GSM-CommSense: A novel inexpensive way to sense the environment using RF bands

Abhishek Bhatta
Electrical Engineering Dept.
University of Cape Town
Cape Town, South Africa
bhattaabhishek0@gmail.com

Amit Kumar Mishra
Electrical Engineering Dept.
University of Cape Town
Cape Town, South Africa
akmishra@ieee.org

***Abstract*—We have recently proposed a scheme to use the channel equalization blocks of telecommunication systems to sense changes in an environment. We named this system communication based sensing or CommSense system. For the initial proof of concept, we implemented a basic system on a laptop and a software defined radio receiver, BladeRF. Since the system is under-determined we introduced Application Specific Instrumentation (ASIN) on which the prediction system of CommSense is based. We got some encouraging results therefore we decided to implement this system as a real-time environment detection system.**

Keywords—Commensal Radar, CommSense, GSM, SDR

I. INTRODUCTION

Radar systems have originally been designed for military specific applications. In the recent past many interesting ways of using Radio Frequency (RF) spectrum for radar applications have been under research. One such concept is commensal radar, that uses signals of opportunity to detect targets without affecting the functionality of the parent system [1]-[3].

In this work we describe another implementation of a commensal radar system which we named Communication based Sensing (CommSense) [4]-[7]. Every digital communication system transmits a known bit sequence embedded within its frames in order to estimate and equalize the effects of the environment on the rest of the signal. In CommSense we use these known bits to extract the channel information which is used to characterize the immediate environment around the receiver. For the current implementation, we have chosen Global System for Mobile Communication (GSM) as the parent system and thus named this implementation as GSM-CommSense.

In order to reduce the cost of implementation of the GSM-CommSense system, we used readily available off-the-shelf hardware and open source software. The data is received in a BladeRF, which is a Software Defined Radio (SDR) hardware which receives the wireless GSM broadcast frames, samples them and passes these sampled frames to the processing unit. The Raspberry pi 3 is used for processing the samples received and extracting the channel information. This information is then sent through Transmission Control Protocol (TCP) through WiFi to a laptop. Rest of the processing is done in the laptop.

In order to reduce the cost of implementation of the GSM-CommSense system, we used readily available off-the-shelf hardware and open source software. The data is received in a BladeRF, which is a Software Defined Radio (SDR) hardware

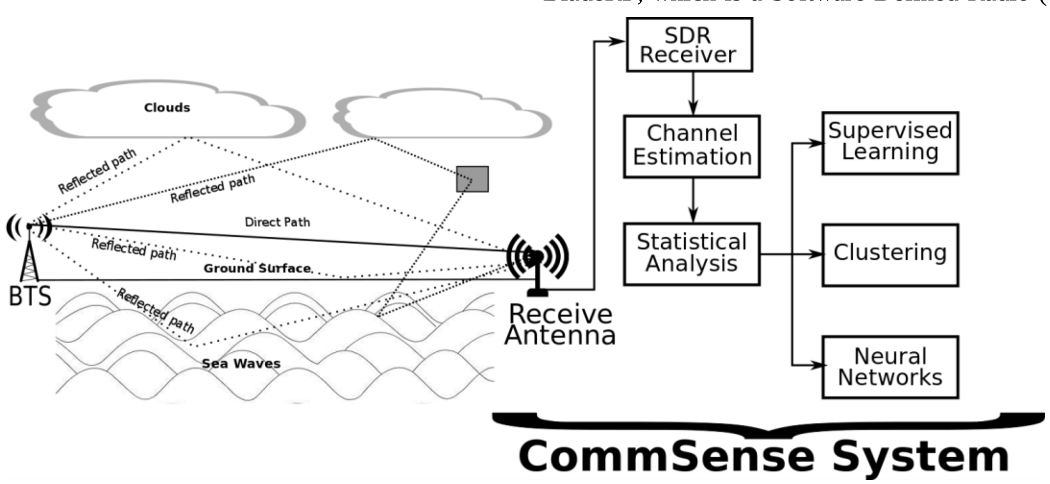

Figure 1: Basic architecture of the CommSense system.

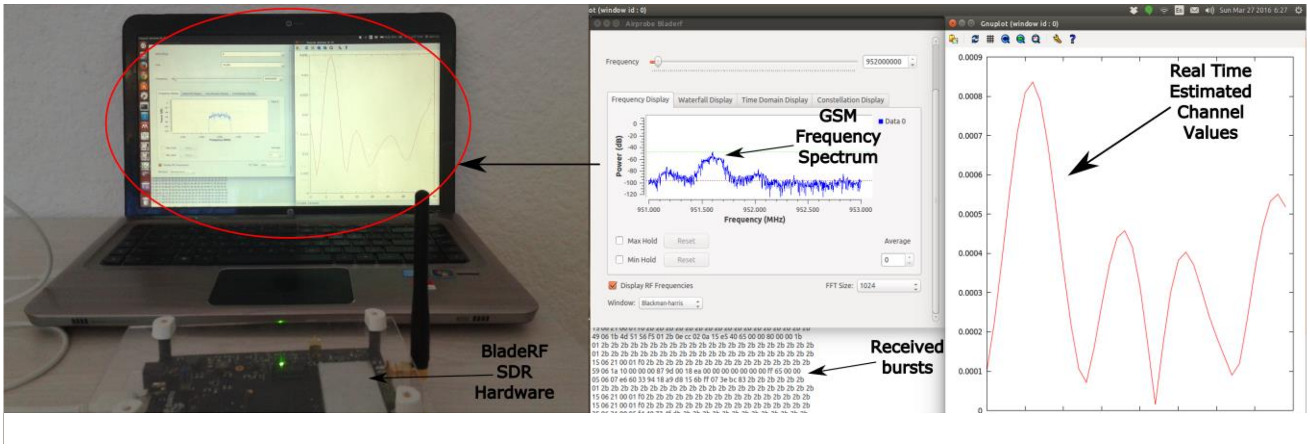

Figure 2: Initial implementation of the GSM-CommSense system.3

which receives the wireless GSM broadcast frames, samples them and passes these sampled frames to the processing unit. The Raspberry pi 3 is used for processing the samples received and extracting the channel information. This information is then sent through Transmission Control Protocol (TCP) through WiFi to a laptop. Rest of the processing is done in the laptop.

II. Proof of Concept

In order to prove our hypothesis that channel equalization blocks of communication systems can be used to analyze the immediate environment of the receiver, we needed a system that can receive and extract the channel information in real-time.

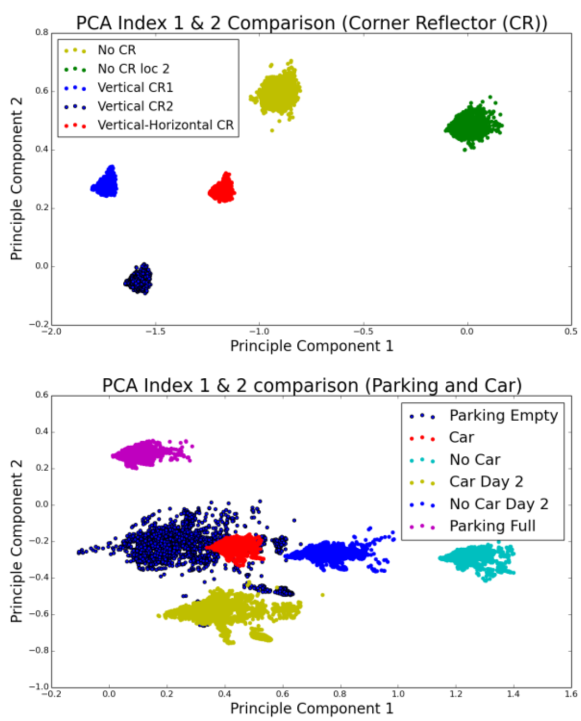

Figure 3: PCA plots showing the first two principal components of datasets captured in different environmental conditions.

Figure 2 contains the image showing the initial implementation of the GSM-CommSense system. Here the receiver is BladeRF which is directly connected to the laptop on which GNURadio is running. The plots on the right side of Figure 2 shows the screenshot of the laptop screen. Here the estimated channel information from GSM frames in real-time is plotted, this information is also saved in a file on which the rest of the analysis is performed.

III. Design Challenges and Solutions

The first design challenge faced during the implementation of GSM-CommSense was to extract the channel information from real GSM base station broadcast data. The solution was found when we decided to use GNURadio for the implementation as there are predefined libraries that can receive the GSM signals and decode them. The most useful library was the gr-gsm library, which contains the blocks needed to receive and decode the GSM signals. We made some changes in the receiver blockset to provide the extracted channel information along with the timestamp information as an output port. This channel information is then used for further analysis.

The next hurdle was to analyze the extracted channel information in order to find out if it is enough to distinguish between the different environmental conditions. In the quest to find a good analysis tool we stumbled upon PCA, which is an algorithm that reduces the dimensionality of possibly correlated data to uncorrelated components. Figure 3 contains the PCA plots showing clusters of dataset for different environmental conditions. Figure 3(a) shows the clusters when there are corner reflectors placed in different orientation near the receive antenna. Figure 3(b) shows the clusters at a parking space in different orientations such as parking space full, parking empty, car and no car in the around 100 meters of the receiver in two different days. The data is clustered separately and that proves this can be an effective way to sense the environment.

The next challenge we faced was the fact that this system is highly under-determined. This is because we are using only a part of the GSM frames to extract the channel information, specifically the central 26 bits of a 148 bit frame. Which only provides us with 48 points of channel information per frame which is approximately 577 µs. This information is not enough to get a picture of the scenario, thus we developed a new framework called Application Specific Instrumentation Framework (ASIN). The basic idea of ASIN is to train the system to detect a particular scenario, for example if we want to detect if a person in a particular room is carrying a weapon, we train the system with this scenario and check the prediction of the system on a new dataset based on the training. This proved to be useful in classifying the events with 75 - 80% of accuracy.

Now since the above three challenges are resolved a new challenge arose, in which we need to increase the accuracy of this system. This is still an outstanding issue but some of the perceived solutions to this issue is by increasing the sensitivity of the system as with higher sensitivity more minute changes can be determined. Another way we can increase the efficiency of the system is by using directed receive antennas to observe only a specific region instead of an omnidirectional antenna.

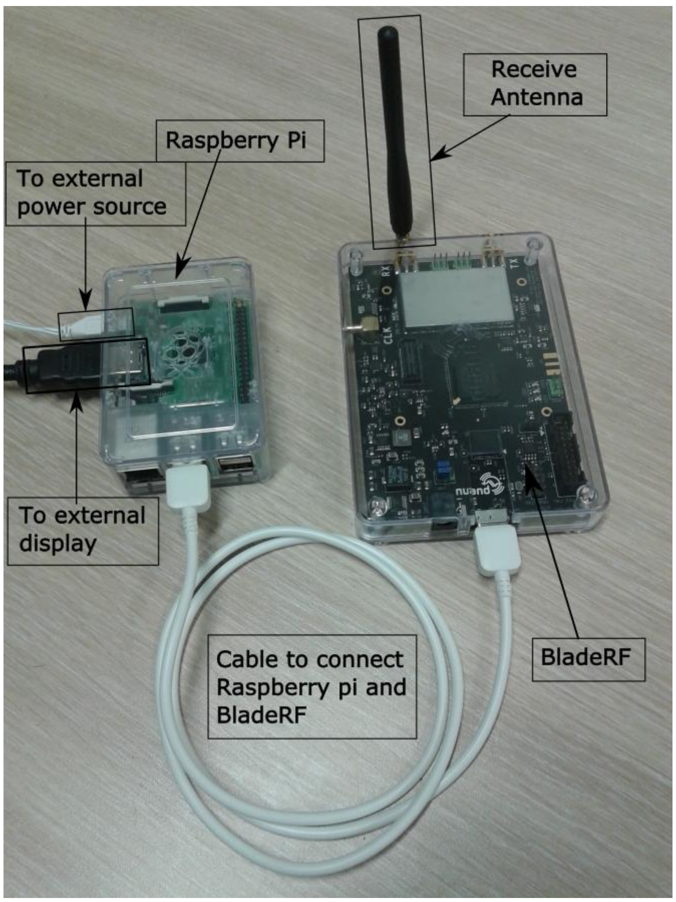

Figure 4: Final implementation of the GSM-CommSense system.

IV. FINAL SYSTEM

Since the basic operation of the system and the feasibility of the hypothesis is tested, it is time to implement the GSM-CommSense as a standalone system. Figure 4 shows the picture of the final system. A Raspberry pi 3 is used as the processing unit running Raspbian operating system which runs the GNURadio and is the main processing blocks for GSM-CommSense.

The receiver hardware is still a BladeRF with an omnidirectional antenna which receives the GSM frames, samples and forwards to the raspberry pi for further processing. A Wi-Fi hotspot is created on the raspberry pi to connect it to another laptop wirelessly and send the received channel information wirelessly. This information is sent through Transfer Control Protocol (TCP) and with a Protocol Data Unit (PDU) frame structure containing the timestamp as frame header and the channel information as the data.

This data is then analyzed in the laptop in real time showing the output corresponding to a particular scenario being observed. A short demonstration video is available online which is trained to detect intrusion of an extra person in the vicinity of the receiver. The learning algorithm used for this demonstration is SVM.

V. APPLICATION

Some of the applications explored for this system are intrusion detection, in which the system generates a trigger signal when it perceives an intruder in the vicinity. In the demonstration video this trigger signal is the message being printed as “Intrusion” or “No Intrusion”. The next application being explored is building monitoring for elderly care, in which the system will generate a trigger signal when an unexpected movement is observed.

Some of the other potential applications of the system are concealed weapon detection, detection of parking space availability, etc..

VI. CONCLUSION

We have successfully designed a system that uses the GSM training sequences to extract the channel information in order to analyze the immediate surroundings of the receiver. The major advantages of this system is that it is made of readily available hardware and open source software so further modifications to the system is not difficult. The performance of the GSM-CommSense system is shown in real-time and the average prediction accuracy is calculated to be 75-80 %. There is still an outstanding issue of increasing the accuracy and a few ways to do so are proposed, although we are open to any comments.

In the future we want to make this system more robust and possibly realize it into a marketable product.

VII. REFERENCES

[1] F. Maasdorp, J. Cilliers, M. Inggs and C. Tong, "FM band commensal radar technology used for the detection of small aircraft and measurement of propeller modulation," in *Radar Conference (RadarCon), 2015 IEEE*, 2015.

[2] M. R. Inggs, A. van der Byl and C. A. Tong, "Commensal Radar: Range-Doppler processing using a recursive DFT," in *Radar (Radar), 2013 International Conference on*, 2013.

[3] M. R. Inggs and C. A. Tong, "Commensal Radar using separated reference and surveillance channel configuration," *Electronic Letters*, vol. 48, pp. 1158-1160, 2012.

[4] A. K. Mishra, "CommSense: Radar system using existing communication infrastructure to sense the environment," in *Radioelektronika (RADIOELEKTRONIKA), 2015 25th International Conference*, 2015.

[5] A. Bhatta and A. K. Mishra, "Implementation of GSM channel estimation using open-source SDR environment," in *ICMOCE, 2015 International Conference*, 2015.

[6] A. Bhatta and A. K. Mishra, "GSM-based CommSense system to measure and estimate environmental changes," *IEEE Areospace and Electronic Systems Magazine*, vol. 32, no. 2, pp. 54-67, 2017.

[7] A. Bhatta and A. K. Mishra, "GSM based hand-held CommSense-Sensor for environment monitoring," in *ICIIS, 2016 International Conference on Industrial and Information Systems*, 2016.