Multi-level Secure Architecture with Authentication and Message Encryption for MESHNET Security

Gunjan Bhatnagar
Dept. of I.T
CGC Landran, Mohali

Mandeep Singh
Dept. of I.T
CGC Landran, Mohali

ABSTRACT
In cellular networks, the data traffic generated by users is becoming more challenging as the network is overloaded and not secured. The three algorithms are used to manage the two networks i.e. 3G networks and Wi-Fi network in the previous research work are Heuristic, Greedy and the Random. The existing scheme used the IPSec for the authentication purpose, hence prone to various types of the security attacks. In the proposed scenario, it is proposing a security mechanism for data offloading mechanism for the secure exchange of data. The proposed model will also use the Multi-level secure authentication for the user & the data privacy and the integrity in the environment of MESHNET. The proposed security architecture includes the RSA encryption with the multi-variate key exchange scheme, which ensures the secure data exchange on the higher data transfer rate. This will reduces the load from the cellular networks in the real time applications. The performance of the proposed model would be tested with the various parameters like the throughput, the transmission delay, the probability of the detection, and probability of the false alarm, etc.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
MESHNET security, Mobile data offloading security, Mobile Wi-Fi data offloading, RSA, encryption, authentication.

1. INTRODUCTION
Earlier cell phones were connected through the cellular networks; therefore they can transfer the data through the cellular networks only. The advancement in the handset technology has taken cellular networks to the next level, where the cell phones can perform the multiple tasks. The new cell phones communicate between themselves through cellular networks by using the various SIM cards. It may also communicate through the various other modes Wireless (Wi-Fi), Bluetooth or RF interfaces. The researchers have found the new ways of using the data networks in a combinative form to create the heterogeneous networks. For the cellular data offloading, the researchers have given the ways to inter-connect with the Wi-Fi networks and the mobile networks. The cellular data offloading is a way through which the cellular calls over the Wireless networks have been transfer, hence, this makes an efficient use of wireless network resources.

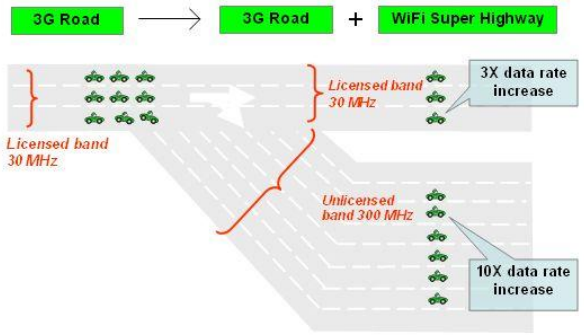

Figure 1.1: The difference of Speeds and Licensing norms between mobile networks and wireless networks

From a scientific point of view, the world of wireless communications is one of the biggest engineering success remarks. The road from the first experiments with radio communication by Guglielmo Marconi1 in the 1890s, to mobile radio communication has been pretty long. As we know, the first generation (1G) mobile radio systems that were based on the analog transmission for the speech services. Before understanding the complex 3G mobile-communication systems of today, it is important that we should first understand where they came from and how the cellular systems have came from an expensive technology for a few selected individuals to today's global mobile-communication systems which are used by almost half of the world's population. The developing mobile technologies has changed, from being a national or regional concern, to becoming a very complex task which is undertaken by global standards developing organizations such as the 3GPP (3rd Generation Partnership Project) and involving thousands of people.

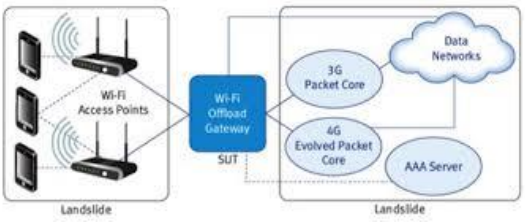

Figure 1.2: Toggle data between Wi-Fi networks and Mobile networks

Due to the increasing demands for high data rates and high quality mobile communication services, mobile communication technology has evolved quickly. The mobile network operators be supposed to address the increasing demand for the data services especially for the Smart phones users. The upcoming new generation of Smartphone's such as iPhones, BlackBerry, Android and Windows Mobile can work

together with 2G/3G/4G enabled mobile networks and wireless networks for accessing the Internet same as the laptops and net books are bringing Internet experience. The great opportunity and a big challenge for the mobile communications industry is the exponentially growing amount of mobile data traffic which is communicated over cellular networks. The uses of many popular social networking services, Mobiles are opening the door for millions of Terabytes to enter into the mobile networks. Because of the increasing popularity of various applications for Smart phones, 2G/3G/4G mobile networks are currently overloaded. As a result of this, revenues are of much concern for the mobile network operators.

In this research work, the main focus is addressing how to overcome the mobile network congestion by offloading a portion of mobile data traffic to complementary wireless access networks using the Wi-Fi. Data offloading means that the use of complementary network technologies for delivering the data, which is originally targeted for the transmission over the cellular networks, in order to save the money and relieve the mobile telephony network.

1.1 Drawbacks in existing system

1. The existing scheme ensures the data privacy, integrity and confidentiality during its propagation between the network access points, routers and the data offloading gateway.
2. The existing model does not ensure the data privacy during the data propagation between the source node and the access point.
3. The existing scheme uses the IPSec, which uses the encryption, which is not considered very secure now-a-days.
4. IPSec uses the predictive methods for the authentication purposes, which are prone to the various types of security attacks.

2. PROBLEM FORMULATION

The mobile services used are offering voice calls, video calls, SMS, internet browsing and various other applications support in today's smart phone era. These all are the services that made the mobile networks more congested day by day with rise in the number of the users. The D2D (device to device) is emerging as a popular trend in today's mobile data offloading practices. Mobile data offloading is generally availed by the emergence in the smart phone technology. In the base paper, the authors have developed a new technique to provide the solution for the 3G networks.

The 3G network data has been offloaded into the Wi-Fi networks using the opportunistic communications and social participation. The major goal of the proposed work is to reduce the weight from the 3G cellular networks. The technique has been known as opp-off. The authors have used the combination of Heuristic, Greedy and Random algorithms to manage the data between the two networks i.e. 3G networks and the Wi-Fi networks.

In this research the Wi-Fi or Wi-Max networks which connect the people with the internet are called social participation networks. The presented scheme can be considered as the insecure networks because the mobile data offloading technique does not offer any kind of data security, confidentiality and integrity for the user data between two cellular users, while they are communicating from cellular cluster to Wi-Fi mobile cluster. Mobile frequency band licenses are quite expensive for the mobile companies. Off loading the cellular data in Wi-Fi networks may save larger amounts because Wi-Fi requires no licensing and ranges up to 300 MHz band, whereas mobile network band ranges between 10-30 MHz only.

We are proposing a new mobile data offloading technique which will offer the application based mobile data offloading architecture to solve the network lag problems especially in the campus Wi-Fi or Wi-Max networks. On the other hand, the IPSec based data security model is proposed to ensure the data security of the internet users connected with WLAN clusters. The WLAN user data is injected or offloaded to the internet leased line based connectivity. The WLAN cluster data security has been ensured while offloading it into the Internet cluster using the secure data propagation techniques using the end to end encryption standards.

3. PROPOSED MODEL

The proposed model will be using the combination of mobile data offloading; 3-level secure authentication and RSA encryption based secure architecture for the data exchange between the cellular and Wi-Fi networks. The proposed technique will be made secure using the 3-level secure authentication before sharing any kind of data between the mobile network and the cellular network. The proposed technique will then use data encryption to ensure the secure voice call communication between Mobile offload cluster (Wi-Fi cluster) and Cellular network. The secure data architecture will be capable of handling the secure voice call sessions between the cellular and Wi-Fi networks facilitate the secure data sharing on higher data transfer rate. The proposed model will increase the security of the calls made between the mobile offload users in the Wi-Fi cluster and cellular cluster and will reduce the load from the cellular networks in the real time.

4. SCOPE OF THE STUDY

Mobile data offloading is the process of transferring the mobile data in the local networks like Wi-Fi or WiMax. The mobile data offloading techniques are used to reduce the operating cost of the cellular setup and other operations. The mobile data is generally offloaded in the campus networks; the city WiMax networks and the other large local networks with a large number of connected users from their cell phones. The mobile data offloading techniques that are made possible using the mobile applications to register the cellular users accessing through the local networks to their cellular service providers. The cellular service providers use the registration information for the call forwarding. The call forwarding in the local networks is done using the controller configured in the local network. The security of such architecture is also a very important aspect. For the purpose of security measures of such type of architectures, the existing scheme has proposed the use of the IPSec based secure tunnel. The existing system has been designed to ensure the security of the mobile users in the offloading architectures. The existing scheme has been used for the security of the data travelling between the access nodes or access points, which can ensure the data privacy during its transmission in the backbone network. The major problem arises when the data is being replicated or hacked during its propagation between the source node and the access point. The proposed model aims at the security of the data at all levels of communication unlike the existing model.

5. METHODOLOGY

We will start our research project by conducting a detailed literature review on the mobile data offloading to know the problems in the detail. Then, a mobile data offloading mechanism would be designed to facilitate the campus network mobile users through Wi-Fi networks. The simulation

would be implemented using Network Simulator (NS2). The obtained results would be examined and compared with the existing data offloading mechanisms to address the similar issues.

6. CONCLUSION

The mobile data offloading has been performed into the Wi-Fi or Wi-MAX networks in order to extend the network availability and to reduce the cost on the same period. These architectures will depend upon the application level connectivity between the cellular users and their centralized SIM based user registration services and the call setups. The application level approach will increases the threat of the attacks on such architectures. In order to reduce the probability of attacks on the MESHNETs, there must be appropriate security solution. There is no strong security architecture present yet to ensure the security of MESHNETs. The proposed model will employ the methods to ensure the security of the MESHNETs by offering the multi-variate security architecture based on the multi-level authentication with message encryption. The results of the proposed model will be concluded in the form of transmission delay, throughput, network load, probability of detection & false alarm, etc.

7. FUTURE WORK

In the future, the proposed algorithm would be implemented the following proposed experimental design. The several types of analysis would be performed on the implementation setup in order to obtain several types of parameters from the model. In the future, the proposed model would be improved or applied to other platforms to judge its performance.

8. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

9. REFERENCES

[1] Han, Bo, et al. "Mobile data offloading through opportunistic communications and social participation*." Mobile Computing, IEEE Transactions on 11.5, pp. 821-834, IEEE, 2012.*

[2] Han, Bo, Pan Hui, and Aravind Srinivasan. *"Mobile data offloading in metropolitan area networks." ACM SIGMOBILE Mobile Computing and Communications Review 14.4, pp. 28-30, 2011.*

[3] Lu Xiaofeng, Hui Pan, P. Lio, *"Offloading mobile data from cellular networks through peer-to-peer Wi-Fi Communication: A subscribe-and-end architecture.*

[4] M.H. Qutqut, F.M. Al-Turjman, H.S. Hassansein, *"MFW: Mobile femtocells utilizing WiFI: A data offloading framework for cellular networks using mobile femtocells", ICC, vol. 1, pp. 6427-6431, IEEE, 2013.*

[5] Mi. Jeong Yang, Soon Yong Lim, Hyeong Jun Park, Nam Hoon Park, "*Solving the data overload: Device-to-device bearer control architecture for cellular data offloading", IVTM, vol. 8, issue 8, pp. 31-39, IEEE, 2013.*

[6] Migault, Daniel, Daniel Palomares, Hendrik Hendrik, and Maryline Laurent. *"Secure IPsec based offload architectures for mobile data." In Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, pp. 95-104. ACM, 2014.*

[7] Petros S. Bithas et. al., "Hybrid Cellular/WLAN with Wireless Offloading: Enabling Next Generation Wireless Networks", IJSAC, vol. 1, pp. 1-29, IEEE, 2013.

[8] Subramanian Vasudevan, Kathiravetpillai Sivanesan, Satish Kanugovi and Jialin Zou, *"Enabling Data Offload and Proximity Services Using Device to Device Communication over Licensed Cellular Spectrum with Infrastructure Control", VTC Fall, vol. 78, pp. 1-7, IEEE, 2013.*

[9] Thomas, Giles, et al. "Wave-induced motions of gas cat: A novel catamaran for gas processing and offloading*." ASME 2009 28th International Conference on Ocean, Offshore and Arctic Engineering. American Society of Mechanical Engineers, 2009*.

[10] Lee, Kyunghan, Joohyun Lee, Yung Yi, Injong Rhee, and Song Chong. "Mobile data offloading: How much can WiFi deliver?." *IEEE/ACM Transactions on Networking (TON)* 21, no. 2 (2013): 536-550.

[11] Sankaran, C. B. "Data offloading techniques in 3GPP Rel-10 networks: A tutorial." *Communications Magazine, IEEE* 50, no. 6 (2012): 46-53.

[12] Gupta, Vishal, and Mukesh Kumar Rohil. "Enhancing WiFi with IEEE802. 11u for mobile data offloading." *International Journal of Mobile Network Communications & Telematics (IJMNCT)* 2, no. 4 (2012): 19-29.

[13] Gupta, Vishal, and Mukesh Kumar Rohil. "Enhancing WiFi with IEEE802. 11u for mobile data offloading." *International Journal of Mobile Network Communications & Telematics (IJMNCT)* 2, no. 4 (2012): 19-29.

[14] Han, Bo, Pan Hui, V. S. Kumar, Madhav V. Marathe, Guanhong Pei, and Aravind Srinivasan. "Cellular traffic offloading through opportunistic communications: a case study." In *Proceedings of the 5th ACM workshop on Challenged networks*, pp. 31-38. ACM, 2010.

[15] Liu, Shu, and Aaron Striegel. "Casting doubts on the viability of WiFi offloading." In *Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design*, pp. 25-30. ACM, 2012.