A Survey on Wireless Network Dependent Dynamic Security

Mr. Shashank Yadav[1] Mr. Kailas Ware[2] Mr. Raju Chougale[3] Prof. Praladh Gamare[4]
[1,2,3]B.E. Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Rajendra Mane College of Engineering and Technology, Ambav, Mumbai University

Abstract— CONSEC Android application is used to scan nearby wireless access points such as Wi-Fi-Routers, Wi-Fi-Repeaters, Wi-Fi-Portable Devices etc. that broadcast on 2.4 GHz of frequency. It enables the scanning of multiple Wi-Fi access points in a short period of time. Depending upon the name and id of the Wireless Access Points, it executes specified processes in the device. All Wireless accessing and connecting techniques as well as authentication technique for security within the application are discussed in various sections of the paper. The main aim of our project is to detect and connect wireless access points and execute actions related to security or general device features.

Key words: WAP (Wireless Access Point), CONSEC (Application Name)

I. INTRODUCTION

Wireless APs are often used to connect to Wifi portable devices for internet or sharing purpose. When one scans a wireless network in a smart phone, it can just connect to it. The connection to WAPs is to connect to a wider network like Internet. Apart from data transfer, connecting to WAPs are not considered for other functionalities. You would use CONSEC application to connect to secure and open WAPs and carry out more functionalities than its traditional one. The other functionality are related to security like muting of microphone and speaker module when in meeting scenario and enabling note taking feature when in presentation or briefing scenario. User gives input by activating the application in its device, the device should be in the known WAP network zones to connect to them and carry out executions of different specified processes automatically upon dynamic changing of WAPs.

II. PROPOSED SYSTEM

The CONSEC application is simply connecting to WAPs usually broadcasted in offices and public places. For the processing of output, CONSEC uses the name and id attribute of the concerned WAP to verify, connect and execute assigned processes. Output of CONSEC is to put the user's device either to a high secure mode or perform general tasks as basic as note taking. Also it is useful for stopping hackers to access information via network as all the connection information is reset each time CONSEC is activated or de-activated.

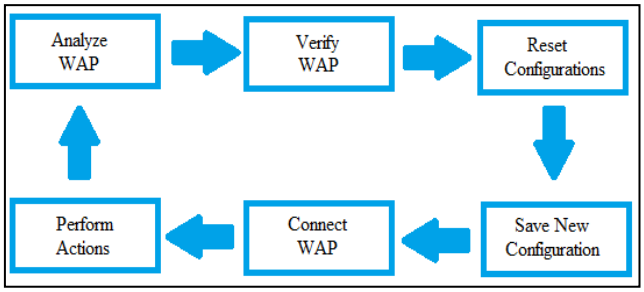


Fig. 1: System Block Diagram

The previous ideas related to such projects have not discovered and explored the possibilities of such dynamic system that provides security as well as other features. In the proposed system, the application takes in the input in the form of WAP, which further gets verified and processed for verification and executions of assigned actions constantly.

III. METHODOLOGY

In order to achieve the accuracy, best performance, automatic mechanism and authentication, we have designed a Pyramid algorithm.

A. Pyramid Algorithm

Here we are using a verification triggered level based system and used languages like JAVA and XML for developing project. We are begun with collecting all the name of scanned WAPs in the vicinity. The collected lists of WAPs are compared with each, using the signal strength attribute to generate the best and strongest WAP. As soon as the process of generating the strongest WAP is completed, the application waits for the user to activate. Upon activation, the achieved WAP's SSID and BSSID is compared with the known WAP's SSID and BSSID that is already stored inside the application. On complete verification and validation, all the previous WAPs saved configuration of connection information in the device is reset. The device is stacked with new WAPs configuration of connection information and gets connected to the required one. The further verification process checks the SSID and BSSID of the connected WAP and executes appropriate processes that were assigned to the particular, verified and connected WAP. In case of a confidential scenario the output, upon connection the device gets into more secure mode by muting microphone and speakers for avoiding unauthorized access or disrupting the scenario. While the other scenario will be a presentation or a briefing where Note taking feature is activated.

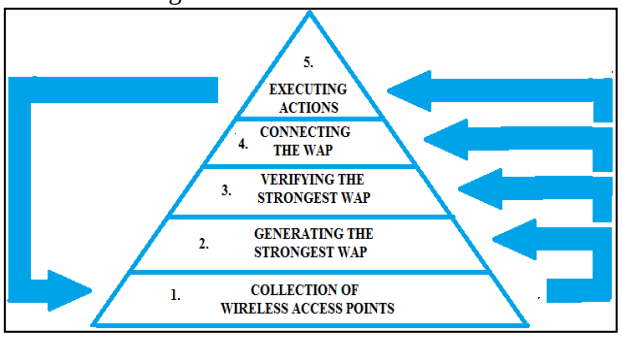


Fig. 2: Pyramid working

IV. IMPLEMENTATION

Here we are using Android Studio for writing java source code for creating various processes and xml source code for designing interface in the application. We begin with the collection of WAPs through the Scanner method inside an

array. This Scanner method is activated as many times as the Intent "SCAN_RESULTS_AVAILABLE_ACTION" is broadcasted by the android operating system. This Intent is called constantly by the operating system as devices changes location eventually and new and efficient WAPs might be available. Along with stacking scanned WAPs in array Scanner method also performs the comparison of the collected WAPs in the array. This comparison is based on the .level attribute of each WAP signal which is the strength of the particular signal in dBm. Upon comparison the Scanner method generates a single signal with highest value of strength and stores it in the bestSignal attribute. Now, upon activation that is input provided by the user, Intent is released and the process of the application from scanning, generating best WAP, resetting of previous configurations and applying of new one's takes place. As these processes are completed the desired WAP is connected. Upon connection, the scanner method automatically calls wifi profile method which verifies the bestsignal through SSID and BSSID attributes. These attributes are compared with the attributes of the saved configurations. These configurations are used to determine the type of scenario, whether a high security demanding one or some general task. The executions of assigned actions are called through different methods. In case of not finding a known WAP the application keeps scanning and accumulating WAPs continuously.

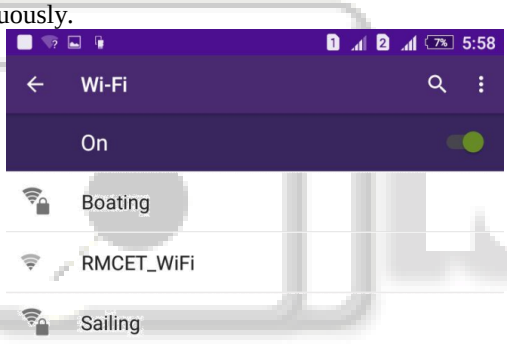
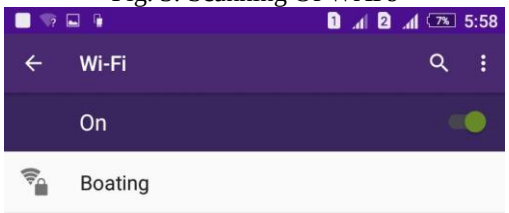
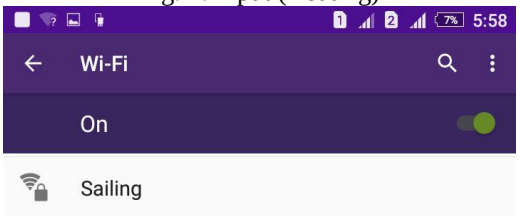


Fig. 3: Scanning Of WAPs




```
wc1.SSID = "Boating";
wc1.BSSID = "C4:6E:1F:72:1B:B8";
wc1.preSharedKey = "\"" + "9876543210" + "\"";
```

Fig. 4: Input (Boating)




```
wc3.SSID = "Sailing";
wc3.BSSID = "F4:9F:F3:B4:89:6D";
wc3.preSharedKey = "\"" + "1234567899" + "\"";
```

Fig. 5: Input (Sailing)

The output of the application when taken into consideration includes two scenarios. First can be explained as a high security demanding mode. Devices like smart phones can be used for recording confidential conversations. The idea of deactivating features like muting of Microphone and device being on vibrate mode increases the security from the user side towards the environment. The other output is a simple task as simple as taking notes. Considering few scenarios where note taking becomes crucial, scenarios like presentations, briefing, feedback in stores etc. The application provides a simple interface for taking notes which are saved inside a file, not accessible by user or anyone. The note taking interface is immediately activated when the assigned SSID and BSSID is found as the connected WAP. The notes that are taken during the respective scenario can be viewed offline.

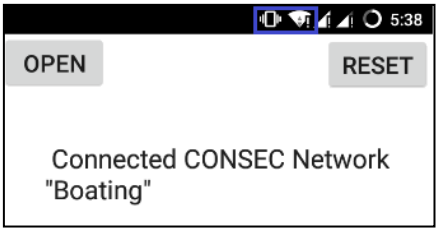


Fig. 5: Output (Boating)

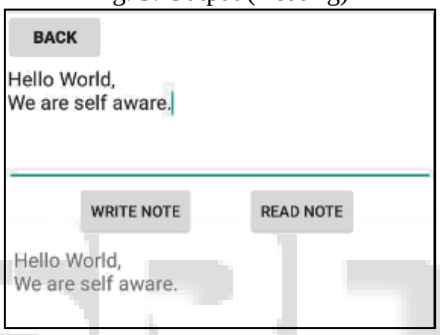


Fig 6: Output (Sailing)

V. Conclusion

The proposed system will demonstrate the plan and implementation of building an application which will determine more scenarios and provide more functionality with higher accuracy. The broadness and flexibility of the application increases collective chances of having many applications in industry. The scope of controlling components for security purpose is very efficient and dynamic. The addition of components and controlling them according to user needs, these are the feature that we intend to achieve in future. The accuracy of the project is more than 90% in huge infrastructures and more than 75% in typical infrastructures.

Acknowledgement

No project is ever complete without the guidance of those experts who have already traded this before and hence became master of it and as a result, our leader. So we would like to take this opportunity to thank all those individuals who have helped us in visualizing this project.

We express our deep gratitude to our project guide and coordinator Prof. Gamare P. S., for providing timely assistant to our query and for his guidance in choosing this project and also for providing us all this details on proper presentation of this project.

We extend our sincere appreciation to all our Professors from RAJENDRA MANE COLLEGE OF

ENGINEERING & TECHNOLOGY for their valuable time during the designing of the project. Their contributions have been valuable in so many ways that we find it difficult to acknowledge them individual.

We are also grateful to our HOD Mr. Naik L.S. for extending his help directly and indirectly through various channels in our project work.

REFERENCES

[1] "Context Based Access Control For Mobile Devices." Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino Computer Science, Cyber Center and CERIAS, Purdue University, West Lafayette, IN 47907, USA .
[2] Wikipedia, "Yureka A5210,", "Cynogen"
[3] G. Zhang and M. Parashar, "Dynamic context-aware access control for grid applications," in Grid Computing, 2003. Proceedings. Fourth International Workshop on, 2003, pp. 101–108.
[4] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca, "Geo-rbac: A spatially aware rbac," ACM Trans. Information System and Security, vol. 10, no. 1, 2007.
[5] https://www.stackoverflow.com, "External file generation for text containing file.
[6] https://www.androidtutorial.com, "Handling the activity life cycle of Android application.
[7] https://www.youtube.com,"Android Tutorials For Beginners.
[8] https://developer.android.com, "Android Studio Installation and Setup."
[9] https://code.tutsplus.com, "Security through authentication process.

