JSPWN
Journal of Signal Processing and Wireless Networks

Smarphone Ad-hoc Network Adoption using Zombie Application and Assessment of MAC Address Spoofing

S. Mythili, E. Shalini*, A.M. Shriram

Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, India
**Corresponding author email : shalinie@bitsathy.ac.in*

ABSTRACT

This great hectic world has filled with enormous things which are unusual or atypical at times, simply called as crisis. It can be prevented or lessened if critical knowledge is identified in advance. Due to the happening of natural or man-made disasters there is a possibility for the people located in that zone gets trapped and difficult to survive by the traditional cellular network destruction which makes paltry communication . At that instant the communication can be carried out by creating a Smartphone ad-hoc network through Wireless Fidelity (Wi-Fi) using the developed android application named as “Rescue-chat”. This application has developed by having the Android studio as a central platform and it is applicable for timely communication in-case of any panic situation. The extensive view of this work is also focused on security of Wi-Fi access though analyzing the MAC address spoofing which is feasible in wireless network.

ARTICLE HISTORY Received 17 November 2017 Revised 16 January 2018 Accepted 20 January 2018

KEY WORDS Smartphone, Wireless Ad-hoc Network, Emergency Application, Wi-Fi hotspot, MAC Address Spoofing

1. Introduction

The advent of Smartphone technology is a combination of a cell phone and a hand-held computer which is considered to be a turning point in history by its salient features like data storage, internet access, e-mail facility, wireless network capability etc. It is a ubiquitous device which brings the entire world in a human palm. The increased connectivity and accessibility of this device enhances the relationships and makes the friendly environment easily even though the communication is beyond the line of sight. It would be very different to imagine a world without smart phones. The number of smart phone users in India is estimated to reach around 244 million by the end of 2017 [4].One of the most attractive thing in this tool is the variety of android applications and its uses.

Disasters such as earthquake, floods etc are the unexpected events which cannot be measured in advance. So there is a need for the engineers to contribute technically to help the trapped survivors to save their life through rescue team. Crisis management is an embryonic area in which there is a scope for researchers to foreseen the problems and exploring several solutions accordingly to the situation. It is implicitly known that the Smartphone technology is able to create a wireless network for communication purpose. So it is applicable for disaster management by having several devices for multi hop communication in a constrained area and forming an ad-hoc network which are typically dynamic and scalable because of the device mobility and decentralized management using Wi-Fi technology. Wireless ad-hoc network helps for sharing real time information which is essential for the rescuers to help the victims who are trapped in a critical situation unexpectedly.

The Wi-Fi communication is possible through radio wave propagation so it more vulnerable to various attacks. This is considered to be a problematic one in an emergency communication. One of the possible and most common attacks is MAC Address spoofing which is a base for several attacks like Denial of Service, Man in the Middle Attack, ARP Spoofing etc. So the counter measures to overcome this are elucidated in detail for the proper Wi-Fi communication.

1.1 Risk Assertion

There are several emergency applications which are readily available to access through android phones. Emergency call facilities are also offered but there is a lack of timely communication when applicable to the crisis situation. Since the created network is a wireless network there is a possibility for several security threats.

1.2 Objective

The main objective of this proposed research is

- To develop an android application for emergency communication which will work even there is no cellular network.
- To create an ad-hoc network using Wi-Fi by having multi application users.
- To scrutinize MAC Address Spoofing attack

2. Decision Making Process

The Fig. 1 represents the flow of decision making model. Initially data gathering is essential which can be attained using some of the external sources like media, Internet etc. for the risk analysis. Then the evaluation of alternatives is made by emotion regulation and approaches the safest alternative, nothing but the 'Rescue - chat' app usage at the time of crisis. This decision is made by considering the internal and external factors. Network coverage is essential and helps to intimate the status and situation of the victims through mobile communication so it is considered as an internal factor. A finite time for response is considered as an external factor in order to get timely help from the rescue team to prevent the trapped survivors.

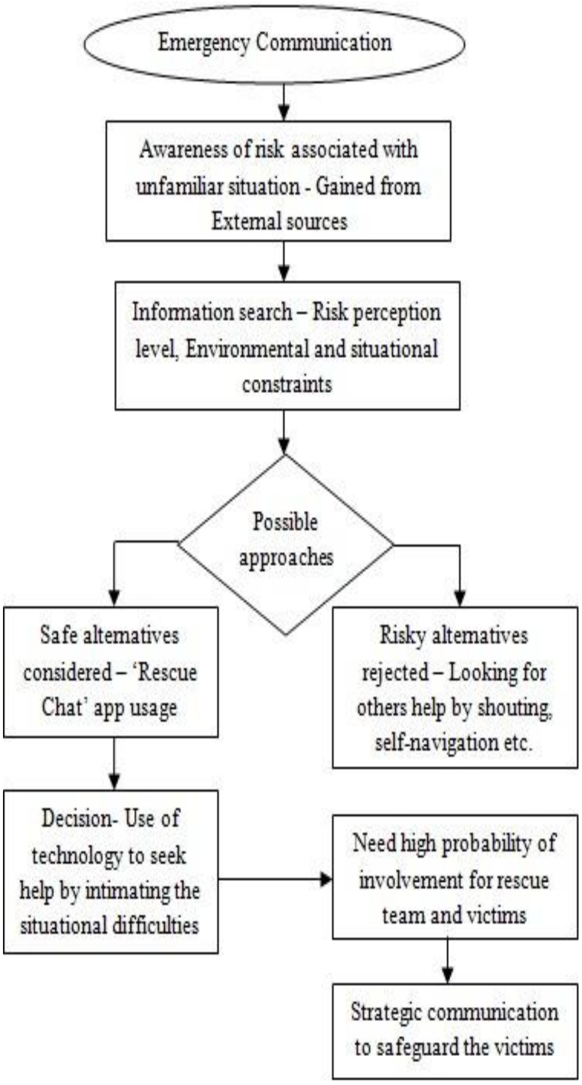

Emergency Communication
Awareness of risk associated with unfamiliar situation - Gained from External sources
Information search – Risk perception level, Environmental and situational constraints
Possible approaches
Safe alternatives considered – 'Rescue Chat' app usage
Risky alternatives rejected – Looking for others help by shouting, self-navigation etc.
Decision- Use of technology to seek help by intimating the situational difficulties
Need high probability of involvement for rescue team and victims
Strategic communication to safeguard the victims

Fig. 1. Model of Decision Making Process

3. Description of Developed Android Application

An android application named "Rescue - chat" is developed which helps to send the rescue messages by creating an infrastructure less or Ad-hoc network using Wi-Fi hotspot [6].

The app (Fig. 2) app is developed using Android Studio which is an official Integrated Development Environment (IDE) of android and also supports variety of android applications easily.

To Communicate and perform some rescue operations the open Wi-Fi network is crucial which facilitates with faster transfer rate compared to Bluetooth. With this booming wireless technology effectiveness of Wi-Fi would be appreciable and used in wide number of applications.

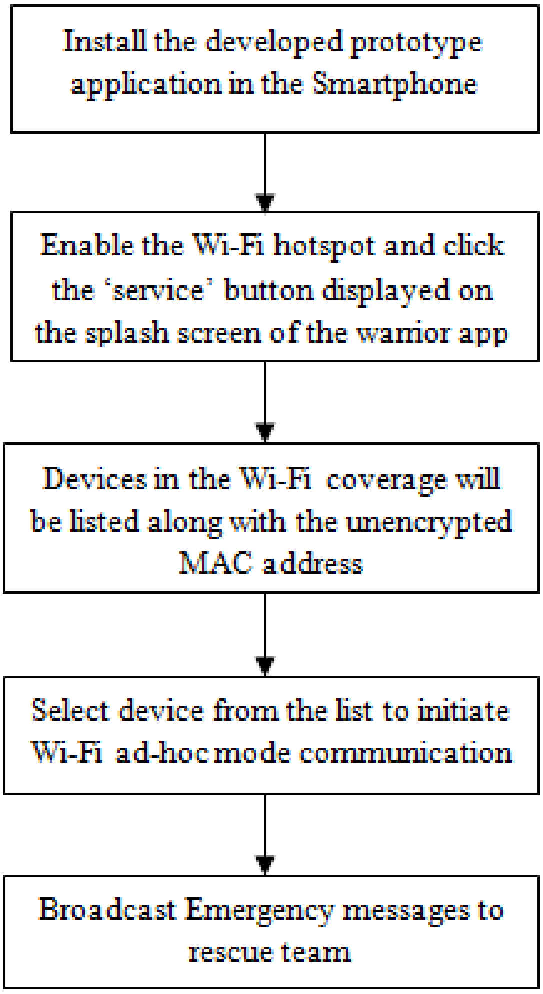
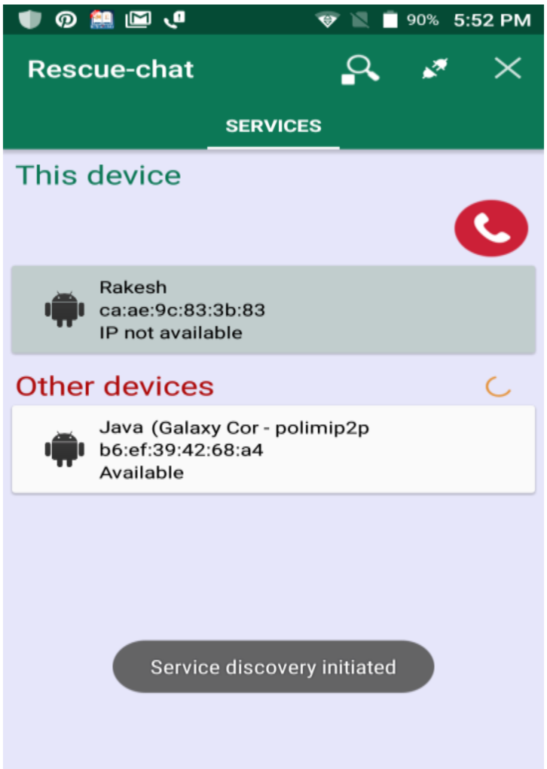

Install the developed prototype application in the Smartphone
Enable the Wi-Fi hotspot and click the 'service' button displayed on the splash screen of the warrior app
Devices in the Wi-Fi coverage will be listed along with the unencrypted MAC address
Select device from the list to initiate Wi-Fi ad-hoc mode communication
Broadcast Emergency messages to rescue team

Fig. 2. Communication Flow of Developed Application

4. Ad-Hoc Network Adoption

The multi hop communication takes place by selecting any of the listed available devices present in the Wi-Fi coverage, helps to broadcast the rescue messages instantly as shown in Fig. 3.

The communication is possible by creating an ad-hoc network which is an infrastructure-less network created on the fly and have no central access point to direct and monitor the flow of communication. The continuous transformation of communication in the network somehow reaches the destination and the proper rescuing operation is carried out successfully.



This device

Rakesh
ca:ae:9c:83:3b:83
IP not available

Other devices

Java (Galaxy Cor - polimip2p
b6:ef:39:42:68:a4
Available

Service discovery initiated

Fig. 3 Data Communication through service discovery initiation

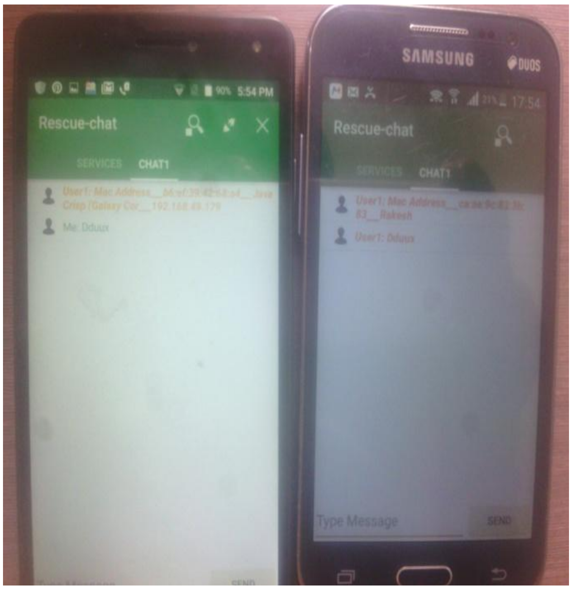


Fig. 4 Snapshot of two terminal communication through Rescue - chat App

5. Mac Address Spoofing

Due to the transparency of the wireless transmission medium, any unauthorized user can observe the transmission process in a network. In that case Wireless spoofing attacks are easy to launch and can malfunction the system directly. Through the MAC Address spoofing or IP Address spoofing the intruder successfully masquerade as a legitimate user in-order to access the resources available in the allotted network [6].

5.1 Scenario of MAC Spoofing Attack

- The unauthorized user scans the MAC address of the users surrounding in the wireless environment.
- This scanned information helps him to change his MAC address as an authorized user to collapse the communication taking place in the critical situation using the fake MAC address.

It is considered to be a serious threat in wireless network. Some of the MAC spoofing Detection methods and its prevention techniques are discussed below.

5.2 MAC Spoofing Detection Techniques

This is the initial step to protect the network from the rogue devices so this process is an essential one.

- MAC Address Spoofing is detected in wireless networks using the Received Signal Strength (RSS) with the help of two sensors.
- Some of the traditional methods to prevent spoofing attacks are cryptographic based authentication by having secured key management among the legitimate users; Utilizing physical properties associated with wireless transmission to detect the intruder, MAC Address Filtering technique etc [2].

Ongoing work is focussed on limiting the spoofing of MAC Address which is considered as a global unique identifier to the Data Link layer. It is used as an authentication factor to access the network. So it is highly focussed to provide security while authentication and de-authentication process takes place for data communication.

6. Conclusion

Smartphone network adoption in time of crisis is an effective way and also acts as a handy safe guard. Rescue - chat app is considered to be a good measure for emergency communication. And an optimistic way of network usage is possible by restricting various kinds of attacks which affect the wireless networks. MAC Address spoofing is an unusual activity and can be limited by proper authentication process and maintaining strict MAC addresses filtering.

References

1. Pahwa, Payal, Gaurav Tiwari, Rashmi Chhabra (2010), “Spoofing Media Access Control (MAC) and its Counter Measures" International Journal of Advanced Engineering & Application, pp. 186–192.
2. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe and Jerry Cheng (2013),“Detection and Localization of Multiple Spoofing Attackers in Wireless Networks” IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, pp. 44-58.
3. Aiman Abu Samra and Razmi Abed (2010), “Enhancement of Passive MAC spoofing Detection Techniques” International Journal of Advanced computer science & Applications, Vol. 1, No.5, pp. 108-116.
4. Mythili, S. and Shalini, E (2016), “A Comparative Study of Smart phone Emergency applications for Disaster Management,” International Research Journal

of Engineering and Technology (IRJET), Vol.3, No. 11, pp. 392-395.

5. Zongqing Lu, Guohong Cao and Thomas La Porta (2017), “TeamPhone : Networking Smart phones for Disaster Recovery,” IEEE Transactions on Mobile Computing, Vol. 16, No, 12, pp. 3554-3567.
6. Sungmo Jung, Jong Hyun Kim, Seoksoo Kim (2011), “A Study on MAC Address Spoofing Attack Detection Structure in Wireless Sensor Network Environment” Advanced Communication and Networking. Communications in Computer and Information Science, Vol. 199. pp. 31-35
7. Sathyaprakash. P, Prakasam. P (2017), “Enhanced approach for wireless sensor network based on localization, time synchronization and quality of service routing”, Cluster Computing, doi : doi.org/10.1007/s10586-017-148, pp. 01-10.
8. Zhuo Lu, Wenye Wang and Cliff Wang (2014), “Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications”, IEEE Transactions On Mobile Computing, Vol. 13, No. 8, pp. 1746-1759.
9. Cardenas, Edgar D (2013), "MAC Spoofing--An Introduction", GIAC Security Essentials Certification, SANS Institute, pp. 01-15.
10. Pahwa, Payal, Gaurav Tiwari, Rashmi Chhabra (2010), “Spoofing Media Access Control (MAC) and its Counter Measures" International Journal of Advanced Engineering & Application, pp. 186–192.
11. Sathyaprakash. P, Prakasam. P (2017), “Proposed Energy Efficient Multi Attribute Time Slot Scheduling Algorithm for Quality of Service in Wireless Sensor Network”, Wireless Personal Communications, Vol. 97, No. 4, pp. 5951-5968.