.8 it leaves many information for opponent (even if it is in encrypted form), because when communication occurs opponent can easily analyze the communication patterns, and this information is sufficient for an opponent to cause harm to the entire network [2].

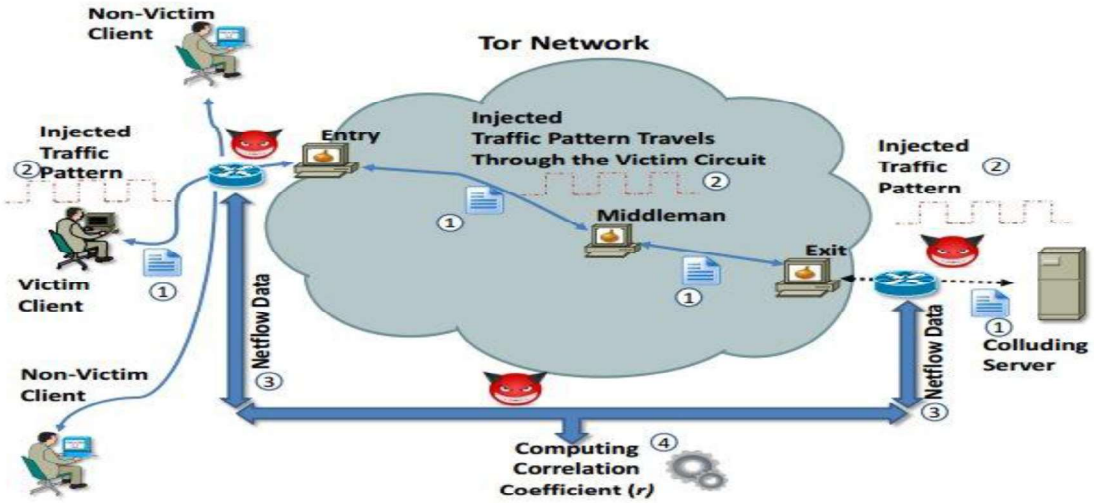

Fig. 1.8 Traffic attack [17]

1.2.1(B)**Active Attacks**:

In case of active attacks, an opponent or an unauthorized member can monitor and listen to the communication between different authorized members. Active attacks modify the data stream in communication channel and they can also affect system resources. Different types of active attacks are as follows:

Fig. 1.9 Active attack [17]

(a)Masquerade: It includes insertion of message into an given network from a false or fraudulent source, this insertion of message behaves as it comes from an authorized member. Masquerade basically occur when one specific entity start behaving as other different entity [1].

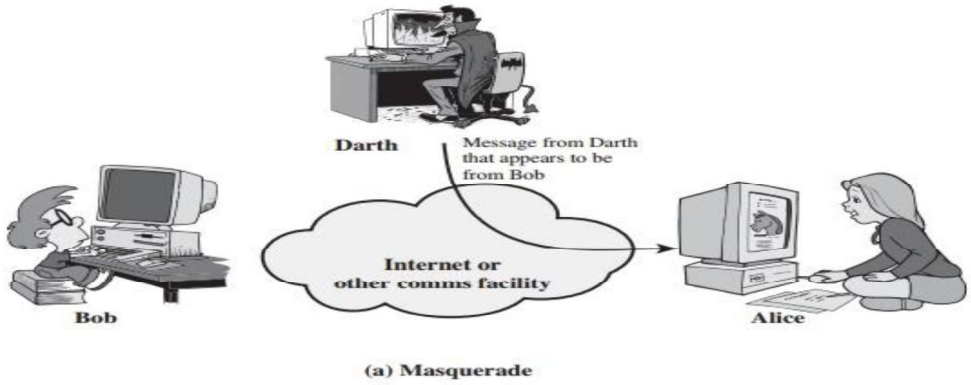

Fig. 1.10Masquerade Attack [17]

(b)Modification of Message: It includes the alteration in the original message contents by an unauthorized access of opponents. Sometimes message can be delayed also to produce an unauthorized effect [10].

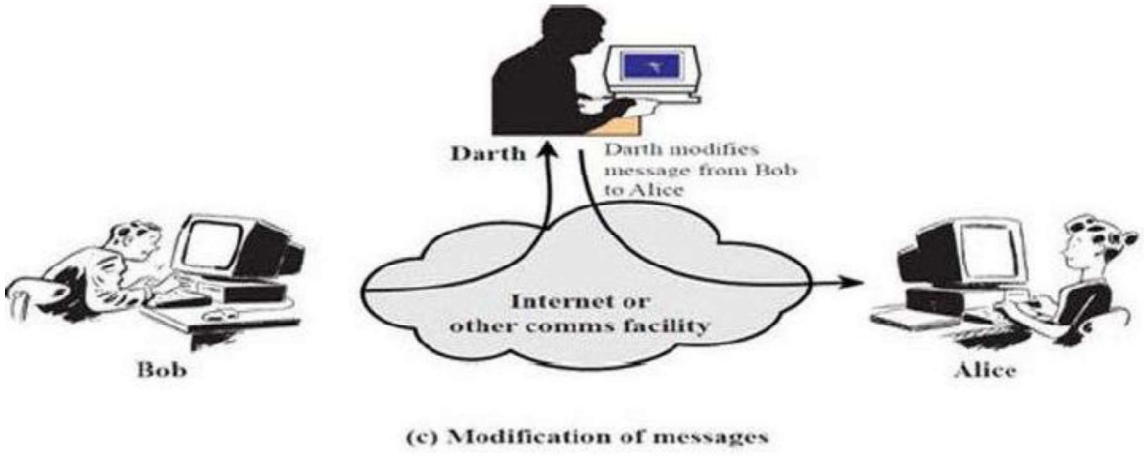

Fig.1.11 Modification Attack[17]

(c)Replay: It includes the passive capturing of a data unit and then its subsequent retransmission in order to waste the system resources.

Fig. 1.12 Replay Attack [17].

(d)Denial of Service: It may lead to the disruption of an entire network due to the unavailability of system resources, or by disabling the network, or by overloading the network with messages so as to degrade its performance.

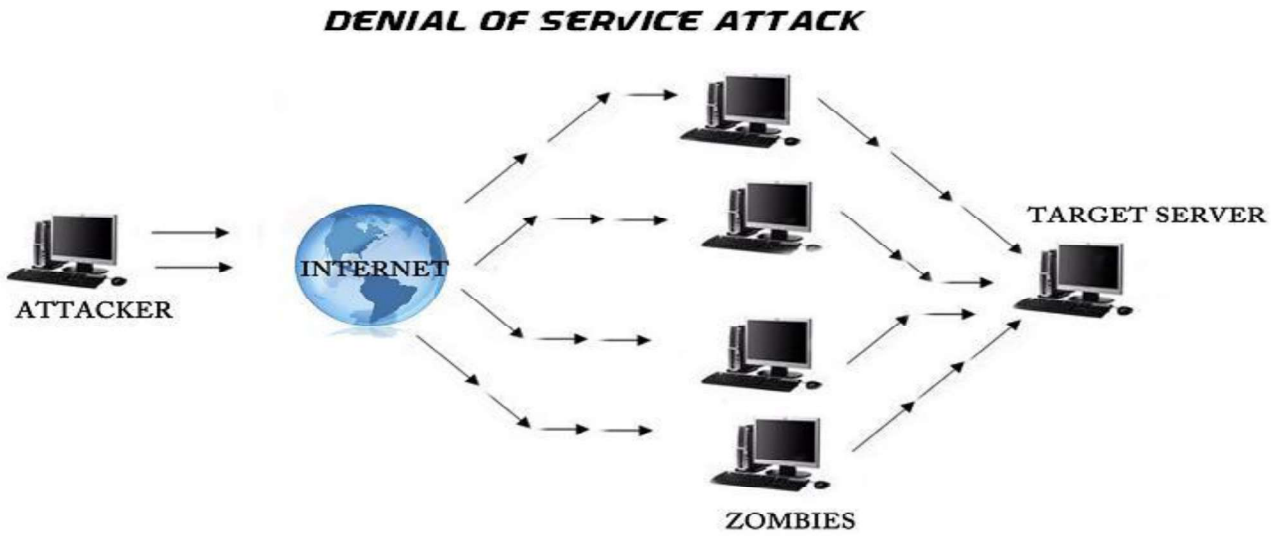

Fig.1.13 Denial of service [17].

(e)Message Modification: To modify ongoing traffic without being noticed by legitimate users is much more difficult but still possible. By using advanced full duplex radio techniques, the attacker is able to receive and transmit signals simultaneously. When the attacker captures ongoing traffic between the transmitter and the receiver, he/she immediately impersonates the transmitter, modifies the message payload as his/her wish, and sends the modified message to the receiver using a directional antenna at significantly higher power, producing a capture effect. In such a case, the receiver will only decode the modified message, while the transmitter has no idea that there is an impersonation going on due to the

directional antenna the attacker uses. Apart from the aforementioned three basic attack modes, WiFi Direct communication faces some other, more sophisticated potential security threats. These security threats either take advantage of the protocol defects or are combinations of the basic attack modes.

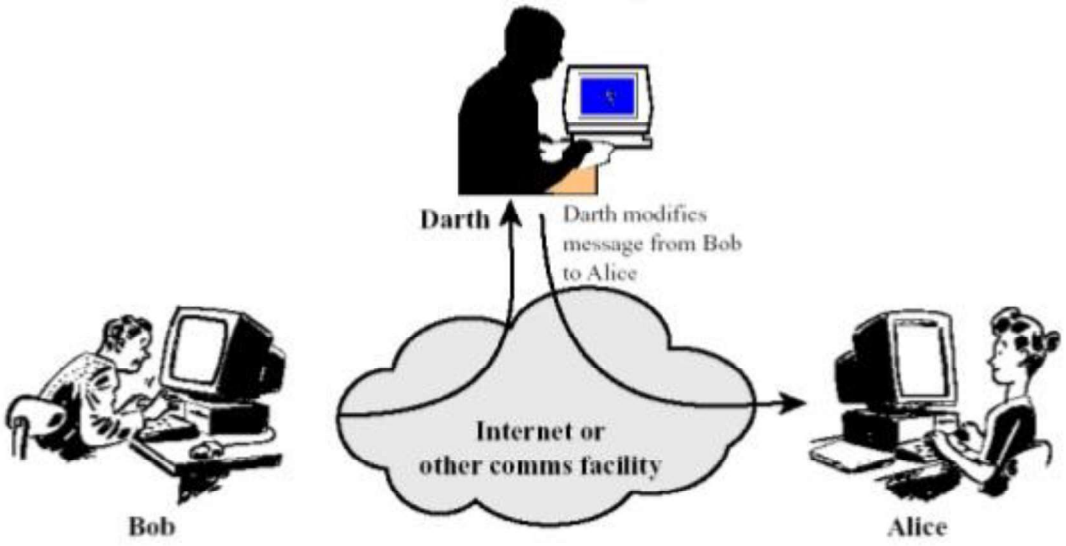

Fig.3.8

Fig.1.14 Message modification attack [17]

(f)Man In The Middle:

MIMTA is a well-known attack in wireless communications, in which the attacker makes independent connections with legitimate users, and relays and modifies the messages between them to make them believe they are talking directly to each other over a private connection. However, the entire communication is under the attacker's control. To avoid detection by legitimate users, the attacker needs to intercept the original communication messages and forge new ones, similar to the above message modification and impersonating attacks. To defend against MIMTA, mutual authentication is required.

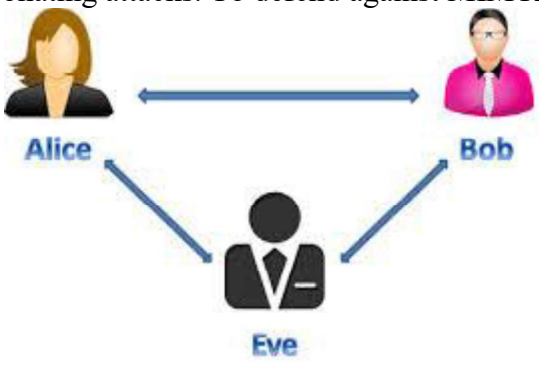

Fig.1.15 Man In The Middle Attack[17]

1.3.1 Security Measures:

In order to prevent entire network system from above discussed attacks, various techniques are available such as:

- **Data Integrity:** It provides protection to original message content from being modified by any unauthorized party. It ensures us that data has not been altered; the final output information received at the destination is changed according to the specified algorithm or by an authorized party only.

- **Data Confidentiality:** It assures that the information transmitted on a wired or wireless channel have not been disclose to any unauthorized user. A basic key component for attain confidentiality would be encryption using public key and decryption using private key.

- **Encryption:** It assures for the secure communication, because by applying this technique in the network, only the authorized user or a user having a right secret key can be able to read the original message content. There are different types of encryption schemes, which exist such as Public key encryption and Symmetric key encryption. Encryption helps to achieve data confidentiality among neighbors.

- **Authentication:** It refers to a process of actually confirming about an authorized user. It is a special case of data integrity, it assures that the entity to which an authorized user wants to interact or start communication with, is also an authorized user.

- **Availability**: It assures that the system resources are sufficient for the effective communication and service to an authorized user have not been denied throughout the entire life cycle of the network [2, 3].

1.4 Wi - Fi Direct Authentication Communication

D2D communications facilitate proximal devices to directly communicate with each other, bypassing cellular base stations or access points, and bring many benefits such as improvement in both spectral efficiency and energy efficiency. Among existing D2D enabling techniques, the recently released WiFi Direct is one promising protocol that offers high data rate D2D communications in local areas.

However, WiFi Direct is susceptible to security threats due to the open access of wireless channels and lack of security infrastructures. In this article, we identify several attacks that challenge WiFi-Direct-based D2D communications. Since pairwise key establishment lies in the area of securing D2D communications, we introduce a short authentication-string-based key agreement protocol and analyze its

security performance. We also integrate the SAS-based key agreement protocol into the existing WiFi Direct protocol, and implement it using Android smartphones.

1.4.1 Characteristics of Wi-Fi Direct Authentication:

The Wi-Fi Direct protocol enables two devices to establish a D2D connection without the help of APs. Figure 1 shows the procedure for D2D connection establishment using Wi-Fi Direct. First, two devices perform channel probing and discover each other. Then they negotiate to determine the group owner (GO), which operates as an AP for this D2D connection in a voluntary or random manner. During the handshake process, each device sends a GO intent value, and the device with the highest value becomes the GO. After the devices have agreed on their respective roles, the GO initiates the Wi-Fi security setup using WPS, and conducts a Dynamic Host Configuration Protocol (DHCP) exchange to set up the IP addresses for both devices.

Thus, the D2D connection between these two devices is established. Wi-Fi Direct is built on the IEEE 802.11 infrastructure mode, and thus can be seamlessly implemented by legacy Wi-Fi devices. Besides, Wi-Fi Direct inherits the features of traditional Wi-Fi, including QoS, power saving, and security mechanisms, and has the capability of forming a more stable and secure D2D underlying network than traditional ad hoc networks. Two typical Wi-Fi Direct application scenarios are-

• Two (or multiple) devices form a local ad hoc network. Messages and files can be shared among this network at no extra cost. This is particularly useful when there is no cellular connection or AP available.

• By Wi-Fi Direct, a cellular-enabled device can share its Internet connection with other devices.

1.4.2 Wi-Fi Direct Protocol:

In the literature, there are few studies on the security aspect of D2D communications. In this article, we discuss the security challenges and identify a number of attacks for D2D communications with WiFi Direct, for example, man-in-the-middle attack and DoS. Pairwise key establishment lies in the kernel for securing D2D links. With the established secure key, a variety of cryptographic encryption algorithms can be implemented to secure D2D communication fig1.1.7 . To this end, we introduce a short authentication-string-based key agreement protocol. We implement the proposed protocol for file sharing

applications in a real system using Android smartphones. Experiments validate the efficiency and effectiveness of the proposed protocol.

The remainder of this article is organized as follows. The following section introduces WiFi Direct. Security challenges are then discussed. Next, we present the proposed key agreement protocol and the experiment results.

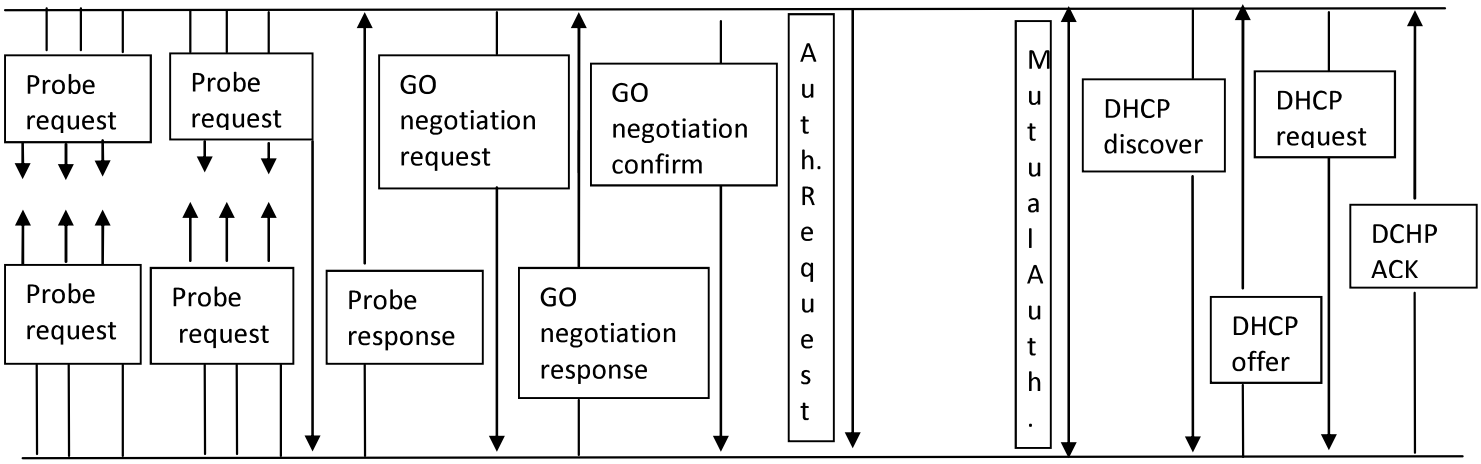

Fig. 1.16 SAS based protocol

Such a paradigm shift from two-hop communications to one-hop ones can bring many benefits such as spectral efficiency improvement, energy saving, and delay reduction. Without the need for infrastructure, D2D technology facilitates mobile users sharing instant information (e.g., pictures and videos) with each other even in areas out of cellular coverage or with no AP [4]. It is becoming an important enabling technology for mobile social networks [5] so that friends in the vicinity can be automatically identified and paired up for direct communications. Moreover, it is evolving to enable so-called mobile ad hoc clouds, which exploit untapped resources of a number of proximal devices to provision cloud services such as data and computation offloading.

Without a trusted infrastructure such as an AP, it is the D2D users' responsibility to secure their communications and protect their sensitive data from various kinds of attacks.

1.4 WiFi Protection Setup (WPS) mechanism inherited from the WiFi specification, WiFi-Direct-based D2D communications cannot be spared from those security challenges. Attacks (e.g., denial-of-service [DoS]) are difficult to prevent with WPS [8]. Moreover, studies have shown that WPS has its own security holes, which can be leveraged by smart adversaries to establish unsafe D2D links. With the proliferation of smartphones and great potential demand for D2D communications, security protection mechanisms are urgently needed.

Further, to strengthen the bond of security two different random number generators respectively generate a Wi-Fi. These Random number generators are explained as:

1.4 Diffie-Helman Key Exchange:

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly, we can define the discrete logarithm in the following way. First, we define a primitive root of a prime number *p* as one whose powers modulo *p* generate all the integers from 1 to *p* 1. That is, if *a* is a primitive root of the prime number *p*, then the numbers

A mod p, a2 mod p,..., ap1 mod p

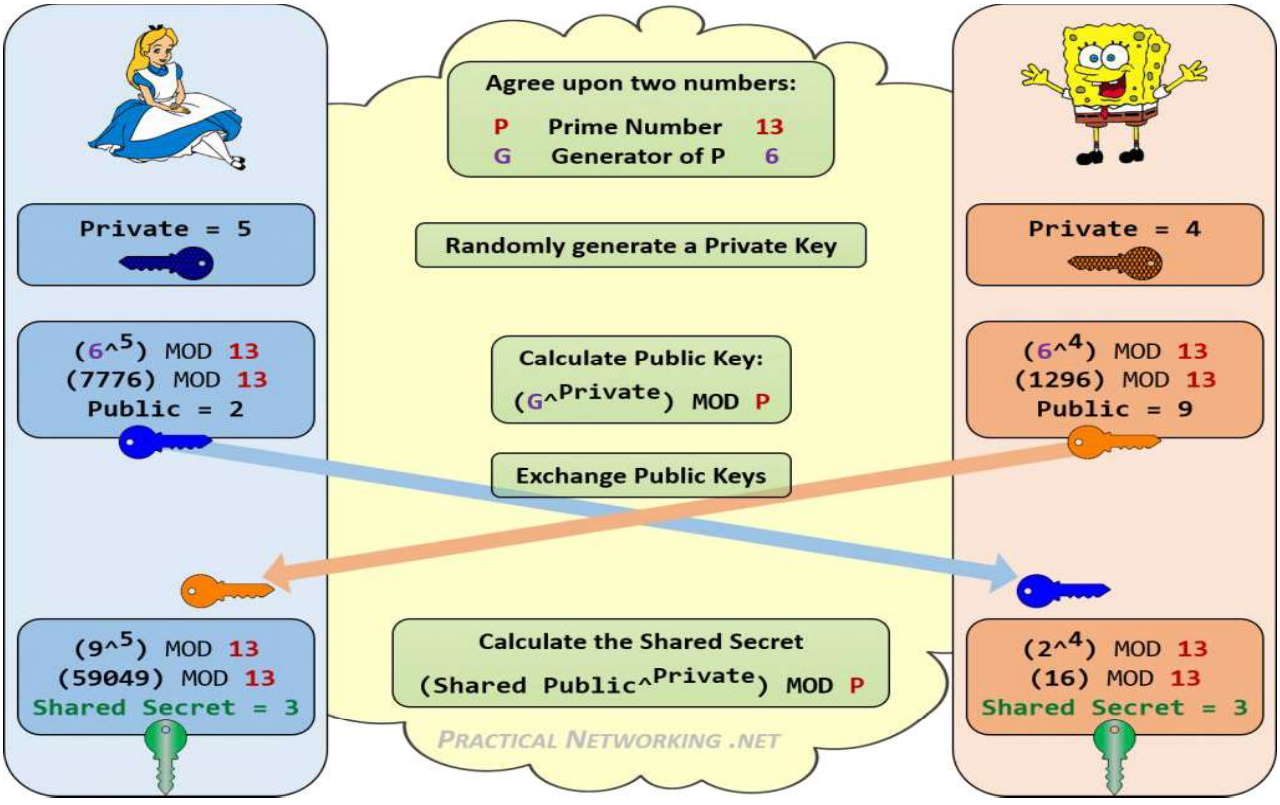

Fig.1.17 Diffie Hellman key exchange

There are two publicly known numbers: a prime number q and an interger that is a primitive root of q. Suppose the users A and B wish to exchange a key.

User A selects a random integer

$X_A<q$ compute $Y_A= aX_A \bmod q$;

Similarly, user B independently selects a random integer

$X_A<q$ compute $Y_B= aX_B \bmod q$;

Each side keeps the X value private and makes the Y value available publicly to the other side.

User A computes the key as

$K =(Y_B)X_A \bmod q$ and

user B computes the key as

$K=(Y_A)X_B \bmod q$

These two calculations produce identical results:

$K = (Y_B)X_A \bmod q$

$= (aX_B \bmod q)X_A \bmod q$

$= (aX_A)^{\wedge XB} \bmod q$

$= (aX_A \bmod q)$

$= (aX_A \bmod q)^{\wedge XB} \bmod q$

$= (Y_A)^{\wedge XB} \bmod q$

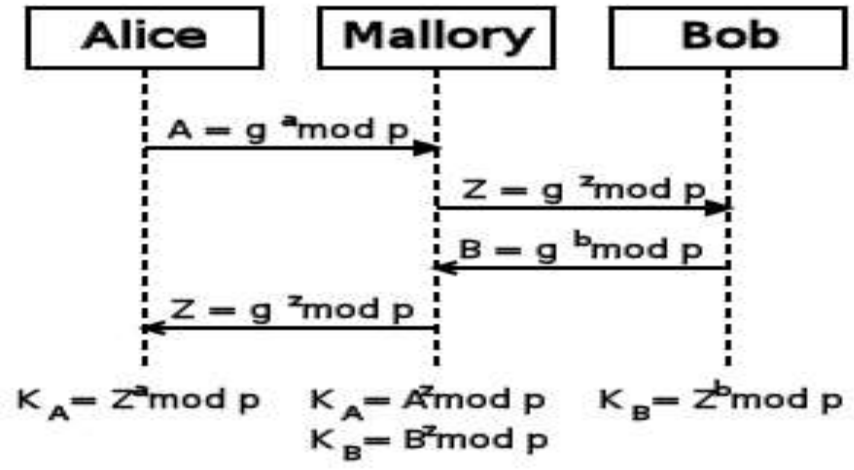

Fig.1.18 Diffie Hellman perform man in the middle attack.

The protocol depiceted in fig 1.1.9 I insecured against in a man in the middle attack. Suppose Alice and Bob are ready to exchange the keys and Mallory is the attacker. The attacker processed in the following steps:

1. Mallory prepare for the attack by generating two random private key X_{D1} and X_{D2} and it computing the corresponding public key Y_{D1} and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Mallory also calculates $K_2= (Y_A)^{XD2}$ mod q.
4. Bob receives Y_{D1} and calculates $K_1= (Y_{D1})^{XB}$ mod q.
5. Bob transmits Y_B to Alice.
6. Mallory intercepts Y_B and transmits Y_{D2} to Alice. Mallory calculates $K_1= (Y_B)^{XD1}$ mod q.
7. Alice receives Y_{D2} and calculate $K_2= (Y_{D2})^{XA}$ mod q.

1.5 SAS (Short Authentication String):

The short authentication string (SAS) based key agreement protocol utilizes a cryptography commitment scheme. A commitment scheme enables one to hide a chosen value through a commit operation, transforming this value into a commitment/opening pair. Anyone who obtains this pair of values is able to reveal the committed value deterministically via an open operation. The commitment value alone, however, leaks no information about the hidden value. An efficient construction of a commitment scheme can be achieved by using a cryptographic hash function [14].

Commitment Scheme:

The commitment scheme is depend upon the CRS model (common reference string model). Captures the assumption that a trusted setup. In which all involved parties get access to the same string CRS taken from the some distribution D exists. Scheme proven secure in the CRS model are secure given that the setup was performed correctly. The CRS model is a generalization of a common random string model, in which D is the uniform distribution of bit string. The CRS model is equivalent to the refrence string model and the public parameter model.

P→V: commitment random string of length p(n).

V→P: send random string length p(n).

P→V: opens up the commitment.

Our protocols are based on commitment schemes. They are used to commit on an arbitrary non-hidden message *m* together with a hidden *k*-bit string *r*. We formalize them by three algorithms. setup which generates a random parameter *KP* (which is used by all other algorithms and omitted from notations for simplicity reasons) and a secret key *KS*. commit(*m*; *r*) which takes a message *x*=*m*jj*r* and produces two strings: a *commit* value *c* and a decommit value *d*. Here, we consider that *x* includes a part *m* which is not meant to be hidden and a part *r* which is a hidden *k*-bit string.

We can call *m* a tag for the commitment so that we have a *tag-based commitment* to *r*. Note that this algorithm is typically non deterministic. open(*m*; *c*;*d*) which takes *m*, *c*, and *d* and yields a message *r* or an error signal. We require this algorithm to be *deterministic* and to be such that whenever there exists *r* such that (*c*;*d*) is a possible output for commit(*m*; *r*), open(*m*; *c*;*d*) yields *r*. Note that the setup plays no real role so far. It is used in extensions of commitment schemes. We keep it anyway to have de£nitions well suited to all kinds of commitment schemes that will be used. Commitment schemes have two security properties.

– (*T*; e)-*hiding*: no algorithm *A* bounded by a time complexity *T* can win the following game by interacting with a challenger *C* with a probability higher than 2¡k+e.

1. C runs setup and sends KP to A.
2. A selects a tag m and sends it to C.
3. C picks a random r, runs commit on (m; r), gets (c;d), and sends c to A.
4. A yields r0 and wins if r = r0.

When $T = +¥$ and e = 0, we say that the scheme is *perfectly hiding*. – (*T*; e)-*binding*: no algorithm *A* bounded by a time complexity *T* can win the following game by interacting with a challenger *C* with a probability higher than 2¡*k*+e.

1. *C* runs setup and sends *KP* to *A*.
2. *A* selects a tag *m* and sends it to *C*.
3. *A* selects a *c* and sends it to *C*.
4. *C* picks a random *r* and sends it to *A*.
5. *A* computes a *d* and wins if (*m*; *c*;*d*) opens to *r*.

When $T = +¥$ and e = 0, we say that the scheme is *perfectly binding*. Commitment schemes can be relative to an oracle, in which case all algorithms and adversaries have access to the oracle. However, they have no access to the complete history of oracle calls. Extensions of commitment schemes have extra algorithms which do have access to this history.

Extractable commitment: In this extension of commitment schemes, there is an additional deterministic algorithm extractKS (m; c) which yields r when there exists d such that (m; c;d) opens to r. When using oracles, this algorithm is given the history of oracle queries. Clearly, extractable commitments are perfectly binding. Adversaries playing the hiding game can make oracle calls to extract, except on the committed m tag.

Equivocable commitment. In this extension of commitment schemes, there are two algorithms simcommitKS (m) and equivocateKS (m; c; r;x). simcommit returns a fake commit value c and an information x, and equivocate returns a decommit value d such that (m; c;d) opens to an arbitrary r for (c;x) obtained from simcommit. For any KPjjKS and any m, the distribution of fake commit values is assumed to be identical to the distribution of real commit values to any r with tag m. From this we deduce that the commitment is perfectly hiding. Adversaries playing the binding game can make oracle calls to simcommit and equivocate, except on the committed m tag, and are assumed not to see x. Namely, the equivocate oracle works only if there was a matching oracle call to simcommit before, and gets x directly from the history. In our paper, we further assume that adversaries are limited to a single query to simcommit and equivocate. This is a quite restrictive assumption, but it will be enough for our purpose.

1.6 Cryptography HASH Function:

The common algorithms used for security applications were Secure Hash Algorithms; SHA-l and SHA-2. Due to someThese also are good cryptographic pnrllltlves. The hash functions transform the variable input length into a fixed one. Their main applications include digital signatures and message authentication codes. For this they are required to meet some properties of security which have:

(i) Preimage resistance, i.e., for a given f (x) it is infeasible to find x,
(ii) Second preimage resistance, i.e., for a given x it is infeasible to find xl _ x : f (x) = f(xl), and
(iii) Collision resistance, i.e., it is infeasible to find x, xl : xl _ x and f(x) = f(xl).
(iv) A collision resistant hash function is the one for which it is impossible to find two distinct messages ml and m2 which can produce the same hash or which is called the message digest.

1.6.1 Significance of HASH

A hash function is a function, which used to map the data of different size into the fixed size. The value return from the hash function is known as hash value, hash code or hashes. Hash functions are related to fingerprints, lossy compression, error correction, codes and cipher.

A MAC algorithm, sometimes called a keyed (cryptographic) hash function (which is somewhat misleading, since a cryptographic hash function is only one of the possible ways to generate a MAC), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

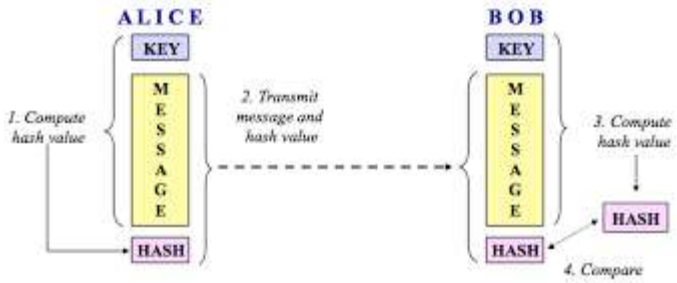

Fig.1.19 Cryptography Hash Function Value

A keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key. As with any MAC, it might be use to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, might be use in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, also on the size and quality of the key [2].

1.6.2 Effectiveness of Data Integrity:

In order to maintain data integrity or to maintain the secure transmission of information in hostile environment different security measures such as authentication, encryption, decryption, etc processes are used, where encryption and decryption provides confidentiality and it hides or protects the original message contents from adversaries, whereas authentication verifies that weather the sender is an authorized member or not and by combining both of the above schemes we have attained data integrity. For maintaining data integrity different Hash Algorithms, Message Authentication Codes (MAC), Digital Signatures and various Encryption techniques have been used.

Integrity refers to a Message Authentication. Authentication is of two types:

Source Authentication: It assures the receiver that the sender node is an authorized member of a network.

Message Authentication: It assures that data received at the receiver node has been fresh and has not been altered by any intruder.

Effectiveness of data integrity is explained as:

- Data Integrity refers to the consistency and accuracy of information transmitted over an unfriendly environment over its entire life cycle. It ensures that data is recorded exactly as intended. It prevents unintentional changes to the original message content.
- Any unintended change to data because of retrieval or processing operation, human error, unexpected hardware failure, including malicious node and storage will lead to failure of data integrity.

- It ensures that the data received by the cluster head or any other sensor node does not alter or it has not been tampered or harmed by any attacker node. The integrity of the network is very important in case of WSNs because sometime an attacker may add false node that starts generating false data, then in that case it plays very important role.

- Data Integrity can be implemented in WSNs by using different types of hashing functions or hashing algorithms

- In order to ensure data integrity, various hashing algorithms are available. Hash function simply maps an input of arbitrary length to a fixed output by using a noninvertible compression function. Hash functions are very hard to reverse, due to which they have been used for providing security services such as data integrity, origin authentication. They are widely used in applications such as secure email, digital signatures, VPN (Virtual private Network), electronic voting, e-commerce and digital cash. Hash functions are more efficient than cryptographic primitives such as symmetric and asymmetric ciphers [4].

1.7 Security Concern in peer-to-peer authentication

Despite all the benefits of D2D communications, security is one of the major concerns that need to be well addressed before D2D technique gets widely accepted and implemented. It is well known that due to the broadcast nature of wireless channels, wireless communication such as Wi-Fi and Bluetooth is vulnerable to a variety of attacks that challenges the three basic principles of security–confidentiality, integrity and availability. Some common attack vectors include surreptitious eavesdropping, message modification and node impersonation. For example, by stealthy listening to the communication between two devices, an attacker can gain critical or privacy information, such as trade secrets or identity related information. Thus, the D2D communications between devices need to be properly secured.

To secure the D2D communications, cryptography solutions are needed to encrypt the messages while they are transmitted via wireless channels. Numerous encryption algorithms have been well developed which can provide different security levels for the encrypted messages, but all of them require two devices agree on a shared secret (either a shared secret key or each other's public keys). Due to the large number of mobile devices, the diversity of device manufacturers and lack of standards, preloading secure

keys into mobile devices is neither efficient nor practical. On the other hand, a trusted third party or infrastructure is not likely to be available in the D2D mobile environment.

Thus, how to establish a shared secret between devices is one of the main challenges for secure D2D communications. One straightforward way to establish a shared secret between two devices is that the two end users of the D2D link interactively set up a secret key via human negotiation (such as making a phone call if they are in distance). The problem for this is that the shared secret established by human interaction will be too weak in most cases. The attackers do not even need to be smart to crack this weak secret via brute force method, considering current computation power. To deal with this issue, cryptologists and researchers come up with two types of approaches which enable two individuals to establish a secure enough secret key: Diffie-Hellman key establishment protocol and secret key extraction from physical channel characteristics.

Physical layer based secret key generation methods have been proposed in recent years as alternative solutions for traditional Diffie-Hellman key agreement protocol. Unlike Diffie- Hellman key agreement protocol, whose security is guaranteed by the computational hardness of discrete logarithms, these physical layer based methods rely on the randomness and uniqueness of wireless fading channel properties: temporal variation, spatial variation and reciprocity. Generally, the two devices first send channel probing packets to measure the physical metrics of the wireless channel, then after using quantization and error correction technique, these two devices can yield the same secret key. The main problem for this type of methods is that the secret key generation rate is in most case very low. Users have to send lots of channel probing packets to achieve a secret key with enough bits and randomness. The communication overhead and relatively longer key generation time are not quite desirable for the case of D2D communications.

CHAPTER-2
REVIEW OF LITERATURE

The smart application of the smart phones and the tablets are generate the maximum traffic in the new generation of the smart and the android phones. The device - to – device is reducing the traffic flows and converse the bandwidth that help to increase the QoS. The technology is enhanced to build the wireless connection for the two parties, it is directly interfacing, and it is not interface without access point. The main improvement of the techniques [2] is the limited or specific power consumption. The power consumption is consumed the power of uplink and downlink with the nearby access points or base stations. Device-to-Device communication is having same frequency band by the Wi-Fi direct. The entity is only required for the authentication of the user which help to access the network. This basic principle is relay on the key exchange protocol of the system [5].

The principle of the system is grid on the research issues, which is electric vehicle, and the ecosystem, which is based on the smart grid latest issue. The vehicle of the system is helps to find the locations of the vehicle and helps to find the identity of the vehicle owner. However, the disadvantage of this system it work only when the system is connected to the power system. To declare the identity of the user it uses the standard like ISO/IEC15448. The simple method of identifier the reliable method is used [4].
The authentication method in the smart grid, which is having the authentication salient features of the signal in the grid. The P2P (Peer-to-Peer) communication the authentication is provided by the devices although the IBC protocol systems [1].

Email is the application of the IBC entity. The author is eliminates the public key as the user or author wants to sharing the data. With the requirements of the data it is eliminates the public keys [8]. Authentication is the major role of cryptography without authentication it is consumes the data as crypt. To check the authenticity of the user it can analyze the authentication to the user. The user have two different types of authentication:
i) Mutual Authentication.
ii) Unilateral Authentication.

At the same time the user is authenticate with the two kinds of authenticity with the help of Mutual Authentication. In the other type of authentication, the user is authenticated on the one time only. For the higher-level security, we used the Mutual Authentication [1]. For enhance the bandwidth Device to Device communication is taken as the best technology [7]. The Prose is used for the LTE-A (LTE-Advance) which provides the services of the Device to Device or we can also known as the 3GPP. In the physical layer of the LTE is allocated the capacity of all the resources, which is help to the Evolved Universal Terrestrials Radio Access Network (E-UTRAN).

If the user has, fewer resources are not worth enough of the high density in cell phones are E-UTRAN. The E-UTRAN is work only for the higher density of the mobile phones, which is not used for the network enough is resources of fewer [9]. With increase the throughput and increase the battery lifetime and the utilization of the services and the resources helps to improve the Device-to-Device communication is the trustworthy[15]. The sub types of the Device to Device are Cyber Devices, Vehicle Ecosystem and Smart Grid of the security system. To solve the authentication problem in the Email application with the help of the Identity Based Cryptography techniques. For the network user the IBC provides the authentication and the administration of the network. The conventional authentication has the advantage enormous the IBC strategies. The public key, Kerberos and pre-shared with it deals with authentication. The Peer- to-Peer authentication the IBC advice the symmetric protocol for the multi domain and the D2D.

The processing of mutual authentication can be prevented from the protocol cryptography, which is based on the Diffie Hellman Authentication. To secure the channel the public key cryptography with the hash key which is exchange the devices to be suggested in the simple protocol of the key. The mutual authentication is conducted with the large number to conduct that authentication[13]. When the user start the communication it shared the time prior shared to intiate the communication with the key protocol agreement. There are many no of ways to share the shared secret key which is used as the response and the challenges as well as the key derived function for the key sharing.
Mutual authentication (MANA protocol) is help to decrease the size of the message which is allocated for the authentication. The message of the authentication with the Kbits so that it provides the authentication channels or more secure channel. Mutual authentication is provides the four rounds for the commitment

scheme than the wireless channels [16]. Organization Change Management (OCM), which occupy for the help to maintain the security tools and the organization.

MANA is the less complicated to attack because it deals only with the short code and not operate many channels at the same operated as if the MAC addresses to be operated. The broadcast, access point and client are the main three stages in which the MANA is operated. MANA is the less entangled to assault since it bargains just with the short code and not work many channels at an indistinguishable worked from if the MAC delivers to be worked. The communicate, get to point and customer are the principle three phases in which the MANA is worked.

Dolev-Yao Model: Easy to attack on the Wireless and WLAN medium or channels. It impersonate the hacker. The hacker can communicate with the another person from the owner of the system. The owner of the system will not know about this activity. Easy to assault on the Wireless and WLAN medium or channels. It imitate the programmer. The programmer can speak with the someone else from the proprietor of the framework. The proprietor of the framework won't think about this movement.

IBC (Identity Based Cryptography): Its main purpose for the IBC is security and the administrative communication. IBC is used for the Pre-Shared key and public shared key algorithm. IBC is the similar technique of the RSA, which is used for the public key algorithm. IBC is have the main application is Emails. Its fundamental reason for the IBC is security and the managerial correspondence. IBC is utilized for the Pre-Shared key and open shared key calculation. IBC is the comparative system of the RSA, which is utilized for general society key calculation. IBC is have the principle application is Emails.

Paved and Martine: Their technique work on hardware security architecture to provide a trusted Computing platform for device authentication, but does not consider co-ordinate cyber physical attacks into consideration [12]. Their strategy deal with equipment security engineering to give a trusted Processing stage for gadget confirmation, however does not consider co-ordinate digital physical assaults into thought [12].

Mutual and Unilateral Authentication: The shared confirmation is the two-way verification though the one-sided is one-way. In common verification, both the members are confirmed in the meantime though in one-sided, one member is validated first which later on verifies the other one and soon. It is watched that the Wi-Fi based D2D correspondence is more solid than cell systems.

Wi-Fi is additionally spoken to as Wi-Fi P2P for the D2D Wi-Fi Frequency band. Hardly any difficulties are recognized which should be dealt with for provisioning of Security i.e. Privacy, Integrity and Availability. The difficulties recognized are depicted. When we transmit the flag through remote channels, we have to secure the message. To upgrade the security, confirmation is must. Confirmation needs key sharing. It can be partaken as open key and shared mystery key, which interfaces with the substantial number of portable clients. On the off chance that the two mobiles are in separation to each other and they need to decide, at that point one channel is built up to share the common mystery key between the two gadgets [2]. Nonetheless, there may be chance; the key built up through the human correspondence is excessively frail in a significant number of the cases. In this way, the third individual can assault effectively through beast drive technique.

The Quantization and the mistake remedy methods for confirmation work on same mystery key yet it has not been actualized broadly on the grounds that the transmission and age rate is low to share the mystery key. For the more drawn out piece, digits like 128 bits to 32 Hex decimals HASH work is recommended [2]. Dolev-Yoo has exhorted a technique to secure the programmers on the remote media [1]. It is watched that advanced cell does not run solid against infection devices as they expend more power. Assaults might be founded on equipment or programming yet the essential expectations are to upset the administrations offered [7]. Secret key based assaults are generally completed by the misfeasors as they probably am aware the casualty well. They utilize secret word speculating strategy to assault the framework.

The gigantic weight for the cell framework and the range for the extensive measure of the information movement which getting to the downloading application it is for advanced mobile phones, tablets and the cell phones to build the prominence. D2D (Device-to-Device) correspondences which is characterizes the individual gadgets that are included offload of the movement load from their foundation of the gadgets

[11]. The cell phones innovation is set up specifically connect between the remote gadgets without it go from the entrance point or cell foundation. Numerous written works have contemplated the application situations and conceivable specialized answers for D2D interchanges. In [11], the creators propose D2D interchanges as an underlay to the cell system, and present an instrument for coordinating D2D correspondences into LTE-Advanced system.

Yu et al. talk about the power control issue for D2D correspondences, and infer an ideal power designation for D2D interfaces under cell arrange control. The work in proposes to utilize Wi-Fi based D2D joins among cell clients to enhance the general system execution in uplink transmission. Wi-Fi Direct, at first called Wi-Fi P2P, is a Wi-Fi standard that empowers gadgets to effectively build up D2D associations utilizing the Wi-Fi recurrence band gives a wide review and exploratory assessment of the Wi-Fi Direct convention considers the functional usage difficulties of Wi-Fi Direct and demonstrates that the Wi-Fi Direct highlights permit sending the D2D worldview over the LTE cell framework.

Despite the fact that D2D correspondence has been a hot research theme as of late, there isn't much investigation concentrating on the security part of D2D interchanges. [11] and [10] talk about the physical layer answers for secure D2D interchanges, however their procedures are hard to be executed utilizing gadgets available.

Truth be told, because of the communicated idea of remote correspondence, remote channels are viewed as powerless against an assortment of assaults, and security is one of the real worries for D2D interchanges. To secure the correspondence between two end clients of a D2D connect, setting up a mutual mystery key is the first and most noteworthy advance. In any case, absence of trusted outsider and framework under D2D association condition makes this stage a non-paltry undertaking. The notable Diffie-Hellman key understanding convention empowers two gatherings mutually build up a common mystery key with no earlier learning. In any case, this convention is powerless against the man-in-the-center assault (MITMA) : a dynamic enemy makes autonomous associations with the casualties, influencing them to trust that they are talking straightforwardly to each other. To address this issue, scientists have thought of different Diffie-Hellman based cryptographic conventions, which can keep the MITMA by directing common verification.

One straightforward convention was recommended in [7], in which gadgets An and B trade the hashes of their open keys over a safe channel, in this manner playing out the shared confirmation. Nonetheless, this convention requires an expansive number of bits to be commonly confirmed. The MANA convention in [8] lessens the span of the verification message to k bits, however requires a more grounded documentation of confirmation channel. [9] presents a convention in view of responsibility conspires and requires 4-round correspondence over the remote channel. In this paper, we propose a 3-round key assention convention in light of responsibility plot. Our proposed convention is like the convention in, yet with less correspondence and calculation overhead, interim accomplishing a similar level of security. Real commitments of this paper are outlined as takes after:

- We break down the protected dangers and difficulties for D2D interchanges;
- We plan a protected and productive Diffie-Hellman based key understanding convention, and give the security investigation;
- We incorporate our proposed enter understanding convention into the current Wi-Fi Direct convention, and actualize it on Android cell phones.

Validation is an imperative cryptographic component in an electronic correspondence. With utilizing the verification it is conceivable to check credibility of the members amid the electronic correspondence. Essential electronic correspondence incorporates two members. The members of the electronic correspondence might be validated commonly or the confirmation might be one-sided. The members are confirmed to each other in the meantime if there should arise an occurrence of shared verification or two-way validation. If there should be an occurrence of one-sided verification or one-way validation the main member is confirmed to the second member or the second member is validated to the principal member amid the electronic correspondence. Common validation is regularly utilized when additional level of security is required, for instance, in the monetary exchanges between the associations.

One-sided confirmation is utilized when the main member of correspondence must be verified, for instance, in the business to distinguish stocks by latent RFID rather than standardized identification, in the Bus Rapid Transit (BRT) or in alternate situations where one side is reliable and the second side isn't dependable and must be validated. The members of electronic correspondence might be confirmed by hilter kilter cryptography or symmetric cryptography. Deviated cryptography is exceptionally well

known on the grounds that it utilizes open key and security key which are numerically related. Security key ought not be deducible from open key. Hilter kilter cryptography is computationally requesting and extremely asset expended on account of its strength.

This makes it unreasonable for minimal effort gadgets. Notwithstanding, there are a few proposition of verification conventions for minimal effort gadgets by uneven cryptography. In [3] proficient uneven test/reaction cross section based shared confirmation convention for ease RFID frameworks in view of their NTRU open cryptosystem adjustment was exhibited. In productive RFID shared verification conspire in view of ECC was proposed. In was exhibited convention in view of the McEliece cryptosystem for lightweight common RFID verification. The validation conventions in and for minimal effort RFID are exceptionally intriguing proposition since they are resistant to assault utilizing Shor's calculation [6] on quantum PCs. Quantum PCs are signified as a successor of transistor processors.

Symmetric cryptography is less computationally requesting and less asset devouring in correlation with awry cryptography. This makes it useful for minimal effort gadgets. The confirmation by symmetric cryptography utilizes a preshared mystery key. This is a sure burden in examination with the validation by hilter kilter cryptography. The preshared mystery enter isn't changed in most verification conventions. There are a few recommendations of conventions for confirmation on ease gadgets which can refresh the pre-shared mystery key on validated side. Minimal effort gadgets are computationally and asset constrained gadgets. This gathering of gadgets incorporates, for instance, the microcontrollers and the shrewd cards.

The expanding portable information utilization of shrewd gadgets requires new answers for information transmission for both indoor and open air remote systems. The idea of Device-to-Device (D2D) correspondences has been acquainted as a methods with offload the cell base stations by enabling close-by gadgets to straightforwardly convey between them [4]. Ebb and flow examine commitments on D2D interchanges have been for the most part done in cell systems with an attention on range productivity, vitality utilization, cell scope, throughput change, video transmission and substance conveyance. The creators proposed a coordination of D2D interchanges in LTE-Advanced systems to stay away from excess transmissions of a similar data asked for by various clients.

Golrezaei et. Al proposed to reserve mainstream video documents on cell phones and parcel every full scale cell into groups of littler cells with the goal that the reaction to a client demand can be performed

utilizing D2D interchanges if the substance is stored in the bunch. Particularly, Asadi et. al. proposed the utilization of LTE and Wi-Fi Direct to limit the adjustments of existing gauges. A bunching plan is utilized to separate clients into bunches in which just the client with the most noteworthy cell channel quality speaks with the base station. Pyattaev et. al. examined the utilization of Wi-Fi Direct for D2D interchanges in urban condition and demonstrates that the limit of the full scale cell can be multiplied.

To the extent we know, there is no work utilizing Wi-Fi Direct innovation to enhance the exhibitions in Wi-Fi systems. In this article, we propose to utilize Wi-Fi Direct, a settled remote innovation incorporated in a large portion of the present cell phones and tablets, for D2D correspondences to offload the Wi-Fi Access Point (AP) in thick remote networks[11]. Our investigation is especially valuable in grounds condition where an expansive number of tablets can be given to understudies in an assembly hall. By empowering Wi-Fi Direct correspondences between clients, joined with bunching, recurrence task and power control procedures, we can offload the entrance focuses and enhance the client's nature of experience.

Information security and protection are a disputable issue. Scientists are endeavoring to do their best to discover the idealize approach to secure the information productively. One of these arrangements is encoding the information utilizing cryptography calculations. Cryptography is the investigation of changing over the comprehensible data into confused or covered up, and just the approved people or machines can recover or get the first messages. It is separated into two noteworthy sorts (symmetric and awry) with respect to their keys.

(1) Symmetric cryptosystems require the clients to have a similar key to be utilized for encryption and unscrambling forms.

(2) Asymmetric cryptosystems require the clients to have two diverse keys (encryption key and decoding key). Symmetric key ought to be changed every now and then to influence it more to secure and unbreakable to keep different clients from getting the plain content.

In this manner, the security of any symmetric cryptography framework relies upon key trade convention utilized by the framework. Key trade convention is the method for conveying the keys in a protected way

among the clients [12]. There are such huge numbers of approaches to trade the keys amongst Alice and Bob, Alice can pick a key at that point to send to Bob physically (mail or individual). Then again, in the event that they have an old key so Alice can pick new key and encode it by the old one and send to Bob. Tragically, those strategies are not secure in wide dispersed frameworks these days for some reasons. Thusly, the mystery of their messages will depend vigorously on the picked key trade convention, for instance, Diffie-Hellman. Moreover, lopsided cryptosystems process is slower than symmetric one.

Symmetric cryptosystems utilizes a mutual mystery key to be utilized for scramble and unscramble forms. While hilter kilter cryptosystems does not utilize a solitary shared mystery key, as an option it utilizes scientific key combines: a private and open key. In this cryptosystems the correspondences are unscrambled with the private key and are encoded with general society key[16]. Therefore unbalanced cryptosystems have devouring excessively processing energy to deliver the two keys (private and open) and that is the reason it's slower than symmetric cryptosystems. Diffie-Hellman key trade convention was gotten 1976 by Whitfield Diffie and Martin Hellman this convention is generally utilized for secure key trade. The procedure of this convention assumes that Alice and Bob have diverse private keys and they need to concur upon two generally prime numbers p, g then each of them utilizes the got data to ascertain the general population keys.

After that they share their open keys between each other and utilize it with the private one, p and g to get the same shared key. Accordingly, both of Alice and Bob got the common key without sending their private keys through the divert in this paper, we will clarify the issue of Man-In-The-Middle (MITM) assault in Diffie-Hellman convention and the current defenses[5]. This paper proposes enhancements which can help avoiding MITM assault. These can check and secure the correspondences amongst Alice and Bob. Clients have usernames and passwords, and these will be utilized to interface them with their frameworks. Passwords as known are a blended string, and it can contain numbers, images, lowercase, and capitalized. These blends can be spoken to in parallel utilizing ASCII code. The twofold can be utilized to produce an alternate paired grouping utilizing arbitrary number generators and concentrate new data, which can be useful to conquer the issue.

The basic calculations utilized for security applications were Secure Hash Algorithms; SHA-l and SHA-2. Because of a few disadvantages of these calculations, National Institute of Standards and Technology

(NIST) reported an opposition on second November, 2007 for the production of another cryptographic hash work that would be entitled as SHA-3 family[5].

The opposition experienced through three rounds. NIST at first acknowledged sixty-four entries by 3151 October, 2008, out of which fifty-one progressed to the underlying round in December, 2008. The passages decreased to fourteen in number in the second round in July, 2009. The third round brought about five last contender to seek the SHA-3 title. The finalist SHA-3 applicants chose were BLAKE, Grostl, JH, Keccak, and Skein. The opposition finished in October 2012 with Keccak as the triumphant possibility to be called as SHA-3. Keccak has been chosen in view of the assessment Criterions of security, execution and adaptability [8] .

Rapid executions have turned into a need as these calculations are generally utilized. Programming based executions may not perform great as on intensely stacked servers. So the interest for high execution exists. A cryptographic hash work must be delicate to the littlest change caused in input information. It should come about an expansive distinction in yield for that little change. The information message might be given as video, sound or instant message. The specialized difficulties managed the hash work are enhancing the throughput and decreasing the region required. When meeting the security levels, execution of rapid must be dealt with. Equipment necessities address the issue of entryway check what's more, measure of RAM while the product prerequisite is the limited code estimate. The calculation needs to keep up the relative outline simplicity[13].

A few methodologies are intended to enhance the usage. They incorporate the unrolling strategy, implanted recollections, pipelining systems and the include enlist layers technique. Include enlist layers procedure is joined with pipe lined design to meet the planning requirements.

Servers store the passwords of all clients which may demonstrate a risk to security [6]. So as opposed to putting away the passwords, it might store their hashes . the info data at that point can be contrasted and the hashed information put away. This outcomes in the fast and secure equipment usage. Cryptanalysis process does the examination and assessment of cryptographic calculations, and makes utilization of the conventions and primitives. The two sorts of cryptographic primitives which are utilized are the stream figures and hash capacities are:

2.1 Stream Ciphers

These incorporate a mystery-shared key, which does the usefulness of XOR-ing with the information message. This is done as such as to give securities in the encryption forms. The content contribution of fluctuating length is changed over to a settled length yield with the utilization of this figure stream. These figures demonstrate exceptionally helpful in security and increment the throughput of the calculation. These are useful in portable applications, RC4 figure utilized by Wireless Encryption Protocol 802.11, Bluetooth Protocol which utilizes EO figure, and the SNOW 3G figure in the 3GPP gathering in the new versatile cell standard .

2.2 Hash Functions

These additionally are great cryptographic pnrllltlves. The hash capacities change the variable info length into a settled one. Their fundamental applications incorporate advanced marks and message validation codes. For this they are required to meet a few properties of security which have:

(i) Preimage protection, i.e., for a given f (x) it is infeasible to discover x,

(ii) Second preimage protection, i.e., for a given x it is infeasible to discover xl _ x : f (x) = f(xl), and

(iii) Collision protection, i.e., it is infeasible to discover x, xl : xl _ x and f(x) = f(xl).

(iv) A crash safe hash work is the one for which it is difficult to discover two particular messages ml and m2 which can create a similar hash or which is known as the message process.

(D2D) interchanges enable spatially proximal gadgets to specifically talk bypassing cell base stations (BSs) or access focuses (APs). Such a change in perspective from two-jump correspondences to one-bounce ones can bring many advantages, for example, ghastly productivity change, vitality sparing, and postpone decrease. Without the requirement for foundation, D2D innovation encourages portable clients sharing moment data (e.g., pictures and recordings) with each other even in ranges out of cell scope or with no AP.

It is turning into an imperative empowering innovation for versatile informal organizations with the goal that companions in the region can be consequently distinguished and combined up for coordinate interchanges. In addition, it is advancing to empower supposed versatile impromptu mists, which misuse undiscovered assets of various proximal gadgets to arrangement cloud administrations, for example,

information and calculation offloading. For gadgets inside little zones (e.g., an office or a home), WiFi is a decent alternative for giving high information rate D2D correspondence at moderately minimal effort.

Advanced from WiFi, the WiFi Direct detail, as of late discharged by the WiFi Alliance, suits D2D applications by evacuating the intercession of an AP in both D2D connect setup and information correspondences. Then again, it enables gadgets to powerfully set up a shared gathering and arrange who plays the part of AP as the gathering proprietor (GO). Gadgets related with a GO are called customers. Not at all like other D2D empowering procedures in neighborhood, for example, WiFi in specially appointed mode and IEEE 802.11z, WiFi Direct arrangements a similar nature of administration (QoS) and vitality sparing systems as foundation based WiFi. Because of the open access nature of remote correspondences, D2D interchanges are defenseless against an assortment of assaults, which raises basic security challenges.

For instance, enemies may test delicate client information (e.g., the contact list put away in cell phones) by tuning in to certain D2D joins. An assailant may likewise profess to be another to set up D2D joins with clueless clients. Without a trusted framework, for example, an AP, it is the D2D clients' duty to secure their correspondences and ensure their touchy information for different sorts of assaults. In spite of the WiFi Protection Setup (WPS) instrument acquired from the WiFi particular, WiFi-Direct-based D2D correspondences can't be saved from those security challenges. Assaults (e.g., dissent of-benefit [DoS]) are hard to anticipate with WPS [8]. In addition, contemplates have demonstrated that WPS has its own security gaps, which can be utilized by savvy foes to set up hazardous D2D joins. With the expansion of cell phones and awesome potential interest for D2D correspondences, security insurance instruments are direly required. In the writing, there are few examinations on the security part of D2D interchanges.

In this article, we talk about the security challenges and recognize various assaults for D2D correspondences with WiFi Direct, for instance, man-in-the-center assault and DoS. Pairwise enter foundation lies in the bit for securing D2D joins. With the set up secure key, an assortment of cryptographic encryption calculations can be executed to secure D2D correspondence. To this end, we present a short validation string-based key understanding convention. We actualize the proposed convention for document sharing applications in a genuine framework utilizing Android cell phones. Tests approve the proficiency and viability of the proposed convention.

The WiFi Direct convention empowers two gadgets to build up a D2D association without the assistance of APs. The system for D2D association foundation utilizing WiFi Direct. Initial, two gadgets perform channel testing and find each other. At that point they consult to decide the gathering proprietor (GO), which works as an AP for this D2D connection in an intentional or arbitrary way. Amid the handshake procedure, every gadget sends a GO goal esteem, and the gadget with the most astounding worth turns into the GO.

After the gadgets have conceded to their individual parts, the GO starts the WiFi security setup utilizing WPS, and behaviors a Dynamic Host Configuration Protocol (DHCP) trade to set up the IP addresses for the two gadgets. Therefore, the D2D association between these two gadgets is set up. WiFi Direct is based on the IEEE 802.11 framework mode, and therefore can be consistently actualized by heritage WiFi gadgets. Plus, WiFi Direct acquires the highlights of conventional WiFi, including QoS, control sparing, and security components, and has the capacity of framing a more steady and secure D2D hidden system than customary specially appointed systems. Two common WiFi Direct application situations are represented.

• Two (or various) gadgets frame a neighborhood specially appointed system. Messages and documents can be shared among this system at no additional cost. This is especially valuable when there is no cell association or AP accessible.

• By WiFi Direct, a cell empowered gadget can impart its Internet association with different gadgets.

To secure WiFi Direct D2D correspondences, a cryptography key is required to play out the cryptography calculations, for example, encryption and validation. In any case, how to create and disperse the cryptography keys among WiFi Direct clients isn't a basic assignment. In this segment, we break down the issues of key age without an earlier shared mystery, and quickly present one run of the mill gadget matching convention using a short confirmation string (SAS). A key dispersion focus (KDC) or an open key framework (PKI) would be the main decision for enter appropriation and administration much of the time.

Not with standing, in the WiFi Direct application situation, as a rule clients set up their D2D connects in a dynamic and appropriated way; subsequently, security frameworks and affirmation specialists may not exist.

Then again, because of the assorted variety of gadget makers and absence of bound together measures, preloading secure keys into gadgets is neither proficient nor viable. Hence, building up a session key amid the WiFi Direct gathering development process would be the correct decision for WiFi Direct D2D correspondences.

Gadget to-Device (D2D) correspondence has been proposed to be promising information offloading arrangement and range effectiveness improvement strategy because of its natural qualities, e.g., enhancing asset use, upgrading client's throughput, broadening battery lifetime, and so on. As needs be, it has attracted extensive consideration examine group as of late. Other than the customary cell operation where client types of gear (UEs) are served specifically by the developed NodeB (eNB), client supplies are additionally ready to discuss straightforwardly with each other over the D2D connect [6] Different from the conventional D2D correspondence techniques such as Bluetooth or Wi-Fi-coordinate, D2D correspondence under laying LTE-Advanced (LTE-A) systems takes a shot at an authorized band, which normally gives an arranged organization rather than a clumsy one, bringing about a superior client experience and QoS ensure.

In this manner, it is essential and vital to grow new capacities and applications with the help of cell systems. Shockingly, regardless of its undeniable points of interest, D2D correspondence still faces two generous specialized difficulties when it applies to substantial scale applications, that is, security and accessibility. As the associations happen specifically between the vicinity gadgets, D2D correspondence may subject to numerous security dangers, for example, change and creation of the information, infringement of the client protection et cetera. Obviously, any malignant conduct of clients may make genuine outcome and lead decayed client encounter.

Besides, accessibility must be accomplished as in clients may be troubled if the administrations are discontinuous or they experience the ill effects of a long sitting tight time for sharing the data. Thus, it is at last essential to build up some detailed and painstakingly outlined conventions to accomplish security and accessibility in D2D correspondence before its down to earth executions. In any case, the extent that we know, exceptionally constrained work has been proposed to address the above issues in D2D correspondence. To cross over any barrier between the exquisite hypothesis and practical application, in this paper, we go for tending to the issue of security affirmation for information transmission in D2D

correspondence. In particular, we present a protected information sharing convention (SeDS) through a cryptographic approach, in which both open key based signature and symmetric encryption are connected to understand the security goals.

Specifically, the information shared among the real clients is marked by the information supplier to guarantee information expert and the marked information will be re-marked by the transmitter to ensure transmission non-denial and additionally offering proof for the information sharing occasion, which is utilized to oppose free-riding assault and enhance framework accessibility. By together considering the qualities of the phone arrange and the advanced mark, traceability is guaranteed with a straightforward secure one-way hash work, which is effective in calculation and correspondence overhead. In the mean time, symmetric encryption system, which is time and vitality effective contrasted and the awry technique, is received to shield the first data from spilling out. To unscramble the information, the collector is relied upon to send a key indication ask for message to the eNB, subsequently accomplishing gathering non-renouncement, which is an imperative element of the proposed convention. In synopsis, our commitments are:

Right off the bat, we propose a SeDS in D2D correspondence condition. With the assistance of SeDS, the assets shared among the clients are classification and honesty guaranteed through endto-end encryption. Also, if the transmitted information isn't started from the approved supplier or changed by a few foes, the collector can distinguish the occasion by signature check and report a criticism message to the administrator. Subsequently the created message can be halted from affecting different clients.

Furthermore, to enhance the accessibility of SeDS convention, we set a record table in eNB for nothing riding recognition, along these lines prompting companions' collaboration in handing-off message. All the while, the record table is utilized to ensure traceability by alluding the pseudo personality to the comparing genuine character. Also, different models are set up to gauge defer under various application situations for choosing the negligible number of introductory specialist co-ops, which are chosen to strike a harmony between the cost and accessibility. Last however not the minimum, we dissect the security qualities in subtle elements and assess the SeDS execution of correspondence cost, calculation cost and accessibility out and out.

2.3 Types of Attack

• Attack in view of correspondence

• Attack in view of vulnerabilities in programming application

• Attack in view of equipment vulnerabilities

• Password breaking

There are different classes of assaults which are talked about in this area:

• **Attack in light of correspondence**: Some assaults depend on correspondence, which is brought out through the SMS and MMS. There are some cell phones, which are having the issue to deal with the SMS. On the off chance that the client is utilizing the Siemens S55 portable, it gets the instant message as Chinese character, which is later denied to give administration to the client [6].

• **Attack in light of vulnerabilities in programming application**: Phone breaking is a firmware, which is completely in view of the web program. Advanced mobile phones are defenseless to these phishing and pernicious assaults which happens while perusing the site.

• **Hardware helplessness**: In these sorts of assaults, the assailant finds the bugs or disadvantages in the equipment and tries to abuse the attributes of the equipment.

• **Password assault**: The secret word assault depends on the keystroke, signal of the versatile frameworks and so on. The aggressor fundamental goals are to assault the weaker frameworks. In spite of the fact that there are a lot of strategies to assault a framework yet in this paper the discourse is limited to couple of huge assaults as it were.

CHAPTER-3

PROBLEM FORMULATION

SECURITY ISSUE

- The comparison string is long so it is difficult to solve. At the receiver ends.
- Existing technology are subjected to MITMA.
- The authentication string is display on the device straightforward the comparison of the authentication is more convenient and efficient way.
- Diffie Hellman is not secure on the physical layer key generation.

CHAPTER- 4
OBJECTIVES

- To implement the Diffie-Hellman and SAS (short authentication string).
- To implementation a robust device-to-device authentication scheme which can prevent against MITMA.
- To implement man in the middle attack on SAS and Diffie - Hellman.
- To shows the result of Diffie Hellman and SAS in which it shows the values which is not change when it goes through the man in the middle attack.
- The future is to improve the longer string, which is to be transmitted at both the end.
- The key agreement protocols to reduce the authentication overhead and enhance user experience.
- To reduce the communication overhead and key generation time.

CHAPTER 5

RESEARCH METHODOLOGY

5.1 DIFFIE-HELLMAN ALGORITHM

Diffie- Hellman key exchange is a cryptography key over a public channel and it is the firt public key protocol. Diffie –Hellman is used to secure a variety of service internet. It estabioish a shared secret between two parties that is used for secret communication for transferring the data over a public network.

1. The parties agree on the algorithm parameter q and α.
2. The parties generate their private keys a,b,c.
3. Alice compute g^a and sends it to Bob.
4. Bob computes $(g^a)^b$ =gab and sends it to Alice.

```
clc;
clear all;
close all;
% Global public element
q=input ('enter the private number');
alpha=input ('enter the primitive root of q');
 % user Alice key generation
XA=input ('enter the private key of Alice less than q');
a= ((alpha) XA);
YA=mod (a, q);
disp (YA);
% user Bob key generation
XB=input('enter the private key of Bob less than q');
 b=((alpha)XB);
YB=mod(b,q);
disp(YB);
% calculate of secret key by user Alice
c=((YB)XA);
```

```
K1=mod(c,q);
disp(K1);
%calculate of secret key by user Bob
d=((YA)^XB);
K2=mod(d,q);
disp(K2)
if (K1==K2)
   disp(K1);
end;
```

5.2 DIFFIE-HELLMAN MAN IN THE MIDDLE ATTACK

The problem about man in the middle attack on Diffie-Hellman is that both sides are not confident about other sides are not confident about other sides public key. If they were sure that they have correct public key of their friend man in the middle attack would not be possible, because adversary bases MITM attack on the forgery of public keys. If for instance Bob and Alice meet for exchanging their key. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants.

1. Eve prepare for the attack by generating two random private key X_{D1} and X_{D2} and it computing the corresponding public key Y_{D1} and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Eve also calculates $K_2 = (Y_A)^{XD2} \bmod q$.
4. Bob receives Y_{D1} and calculates $K_1 = (Y_{D1})^{XB} \bmod q$.
5. Bob transmits Y_B to Alice.
6. Eve intercepts Y_B and transmits Y_{D2} to Alice. Eve calculates $K_1 = (Y_B)^{XD1} \bmod q$.
7. Alice receives YD2 and calculate $K2 = (Y_{D2})^{XA} \bmod q$.

```
clc;
clear all;
close all;
% global public
q=inpu('enter prime number');
```

```
alpha=input('enter primitive root of q less than q');
 % user Alice key generation
XA=input('enter the private key of Alice less than q');
a= ((alpha)^XA);
YA=mod(a,q);
disp(YA);
% user Bob key generation
XB=input('enter the private key of Bob less than q');
 b=((alpha)^XB);
YB=mod(b,q);
disp(YB);
%  calculation of secret key by user Alice
C=((YB)^XA);
K1=mod(c,q);
disp(K1)
%  calculation of secret key by user Bob
d=((YA)^XB);
K2=mod(d,q);
disp(K2)
if(K1==K2);
 disp(K1);
end
```

% man in the middle attack

```
XD1=input('enter the private key of EVE as Alice');
XD2=input('enter the private key of EVE as Bob');
D1=((alpha)^XD1);
D2=((alpha)^XD2);
YD1=mod(D1,q);
YD2=mod(D2,q);
d1=(YD1)^XD2;
d2=(YD2)^XB;
K1=mod(d1,q);
```

K_2=mod(d2,q);

$d_3=(Y_B)^{XD1}$;

$d_4=(Y_{D2})^{XA}$;

K_1=mod(d3,q);

K_2=mod(d4,q);

disp(K_1);

disp(K_2);

The main research is on pair wise key agreement protocol, which includes the minimum mutual authentication. In the paper, it introduces the authentication pair wise authentication pair wise authentication, which is short string or very short string. The protocol is all about the length of bits, which is required for mutual authentication in two parties.

SAS protocol defines the commit scheme or cryptography commitment scheme. Commit scheme is define to hide a choosen value from the other and transform the commit that value is the be open with the opening value. Anyone can open the pair and reveled the of pair value which the help of open operation. Commitment value is not leaked the information of hidden value. Custing the cryptography hash function. It efficient make the commitment scheme with the help it is not detect or difficukt to detect the messages. H is the notation of cryptography hash function.

The following commitment scheme is applied in the paper :

- Commit: given x, random pick r{0 1} ^n and compute c=H(x,r).
- Open: let d=(x,r). output x if c=H(x,r) [10]

The commitment scheme is provides the level of difficulties and security. The commitment scheme is depend upon the hash function which is used. By adopting the SAS key agreement protocol the commitment scheme is enchancing the mutual authentication and protect the diffie hellman from man in the middle attack (MIMTA). Excluding it used the differ hellman parameter that is ga and gb, Alice and Bob generate the value with the concatenation of identity of the Alice and Bob, Parameters of diffie hellman that is ga, gb and random string k-bit.

Alice choose the value like mA=Ida||ga||Na. ma is the commitment scheme of Alice. Opening commitment pair value must be (c,d). To obtain the secret key. Alice and Bob are transmit the message on the public channel.

- To commit Alice send C to Bob.
- Bob send mB to Alice.
- When Alice receive mB it send the open value D to Bob where D is the secret of ma.With the help of this Bob reveal the choosen value of Alice. With the opening operation is generating the shared secret key which is depend upon the parameters of diffie hellman. If Alice and Bob are outof band channel still they are authenticate each other. The SAS is providing the Alice and Bob generate k bit string which defines the size of string.

$S_A=N_A$ xor N_B

And

$S_B=N_A$ xor N_B

Where N_A and N_B are revealed from mA and extracted from mB.

Over the secure trusted channel it verify with the comparison of SA=SB.

If it is not matched with each other then the MITMA(man in the middle) is performed. The Alice and Bob stop the process of key establishment. In SAS protocol Alice commit the value of mA prior to showing the Bob value. Bob commit value mB prior to showing the Alice value. If EVE tries to attack MITM(man in the middle) Alice and Bob don't know the strategy is using by the EVE.

5.3 SAS (Short Authentication String)

```
clc;
clear all;
close all;
g=input('enter the public value');
x=input('enter the random value');
r=[0 1];
```

c=input('enter the open value');

g_A=input('enter the public value of alice in DH');

g_B=input('enter the public value of bob in DH');

N_A=input('extract from m_B');

N_B=input('revealved from m_A');

$S_A=N_A+N_B$;

$S_B=N_A+N_B$;

Id_1=input('enter the Id_A value');

Id_2=input('enter the Id_B value');

m_A=Id1||s1||N_A;

m_B=Id2||s2||N_B;

s_A=xor(N_A,N_B);

s_B=xor(N_A,N_B);

$y=N_A+N_B$;

$Y=N_A+N_B$;

5.4 Security Analysis

In this paper the author is provides the security with SAS key agreement protocol Alice has commit the value oh mA before knowing mB, and Bob has to submit on mB before knowing mA. The EVE is have strategy to perform MITM attack Alice and Bob don't know the strategy about that firstly to attack EVE commit the value mE and authentication string Ne. EVE starting the protocol in which make believe to Bob it is Alice. Initial the EVE commit mE=Ida||ge||Ne and do commitment ce and send it to Bob. In the time following Bob collect me and send to EVE mB. EVE change mB into m′B =IDb||ge||Nb and transmit to Alice. But the mutual authentication between Alice and Bob it compare Sb=Nb xor Ne with Sa=Na xor Nb though the particular channel band them they come to know Sa≠Sb. EVE only have tries to attack successfully when Alice and Bob agree with the authentication string is have Ne=Na but EVE randomly guess this Na. to getting the exact Na it can perform 2^-k times. If EVE replaying the me to perform the attack then me=IDb||ge||Ne.

5.5 SAS MITM Attack

clc;

clear all;

close all;

g=input('enter the public value');

x=input('enter the random value');

r=[0 1];

c=input('enter the open value');

g_A=input('enter the public value of alice in DH');

g_B=input('enter the public value of bob in DH');

N_A=input('extract from m_B');

N_B=input('revealved from m_A');

$N_E=N_A$;

$S_A=N_A+N_{B;}$

$S_B=N_A+N_B$;

Id_A=input('enter the IdA value');

Id_B=input('enter the IdB value');

Id_E=input('enter the IdE value');

$m_A=Id_A||s1||N_A$;

$m_B=Id_B||s2||N_B$;

$m_E=Id_A||s3||N_E$;

$ME=Id_B||s4||N_E$;

s_A=xor(N_A,N_B);

s_B=xor(N_E,N_B);

$y=N_A+N_B$;

$Y=N_A+N_B$;

Wi-Fi Direct protocol enables two devices to establish a D2D connection using Wi-Fi frequency without the help of access points. Fig. 2 shows the procedure for a D2D connection establishment using Wi-Fi Direct. First, two devices perform the channel probing and discover each other. Then the two devices will go through a 3 way handshake to determine the group owner (works as an access point) for this D2D connection. After the devices have agreed on their respective roles, a DHCP exchange will be conducted

to set up the IP addresses for both devices. Thus, the D2D connection between these two devices has been established. We add our proposed key agreement protocol on top of the existing Wi-Fi Direct protocol. After the address configuring phase, the two devices will go through our proposed key agreement protocol as well as the mutual authentication process to agree on a shared secrete key. As long as the two devices have agreed on the authentication message, they can subsequently use their shared secret key for future communication.

The k bit length of authentication string are tries to the usability and balance the security level. For the k bit larger attacker smaller possibility to the attack but the two user need to compare the string longer as possible depend on band channel. If the 20 bit string of authentication so that it provides the same security as compare to ATM.

CHAPTER 6
RESULT AND DISCUSSION

6.1 Analysis using MATLAB

The security key analyzed with the efficient manner it analyzed only with the two scenario one is random features or characteristics and different from other or uniqueness. In the Nation Institution of Standards and Technology, which the engineers are, discuss some scenario of the security while testing and the selection of the random generating numbers. With the help of security, application, which is, helps to generating the security keys that is private keys it shows in the output of the generating key application. The security application is handle the attack by generating the security key and it is enough to secure the attack in the application.

If the user is understand the seeds the output or the data couldn't be understand by the third party. The major issue is generating the key, which should be the random. Some techniques are ther to generate the random keys but they are not properly efficient to the user. The random generation of testing the random application this is used for random selecting keys. To check the keys it should be random p and q values. The private key helps to generate the public keys. The MITMA is performed by in the Diffie-Hellman.

The SAS is not performed MITMA. It has different manner to generate the public key and the it uses the xor function. The overview of generating the keys for diffie –hellman and short authentication string is define below:

6.2 **Results in Paper**

In this paper the author took the application of the android mobile phones. It seen the secure transmission of the file on the android mobile applications. The secure key establishes by the functionality of the Wi-Fi direct functionality applications [10]. The under can establish pair wise key to communication with the two parties. With the help of pair wise key agreement, it encrypt the data for transmission through the Device to Device communication. The development in some applications like Wi-Fi direct, which is used with the help of Smart Phone Nexus 5 (two Google Nexus 5 smart phone) and also with the help of 4.4 kitkat Android phones also [12].

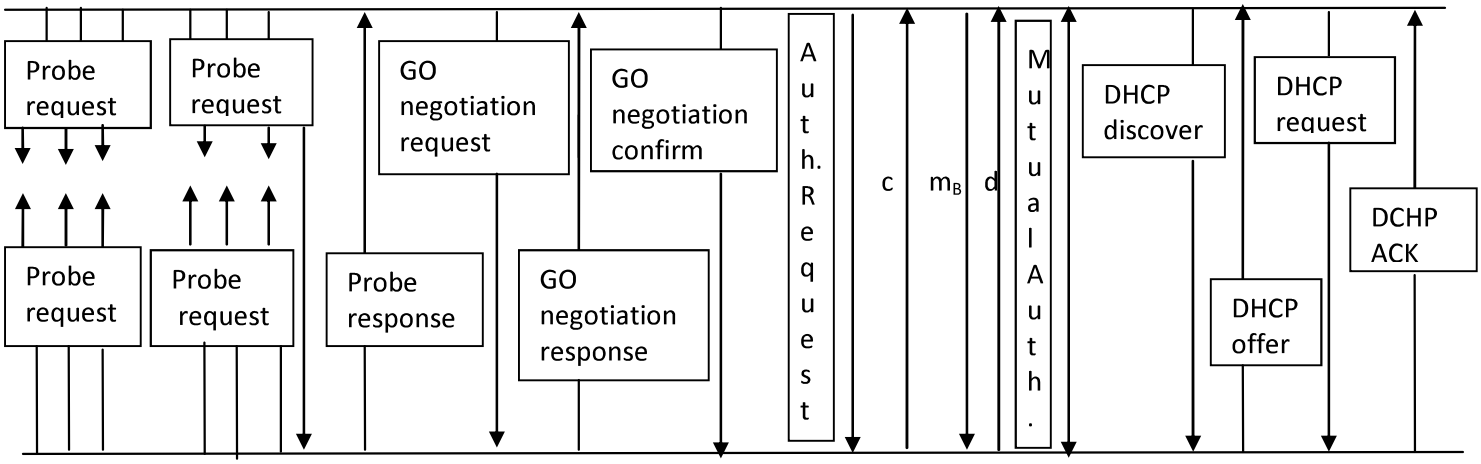

Fig. 6.1 Secure Wi-Fi Direct Protocol.

With the key agreement phases is not occurring when it working in hash based scheme commitment. The based on hash function it encrypted the data and transfer that on the commitment system. The author used the hexadecimal values in the implementation on the Diffie–Hellman[10]. The authentication string and the parameters fig 6.1 in Diffie-Hellman are taken the hex value only one at the time. If we took the p, value is up to 40 digits or hex value then at the output, it shows 130 bits of the secret key.

For the security purpose the author suggest to used the 5 hex digits values of the authentication string which helps to maintain the security level of the parties. The time is very less in the Nexus 5 in which the time is computation of the communication delay. It happens when the agreement process is involved upto 2.26Ghz. The whole processor is running in the key agreement of the processor.

i) Results of Diffie-Hellman program

enter prime number 7

enter primitive root of q less than q 5

enter the private key of Alice less than q 8

4

enter the private key of Bob less than **q** 4

2 4 4 4

Value of alpha α^{XA} **a** = 390625

public key of Alice is $\mathbf{Y_A}$ = 4

value of alpha α^{XB} **b** = 625

Public key of Bob is $\mathbf{Y_B}$ = 2

To generate the secret key $(Y_B)^{XA}$ **c**= 256

secret key generated by the user Alice $\mathbf{K_1}$ = 4

To generate the secret key $(Y_A)^{XB}$ **d** =256

secret key generated by the user Bob $\mathbf{K_2}$ =4

ii) Result of Man In The Middle in Diffie Hellman

enter prime number 7

enter primitive root of q less than q 5

enter the private key of Alice less than q 8

4

enter the private key of Bob less than q 4

2 4 4 4

enter the private key of EVE as Alice 5

enter the private key of EVE as Bob 6

4 1

Value of alpha α^{XA} **a** = 390625

public key of Alice is $\mathbf{Y_A}$ = 4

value of alpha α^{XB} **b** = 625

Public key of Bob is $\mathbf{Y_B}$ = 2

To generate the secret key $(Y_B)^{XA}$ **c**= 256

secret key generated by the user Alice $\mathbf{K_1}$ = 4

To generate the secret key $(Y_A)^{XB}$ **d** =256

secret key generated by the user Bob $\mathbf{K_2}$ =4

$\mathbf{D_1}$ =3125

$\mathbf{D_2}$ =15625

$\mathbf{Y_{D1}}$ =3

$\mathbf{Y_{D2}}$ =1

$\mathbf{d_1}$ =729

$\mathbf{d_2}$ =1

$\mathbf{K_1}$ =4

$\mathbf{K_2}$ =1

$\mathbf{d_3}$ =32

$\mathbf{d_4}$ =1

$\mathbf{K_1}$ =4

$\mathbf{K_2}$ =1

iii) Results of SAS protocol

enter the public value 7

enter the random value 5

enter the open value 4

enter the public value of alice in DH 4

enter the public value of bob in DH 2

extract from $\mathbf{m_B}$ 1

revealved from $\mathbf{m_A}$ 1

enter the $\mathbf{Id_A}$ value 3

enter the $\mathbf{Id_B}$ value 9

$\mathbf{S_A}$=2

$\mathbf{S_B}$ =2

$\mathbf{s_a}$ =0

$\mathbf{s_b}$ =0

Output of SAS Alice **y** =2

Output of SAS Bob **Y** =2

iv) Results of Man in the Middle Attack on SAS

enter the public value 7

enter the random value 5

enter the open value 4

enter the public value of alice in DH 4

enter the public value of bob in DH 2

extract from $\mathbf{m_B}$ 728791

revealved from $\mathbf{m_A}$ 940497

enter the $\mathbf{Id_A}$ value 3

enter the $\mathbf{Id_B}$ value 9

enter the $\mathbf{Id_E}$ value 7

$\mathbf{S_A}$= 1669288

$\mathbf{S_B}$ =1669288

$\mathbf{m_A}$ =1

$\mathbf{m_B}$ =1

$\mathbf{m_E}$ =1

$\mathbf{M_E}$ =1

$\mathbf{s_a}$ =0

$\mathbf{s_b}$ =0

output MITMA on SAS Alice and Eve **y** =1669288

output MITMA on SAS Bob and Eve **Y** =1669288

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

Wi-Fi direct protocol is used for the device-to-device (D2D) secure communication. Wi-Fi direct protocol is initial analyze the security potential and the threats of security and the challenges of the Wi-Fi direct. After analyzed we have to established a secure key of cryptography which protect the Wi-Fi direct communication. The implementation of this experiment is on the Android smart phones which is demonstrated.

In future a hash function is introduced which help to developed and it must be resulting in the most efficient and integrity of the providing system. This algorithm as the performance which is existing the improvement of the algorithm, through that the complexity is increased of the system.

The Device to Device is improving the Qos with the reduction of traffic and the bandwidth will increase and the capabilities of the communication. The data disclosure opposite to the attacks the network are the retain to resistance for the QoS. The non- legitimate user are prevented from the attack with the help to increasing the Qos. The non- legitimate user are access the services. It will only possible if the user is having the authenticated. The certificates and the private key of the user check the authentication.

REFERENCES

[1] W. Shen, W. Hong and X. Cao, "Secure key establishment for device-to device communication," IEEE Global Communications Conference, pp.336-340, 2014.

[2] A.C-F Chan, J .Zhou, "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," IEEE Journal on Selected Areas in Communication, vol. 32, no. 7, pp.1509-1517, 2014.

[3] K. V. Nguyen, "Simplify Peer to Peer Device Authentication Using Identify-Based Cryptography,"Proceedings of the IEEE, International Conference on Network and Services, pp.43-47, 2006.

[4] N. Saxena, V. Jun Choi, R. Lu, "Authentication and Authorization Scheme for various user Roles and Device in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp.907-921, 2016.

[5] V. Clupek, V. Zeman, "Unilateral authentication on low-cost device," 38th International Conference on Telecommunications and Signal Processing, pp. 88-92, 2015.

[6] R. Hau Hsu and J. Lee, "Group anonymous D2D communication with end-to-end security in LTE-A," Proceedings of the IEEE, Conference on Communications and Network Security, pp. 451-459, 2015.

[7] A. Zhang, J. Chen and R. Qingyang Hu, "SeDs: Secure Data Sharing Strategy for D2D Communication in LTE-Advance Network," IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp.2659-2672, 2016.

[8] M.A.Patil,P.T.Karule,"Design and Implementation of keccak Hash Function For Cryptography,"IEEE," 0875-0878,"2015.

[9] A.S.Khader,D.Lai,"Preventing Man-In-the-Middle in Diffie-Hellman key Exchange Protocol,"22nd International Confrence On Telecommunication,"IEEE,"2015.

[10] W.Shen, B.Yin,X.Cao, L.X.Cai and Y.Cheng,"Secure Device to Device Communication over Wi-FiDirect,"IEEE,"4-9,"2016.

[11] L.Li, X.Zhao,G.Xue,"A proximity authentication system for smart phone," IEEE,"1545-5971,"2015

[12] S.I.Kouner, T.M.T Nguyen,S.Monnet and L.Hamidoochae,"Device-To-Device Communication Using Wi-Fi Direct for Dense Wireless Networks,4671-4674,"IEEE,"2016.

[13] C.kaur,G.S.Gaba,R.Miglani,S.K.Arora,"A Survey on Device to Device Authentication scheme,"IJCATA International science press ,"327-333,"2016.

[14] R.Pass,"On deniability in the Common refrence string and random oracle model,"International association for cryptologic research ,"316-337,"2003.

[15] E.Gonen,"H,uaku and P.joshi,"A Peer-to-Peer Architecture of Mobile Communication ,"IEEE,293-297,2005.

[16] S.Veiudenay,"Secure Communication over Insecre Channel based on Short authenticated strings,Lausane Switzerland, 2014.

[17] https://www.google.co.in/search

[18] http://telcomarticle.blogspot.in/2011/01/definition-of-soft-hand-off-and-hard.html.