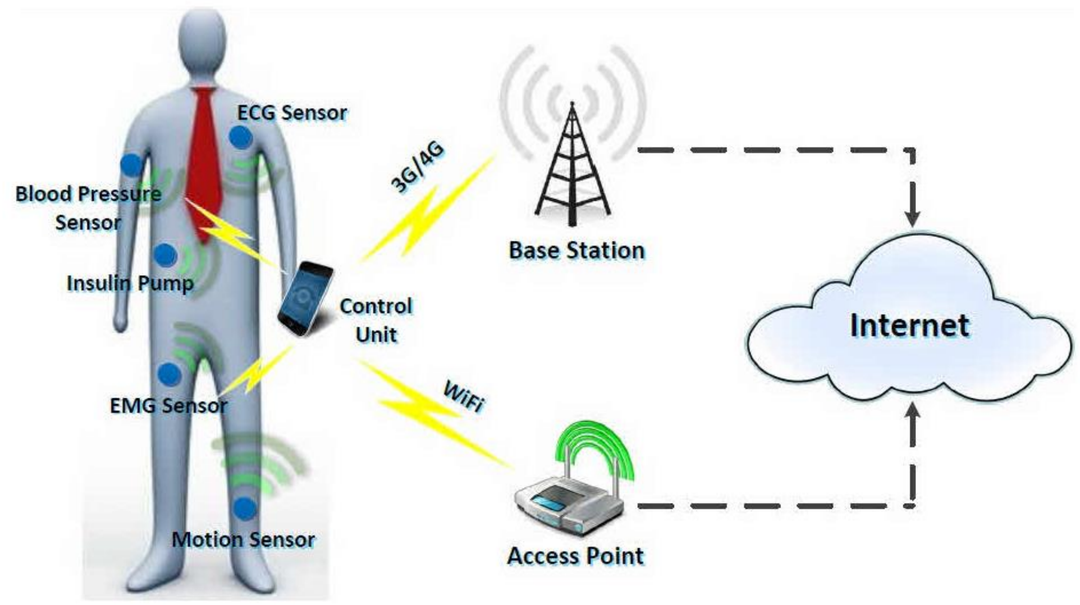
Body Area Network Security using Discrete Wavelet Transform

- STUDENTS / UNIVERSITIES
  Arca Özkan
  Eda Yardım
  Yiğithan Bilge
- SUPERVISOR(S)
  Duygu Karaoğlan Altop
  Albert Levi

Sabancı Üniversitesi

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

ABSTRACT

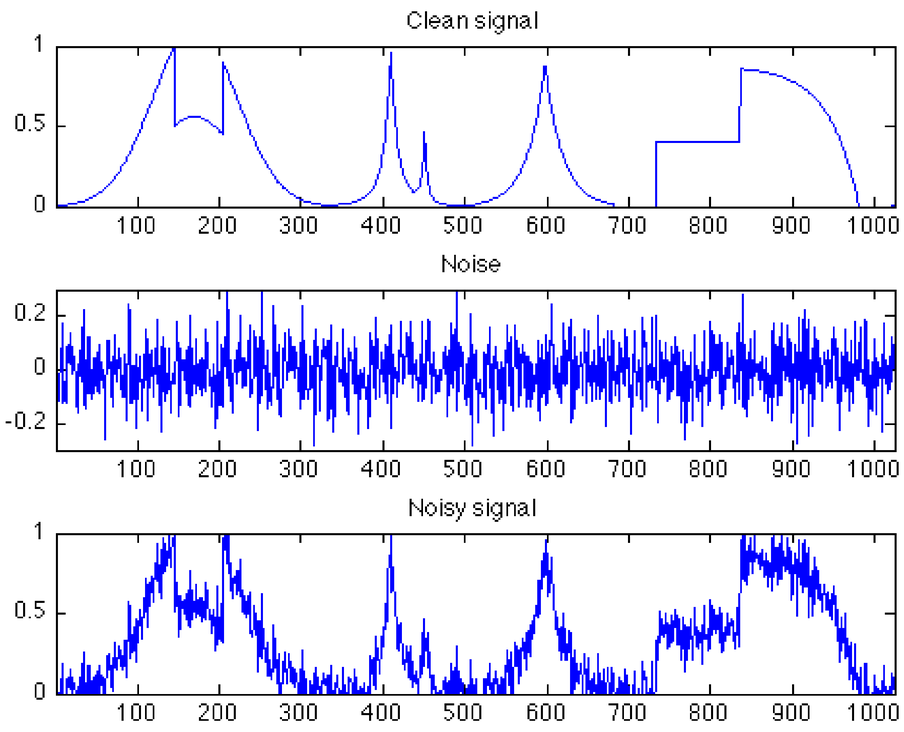


The main objective of the project is to find an appropriate way of deriving physiological parameters from ECG and Blood Pressure (BP) data, in order to generate cryptographic keys, which will be used as a security mechanism for Body Area Networks (BAN). Discrete Wavelet Transform is used as a noise reduction technique and it is not enough by itself when generating a physiological parameter, so Fast Fourier Transform is also applied after DWT. Dividing the signal into pieces of 250, then applying Fast Fourier Transform on each piece and concatenating them provides better results compared to applying FFT to the whole signal. Since the y coordinates of the resulting signal are not consistent, comparing the x coordinates seems like the better option.

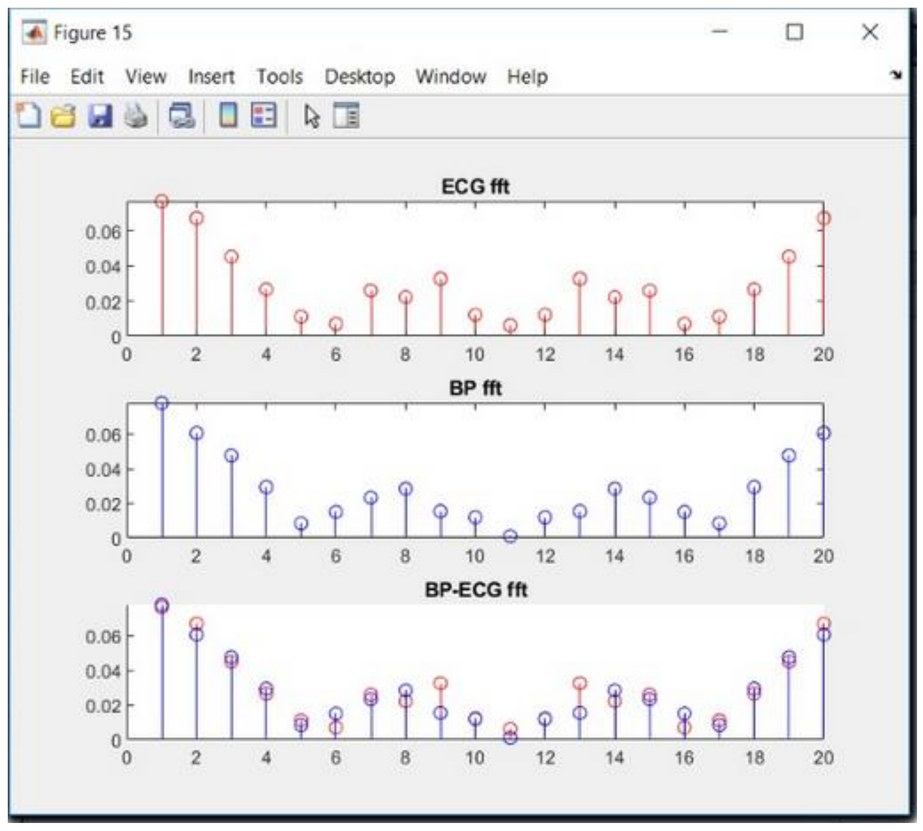
OBJECTIVES

The main objective of the project is to find an appropriate way of deriving physiological parameters from ECG and Blood Pressure (BP) data, in order to generate cryptographic keys. These cryptographic keys will be used as a security mechanism for Body Area Networks (BAN).

PROJECT DETAILS



Body Area Networks (BAN) are interconnected nodes of biosensors, which are placed either on or within the human body. They collect data which can be chemical/physiological signals or motion pattern. These physiological signals, which are ECG and BP data in our case, are used to derive physiological parameters, which will be used to create security providing cryptographic keys. Since they are carrying sensitive and vital information we need to provide security.



We had a database of 50 patients, each with 5 minutes of BP and ECG data. The physiological parameters generated by using these BP and ECG data, needed to be similar for the same patient, but different for others for our project to be successful. We decided to use Discrete Wavelet Transform as our physiological parameter generation technique. We made a research about DWT, and made a presentation about it. Then, we realized that DWT is not appropriate for a physiological parameter generation by itself, it is used mainly for denoising and compression. So, we decided to use DWT to get rid of the noise, but we needed another technique to generate the parameters. We decided to use Fast Fourier Transform (FFT) this time, but the results were not as good as we expected, so we decided to divide the signal into pieces and perform FFT, then concatenate the results. We tried pieces of 126 points, 250 points, 256 points, 500 points and 512 points. 250 points gave the best results, so we decided to find the x coordinates of the peaks of the concatenated signal. After normalization, we realized that the first 50 points of each piece of 250, produced similar x coordinates of peaks for both ECG and BP signals. So, we decided to compare the x coordinates of these pieces and analyze the results.

CONCLUSIONS

While our project is not finished yet, we can make some conclusions. First of all, Discrete Wavelet Transform is used as a noise reduction technique and it is not enough by itself when generating a physiological parameter. Also, changing the Wavelet used in DWT (Debauchies, Symlets etc.) changes how similar the BP and ECG signals are. Dividing the signal into pieces of 250, then applying Fast Fourier Transform on each piece and concatenating them provides better results compared to applying FFT to the whole signal. Since the y coordinates are not consistent, comparing the x coordinates seems like the better option. To sum up, even though we couldn't find the perfect parameter generation technique for cryptographic key generation, we have made some advances towards our goal.

REFERENCES

[1] R. L. Bashshur, T. G. Reardon, and G. W. Shannon, "Telemedicine: A new health care delivery system," Annual Review of Public Health, vol. 21, pp. 613–637, 2000.

[2] J. O'Donoghue and J. Herbert, "Profile based sensor data acquisition in a ubiquitous medical environmet," in Proceedings of the Pervasive Computing and Communications Workshops (PerComW), pp. 570–574, IEEE Computer Society,Washington, Pisa, Italy, 13–17 March 2006.

[3] G.-Z. Yang, Body Sensor Networks. London: Springer-Verlag, 1st ed., 2006.

[4] U. Varshney, "Pervasive healthcare and wireless health monitoring," Mobile Networks and Applications, vol. 12, no. 2/3, pp. 113–127, 2007.

[5] N. A. Pulur, Medically Adaptive Role Based Access Control Model (MAR-BAC). PhD thesis, Sabancı University, 2015.

[6] K. V. Laerhoven, A. Schmidt, and H.-W. Gellersen, "Multi-sensor context aware clothing," in Proceedings of the International Symposium on Wearable Computers (ISWC), pp. 49–56, IEEE Computer Society, Washington, Seattle, WA, 7–10 October 2002.

[7] Wang, Q. et al., "I-Living: An open system architecture for assisted living," in Proceedings of the International Conference on Systems, Man and Cybernetics (SMC), pp. 4268–4275, IEEE Press, Portland, Taipei, Taiwan, 8–11 October 2006.

[8] E. Jovanov, A. Milenkovic, C. Otto, and P. C. d. Groen, "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," Journal of NeuroEngineering and Rehabilitation, vol. 2, no. 6, pp. 2–6, 2005.

[9] A. Wood, J. Stankovic, G. Virone, L. Selavo, Z. He, Q. Cao, T. Doan, Y. Wu, L. Fang, and R. Stoleru, "Context-aware wireless sensor networks for assisted living and residential monitoring," IEEE Network Magazine, vol. 22, no. 4, pp. 26–33, 2008.