Mobile Social Networking

Tabassum Afrin
6th sem Information and Science dept.
Sai Vidya Institute of Technology
Bangalore-64, India

C. S Naveena
6th sem Information and Science dept.
Sai Vidya Institute of Technology
Bangalore-64, India

***Abstract*— Social Networking has become an important part of our lives and with the boon of Smartphones the access of social networking sites (SNS) has become easier. Security and privacy remains as the major issues of concern. In this article, we examined MSN architecture, privacy, security, malicious attacks and trustworthiness. We then explore the possible methods of data transmission using Li-Fi and RSA algorithm.**

Keywords—Mobile Social Network ; MSN Privacy ; MSN Security ; Li-Fi; RSA;

I. INTRODUCTION

The concept of social media has been around for ages, even cavemen posted on each other's walls. The mobile Internet just scaled this to a whole new level with almost 2.3 billion people on mobile social networks. Social media is a shift in how people discover, read and share news, information and content transforming monologs (one to many) and dialogs (many to many). Social networks have become an important aspect of people's daily life. Checking the social network newsfeed is the first thing some people do each time they turn on Smartphones. Facebook is the largest social networking site which has around 2.3 billion users. Facebook and Twitter have reached 84 percent of the world's online population with Twitter having around 271 million users. Meantime fueled by the advancements of Smartphone and ubiquitous connections of Internet network, social networking is further available for mobile users and keeps them posted up-to-date on worldwide news and messages from their family and friends anytime anywhere.

Mobile Social Network (MSN) helps us to stay connected better than ever. Fig. 1 lists some advantages and disadvantages of Social networking sites. Security and speed are the major issues that are challenging present social networking technology. Security and privacy are always compromised when it comes to speed.

But security and privacy are important aspects of data exchange. We need to establish a network which is very secure and does not compromise with speed. In this article we enlightened architecture of MSN and a few of the challenges regarding security, privacy and trustworthiness. We tried to implement Li-Fi with RSA algorithm which provides both speed and security for data transmission. Hence the process of bringing the world much closer becomes fast and secure.

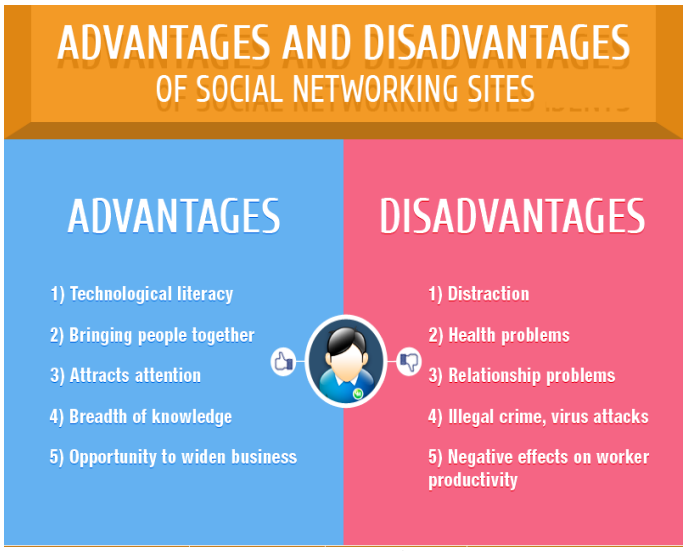


Fig. 1. Advantages and disadvantages of social networking sites

II. MSN ARCHITECTURE

In this section, we present MSN architecture by introducing the common entities, MSN security and privacy, and the communication pattern.

A. Entities involved in MSN communication

As shown in Fig.2, an MSN is virtual environment that consists of Smartphone Users (SUs) present in a local area, Internet Service Providers (ISPs) and Local Service Providers (LSPs). MSN communication is formed upon the agreement of the participating SUs and LSPs.

Smartphone Users: The communication technologies for different applications are chosen by the SUs. The SUs can not only access Internet via Wi-Fi/Cell networks but can also communicate with neighboring SUs via NFC/Bluetooth technologies. For example the SUs may use Internet to obtain service information and service reviews can be obtained from nearby SUs by using Bluetooth for communication.

Fig. 2. Mobile social networking in a city

Local Service Providers: The LSPs that are either static or mobile provide services to the SUs in the vicinity. When the LSP is mobile it can be equipped with a Smartphone that disseminates service information to the encountered SUs. When the LSP is static, it could be in restaurant or local store that is visited by the nearby SUs. The static LSP is equipped with enhanced communication and storage devices that are placed in, on or around their buildings. These communication devices are used by LSP to interact with nearby SUs.

Internet Service Provider: Due to pervasive deployment of cellular network mobile access to internet service is available. SUs can also access Internet via Wi-Fi hotspot, which are widely distributed in shopping malls, restaurants and even residential communities. ISP can provide service information to SUs in MSN whenever and wherever the SUs need it.

B. Communication pattern in MSN

SU to ISP- There are two common communication technologies that are enabled on Smartphones to help SU to ISP communications. One is cellular networks and the other is Wi-Fi technology. The SUs purchase a data plan from wireless carriers. Their Smartphones are connected to the Internet through the cellular network infrastructures maintained by such companies. Wi-Fi technology offers pervasive Internet access at larger bandwidth and cheaper cost. Free Wi-Fi access is provided in many LSP commercial business solutions.

SU to LSP- The SU and LSP communication help SUs to obtain the better service information of nearby LSPs. Short-range wireless technologies, such as Wi-Fi and Bluetooth are used for communicating. Due to the ease of setup and low costs, many LSPs have been equipped with wireless routers to offer Internet access to their customers. These LSPs are connected to their customers through Wi-Fi.

SU to SU- SU to SU communication is useful for the SU to share information efficiently. Short-range communication technologies like NFC, Bluetooth, and Wi-Fi Direct are integrated into smart phones to implement SU-to-SU communication. NFC has a lower transfer rate than Bluetooth though it sets up more quickly than standard Bluetooth. Maximum work distance of NFC is less than 20cm, which reduces the likelihood of unwanted interception. It makes NFC suitable for crowded areas. Whereas Bluetooth and Wi-Fi direct support wireless communication for longer range, this
makes it more suitable for SUs to share information over distance. Wi-Fi direct consumes more energy but promises
data transfer speed of up to 250 Mb/s which is much faster than Bluetooth and NFC.

III. PRIVACY IN MULTIMEDIA ORIENTED MOBILE SECURITY NETWORK

Users never like to open up their personal information and unique data to strangers and unknown persons. So privacy always holds the first prominence in Multimedia oriented Mobile Security Networks (MMSN) where the matter might be directly related to user's privacy and other confidential information .The information might be about user's place choices and social status and relationships. Cryptography is usually employed to save the data being disclosed by any hackers or attackers during processing and transmitting the contents. Cryptography is the process of encompassing the principles of transforming the intelligent messages into that is unintelligible and then transforming that message back to its original form. When users are matching their profiles, always secure profile matching is exploited to make sure that users' any personal and unique information is directly disclosed. But in spite of all this some information is opened to users' friends' .A simple example is that if someone makes an inquiry to the centralized server or to his or her friends, it might probably refer to the personal interest, so here the term privacy is destroyed. Sometimes users neglect the fact that their privacy is being disclosed and do not try to protect it. So privacy must be accomplished so that users can be guaranteed a secured mobile networking service.

A. Malicious Attacks

Malicious attacks can be launched in MMSN to reduce quality of network performance or to disregard lawful users' data. At the time of content sharing malicious attackers duplicate the contents and unreal ones are shared or presented to the users. Fig. 3 depicts how the attacker silently redirects the user to the exploit site. These malicious users do not help and pay as other users do and sometimes show denial of service attacks.

To help bring about cooperation and content sharing user's long term relationships and trust relationships are examined. Game theoretic frame works are proposed to model and analyze conspiring attackers in multimedia social network. In case of service assessments with the User - to -Local Service domain, a local service usually posts positive reviews and removes and omits negative feedback. It might also collude

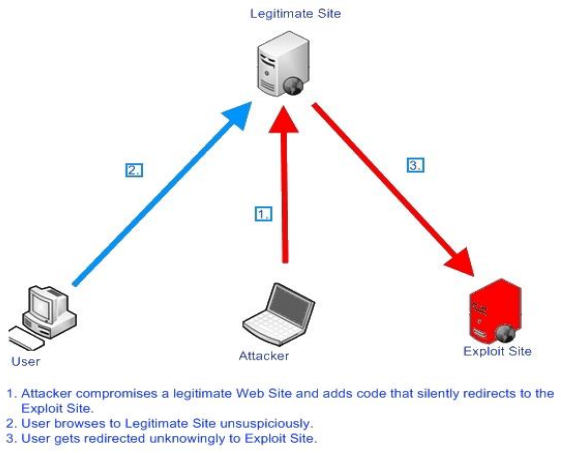


Fig. 3. Malicious attack

feedback are hidden on particular stores. In short the security measures are to be taken to defend malicious attacks and give out with a secure Multimedia oriented Mobile Networking Services for users.

B. Trust Associations

The main requirement of any social-based application or software is trust in other words reliability. The contents shared among friends are more reliable than those with unknown people. Content sharing can be done in a decentralized way of social networking to utilize trust relations and associations among users. It is still very difficult and challenging to identify and recognize the correctness, reliability and trustworthiness of the delivered data in the mobile or local surroundings. In case of local service evaluation people mainly believe in the reviews of their friends rather going by an unknown person's reviews as the expectations of strangers and user might be completely different. The user might not find these reviews very useful. The reliability and trustworthiness can be enhanced only if the reviewer's preferences are taken into picture. If the comments and reviewer's preferences are linked it definitely affects the privacy of the reviewer. So privacy must also be taken into picture and should be made sure that it should not be affected to improve the services for users. The process of building the trust relationships between mobile users MMSN is a very challenging issue as it also involves providing trustworthy and reliable information so that users are not misguided.

C. Different secuity solutions

Content inquiry is used widely used in social networks and is an unexceptional part of the MMSN. Queries made usually mirror images the mindset of the users and ultimately it is the main aim of the Multimedia-oriented Mobile Network Services .It might in User-to-Centralized domain, User-to-Local Domain and User- to- User domains according to the type of contents. Centralized server has largest capacity of storage and, calculation and communication. It maintains relations with worldwide content resources, so that data can be easily joined together on the centralized Service side. When cloud computing has been introduced lately the cloud servers are capable of storing large amount of data .They store majority of multimedia data and process them.

IV. MOBILE SOCIAL NETWORK USING LI-FI

Currently Wireless communication is carried out using Radio Spectrum. We come across many disadvantages with Radio Spectrum like Cost and expensive, Less bandwidth, Limited availability, Less secure and millions of base stations consume huge amount of energy for transmitting the radio waves and to cool the base station cabins. Radio spectrum is congested but the demand for wireless data double each year. It seems that everything wants to use wireless data but the capacity is drying up. We have different options to replace Radio Waves for wireless communication. Fig. 4 shows the various options available for replacing radio-waves, out of which visible light is chosen since it has larger bandwidth and is safe to use. Li-Fi can replace radio waves for wireless communication. Li-Fi can be thought of as light based Wi-Fi, which uses light instead of radio waves to transmit information.

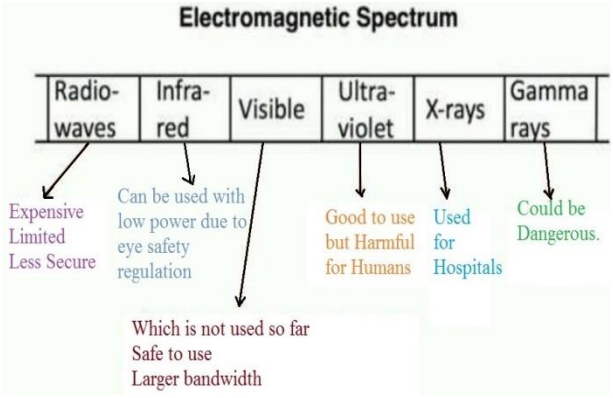


Fig. 4. Options to replace Radio-waves

Li-Fi uses transceiver-fitted LED lamps instead of Wi-Fi modems that can light room as well as transmit and receive information. In Li-Fi the data is sent through an LED light bulb that varies in intensity faster than human eye can follow.

A. History

The technology began in 1990's in countries like Korea, Japan and Germany where they discovered LED's could be retrofitted to send information. On 12th July 2011 Harald Haas used a table lamp with an LED bulb to transmit a video of blooming flowers that was then projected onto a screen behind him. He periodically blocked the light from lamp during this even to prove that the lamp was the source of the incoming data.

At TED Global, Harald Haas demonstrated a data rate of transmission around 10Mbps, which is comparable to a fairly good UK broadband connection. He achieved 123Mbps two months later. In 2011 a German scientist succeeded in creating an 800Mbps capable wireless network by using nothing more than normal red, green and yellow light.

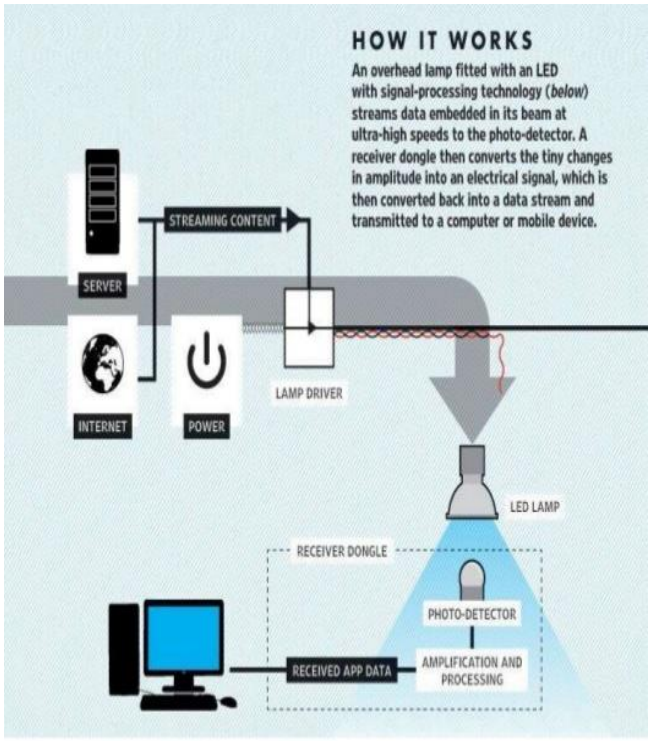
B. Basic Concept

LED (Light Emitting Diode) can be switched on and off faster since the operating speed of LED is less than 1µs, than the human eye can detect, causing the light source to appear continuously. This invisible on-off activity enables a kind of data transmission using binary codes. Switching on the LED is logical '1', switching it off is logical '0'.Encoding data is possible in the light by varying the rate at which LED's flicker on and off to give different stings of 1s and 0s. Modulation is so fast that the human eye does not notice.

Further enhancements can be made in this method, like using an array of LEDs for parallel data transmission, or using mixtures of red, green and blue LEDs to alter the light's frequency with each frequency encoding a different data channel. Such advancements promise a theoretical speed of 10Gbps.

C. Data transmission using LED

An overhead lamp fitted with an LED with signal- processing technology streams the data embedded in its beam at ultra-high speed to the photo detector. A receiver dongle then converts the tiny changes in amplitude into an electrical signal, which is then converted back to a data stream and transmitted to a computer or mobile device (Fig.5).



a.

Fig. 5. Working of Lifi

TECHNOLOGY	SPEED	DATA DENSITY
WIRED		
FIRE WIRE	800 Mbps	*****
USB3.0	5 Gbps	*****
THUNDERBOLT	2X 10 Gbps	*****
WIRELESS (CURRENT)		
WI-FI-IEEE (802.11N)	150 Mbps	*
BLUETOOTH	3 Mbps	*
IrDA	4 Mbps	***
WIRELESS (FUTURE)		
Wi-Gig	2 Gbps	**
Giga-IR	1 Gbps	***
Li-Fi	>10 Gbps	****

Fig. 6. Comparision between different technologies.

The issues related to Capacity, Efficiency, Availability and Security in Radio Wave can be overcome with Li-Fi since it has 1000 times more spectrum than radio wave and light boxes are already present so, infrastructure is available already and installed. Li-Fi is highly efficient because LED consumes less energy. Light is present everywhere and data is present where light is present. Hence data will also be present everywhere. If Li-Fi is implemented every bulb can operate as Wi-Fi hotspot. Since light waves does not penetrate through walls they can't be intercepted, that is data cannot be hacked. Fig. 6 shows the comparison between different technologies.

V. RSA ALGORITHM

Cryptography has got a very long and interesting history. Cryptography was used to protect important national secrets and strategies. The process of transforming the data or message into a code which is shared by two parties is called cryptography. It is done so that the outside watcher or intruder cannot detect it. Before moving into the topic enlighten yourself with certain terminologies like:-

Encryption:-It is the process of encoding the message in such a way that only authorized persons can read it.

Decryption:-It is the process of decoding the data that has been encrypted. It requires a secret key or password.

Cipher text:-The result of encryption performed on a plain text using an algorithm is called cipher.

This encrypted message should be decoded at the receiver's side before processing. The operator used by the security experts to encrypt the data is Exclusive-OR.

In networks systems encrypted data can travel between both users. The main tool that network security experts are using to encrypt a message is a secret key.

There are two types of encryption techniques:-

- *Secret key encryption*
- *Public key encryption*

Secret key encryption model - In a secret key encryption models both sender and receiver makes use of same key for encryption process. There are again two protocols here they are:-

- *Data Encryption Standard*
- *Advanced Encryption Standard*

Public key encryption model:-This model brought a revolution to the field of cryptography. In this model different keys are used by sender and receiver. This system is very powerful than the secret system and provides security and message privacy in an efficient manner. In this method, there are two related keys out which one can be used for encryption and the other for decryption. So a pair of keys is generated by a system using this encryption technique. The encryption key is placed in a public register and is now identified as public key. The other key generated is kept private. So it is called a private key. Both sender and receiver can know public key but only receiver must know private key. Consider an example where A wants to send a message to B. A makes use of B's public key to encrypt the message. After B receives the message, it starts decrypting the message using its private key, so no one can decode the message other than B as only B knows the private key (Fig. 7).

There are two types of public-key encryption protocol:-

- *RSA protocol*
- *Diffie – Hillman key exchange protocol*

Now we are concerned about RSA algorithm. This algorithm was developed by Rivert, Shamir and Aldeman. This algorithm has three phases:

- *Key generation*
- *Encryption*
- *Decryption*

Key generation Algorithm:

1. Choose two roughly 256-bit prime numbers, a and b and obtain n=ab.
2. Find x, Select encryption key x and (a-1) (b-1) are relatively prime (Two numbers are said to be relatively prime only if they have no common factor other than 1).
3. Find y. Calculate decryption key y:
4. xy mod (a-1) (b-1) =1
5. At this point a and b are discarded
6. The public key={x, n}
7. The private key={y, n}

So both sender and receiver can know about x but only receiver knows about y. Both a and b must be of similar sizes and greater than 1024 bits. The two values a and b should be made as large as possible for secure encryption.

Encryption

The value of n should be known for both sender and receiver. Consider m to be the plain text .Given m<n, cipher text c is constructed by

$C=m^x \bmod n$

(a and b are chosen in order of 1024 bits)

Decryption

Given the cipher text, c, the plain text, m, is derived by

$m=c^y \bmod n$

Practically calculations are done using math library.

So we are implementing Li-Fi and RSA algorithm together .The encrypted messages using RSA algorithm are sent from source through Li-Fi, which are later decrypted at the receiver side. This helps in maintaining the security of the data over Social Networking.

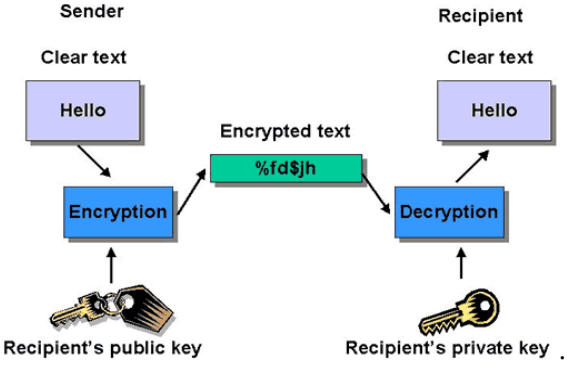


Fig. 7. Encryption and decryption using public and private key

CONCLUSION

In this article we have studied about MSN architecture and we have defined MSN communication patters. We even identified and dealt with security and privacy challenges. We have discussed about Li-Fi, its advantages and RSA algorithm. We have tried to make advancement in MMSN by implementing Li-Fi and RSA together which will certainly speedup the delivery of messages and provides a secured data transmission.

REFERENCES

[1] Xiaohui Liang ; Kuan Zhang ; Xuemin Shen ; Xiaodong Lin "Security and privacy in mobile social networks: challenges and solutions" Wireless Communications, IEEE (Volume:21, Issue: 1) pp 33 –41.

[2] Kuan Zhang; Xiaohui Liang; Xuemin Shen ;Rongxing Lu "Exploiting multimedia services in mobile social networks from security and privacy perspectives" Communications Magazine, IEEE (Volume:52 , Issue: 3) pp58-65.

[3] "Li-Fi gets ready to compete with Wi-Fi" Spectrum, IEEE volume: 51, Issue: 12 pp 13-16.

[4] Wozniak, S. ; Rossberg, M. ; Schaefer, G." Towards trustworthy mobile social networking services for disaster response "Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference pp 528-533.