

A Study on Memory Management in Wireless Sensor Nodes during Key Agreement Generation

Lunda Machaya*, Simon Tembo

School of Engineering, University of Zambia, Lusaka, Zambia

Abstract The objective of the research was to efficiently manage memory in wireless sensor nodes during key agreement generation using minimax sampling. The wireless sensor nodes are faced with scarce memory resources, which limits their computing power and communication capabilities in highly dynamic environments. Wireless sensor networks represents a new generation of distributed embedded systems with a wide range of real-time applications. The applications of such nodes include process control, fire monitoring, cross border surveillance, health care, fixed and mobile asset tracking, agriculture, highway surveillance. In our research, we have proposed minimax sampling during key agreement generation to efficiently manage memory usage in wireless sensor nodes. The adopted experimental approach involved the use of Matlab. The signal was analysed at various frequencies using uniform sampling to determine memory variations with changes in the number of samples considered for key agreement generation. The results showed that as the number of samples increases, the memory usage in the wireless sensor node increases and vice versa. Our proposed minimax sampling method reduces the number of samples, thereby efficiently managing the memory. This results in memory availability for other tasks in the wireless sensor node.

Keywords Wireless Sensor Node, Network, Key Agreement Generation, Memory Management, Minimax Sampling

1. Introduction

A Wireless Sensor Network (WSN) is a network of wearable and implantable computing devices [1]. The computing devices are either medical, weather or environmental sensing devices. With the growing demand and implementation of WSNs, there is need to optimize the resources of sensor nodes to ensure reliable and accurate collection and communication of data by the nodes. The WSNs represent a new generation of distributed embedded systems with a wide-range of real-time applications including process control, fire monitoring, cross border surveillance, health care, fixed and mobile asset tracking, agriculture, highway surveillance [2]. A WSN system can be integrated with existing communication systems infrastructure to reach longer distances. This allows for connection to remote servers via internet or mobile communication technologies (GSM/GPRS/3G). This way, the collected data can be accessed online using the fixed or mobile communication technologies independent of the sensor location. The rapid development of sensor technology, low-power integrated circuits, and wireless communication has enabled a new generation of wireless

sensor networks such as Mobile Adhoc Networks (MANETS), Vehicular Adhoc Networks (VANETS), Military MANETS, Internet based MANETS (iMANETS) and Smart Phone Adhoc Networks (SPANs) [3]. This research proposes minimax sampling during key agreement generation to efficiently manage memory resources in the sensor nodes during agreement key generation. Minimax Sampling is the method where the analog signal is sampled at its local maximum and minimum points [4]. The key generated ensures confidentiality and authenticity of the data collected by the sensor nodes.

2. Related Work

In [5], the authors propose the introduction of a third party node for key generation purposes. This is to relieve the memory stress of the WSN. The other reasons for the introduction of the third parties include relieved computational burden and reduced communication overhead. The highlighted reasons are mostly due to resource constraints of WSN nodes. This method tends to be expensive because of extra hardware.

In [6], key generation was performed by the two communicating sensors, by performing uniform sampling on the ECG signal at 125Hz for a duration of 5 seconds. The uniform sampling produced 625 samples which were further divided into 5 parts of 125 sample values. The 128 point Fast Fourier Transform (FFT) was performed on the 125 sample

* Corresponding author:

machayalun@yahoo.com (Lunda Machaya)

Published online at <http://journal.sapub.org/ijnc>

Copyright © 2016 Scientific & Academic Publishing. All Rights Reserved

values to obtain 128 FFT coefficients the first 64 of each where used for feature vector generation, which was quantized to obtain the binary key. This method equally requires more memory to handle the computations and the samples.

In [7], the authors propose a new approach to symmetric cryptographic key establishment, based on biometrics physiology with careful consideration on Body Sensor nodes performance constraints such as limitation in energy resources, data-processing and topology. In this paper, the authors used changeable topology to improve network performance and increase level of security. The hybrid topology, Star and Mesh topology, was deployed in this setup to ensure efficient usage of Body Sensor Node resources.

In [8], the authors discuss how different WSNs operating systems (OS) manage memory. They discuss OSs such as MANTIS, LiteOS, TinyOS, Nano-RK, LIMOS, SOS, Contiki, Enix and $\mu\text{C}/\text{OS-II}$. Among the methods used by the different OS to manage memory include pre-emptive scheduling, module level programming, dynamic memory management, hybrid operating system, and support of virtual memory. They also discuss the research gaps and OS design with respect to memory management in WSNs. The research proposes inclusion of secondary memory management in future OS design and fair scheduling to ensure support for concurrent tasks. However, the research does not look at memory management during key agreement generation,

which is the objective of this research.

In [9], the authors proposed the use of Attribute-Based Encryption (ABE) for security and privacy implementation in Wireless Body Sensor Networks. The authors described the ABE as a fined-grained access control, which is a one-to-many encryption method, where the cipher-text is meant to be recognizable only by a group of users that satisfy a certain Access Policy (AP). The paper highlights the constraints of the Sensor nodes resources and the negative effects these resources have on the implementation of the security and privacy method to be deployed in WBSN. The need for high efficiency and strong demand for data security in WBANs, not only because of the resource constraints, but also for the applications.

3. Findings and Discussions

The signal as illustrated in equation 1 [10] was used in the

$$x = 0.3 \sin(t) + \sin(1.3t) + 0.9 \sin(4.2t) + 0.02 \text{randn}(1,101) \quad (1)$$

analysis. The equation was uniformly sampled at frequencies 1Hz, 2Hz, 4Hz, 5Hz, 10Hz, 20Hz, 25Hz, 40Hz, 50Hz, 100Hz and 125Hz for a duration of 10 seconds. Sampling frequency (sample rate) is the number of samples per second taken from a continuous signal to make a digital signal [12]. From this definition, we obtain equation 2. The number of samples after sampling is given by;

Table 1. Sampling Frequency Verses Number of Samples

f_s	1	2	4	5	10	20	25	40	50	100	125
N_{samples}	10	20	40	50	100	200	250	400	500	1000	1250

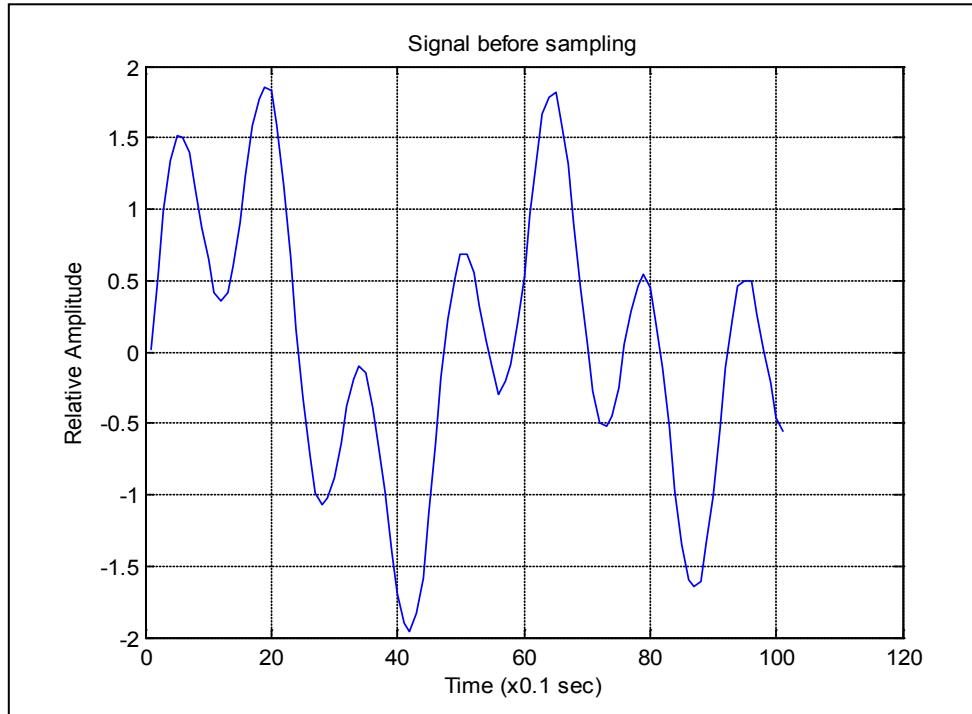


Figure 1. Signal before Sampling

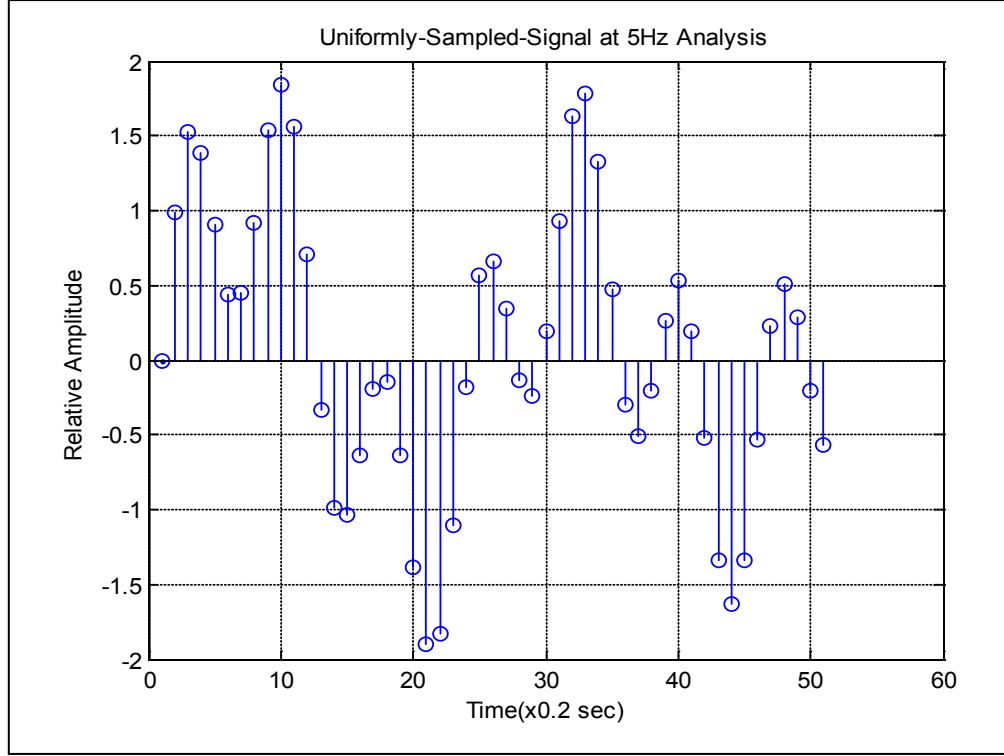


Figure 2. Signal Uniformly Sampled at 5Hz

$$N_{samples} = f_s \times t_s \quad (2)$$

Where f_s is the sampling frequency and t_s is the signal duration for which the sampling instant is considered. From Equation 2, we obtain table 1 has shown.

Minimax sampling a sampling method where the signal is only sampled at the maximum and minimum points. Table 1 shows the sampling frequencies f_s and number of samples $N_{samples}$ obtained after sampling at different frequencies.

Figure 1 shows the MATLAB simulation of the signal before sampling for a duration of 10 seconds.

Figure 2 shows the MATLAB simulation of the signal after sampling at 5Hz.

To illustrate the memory saving capabilities of minimax sampling, consider a signal sampled at f_{max} for a duration of 1s. The number of samples will be;

$$f_{max}$$

The same signal is subjected to minimax sampling through a minimax sampler $Q_{min,max}$ shown in figure 3 for a duration of 1s.

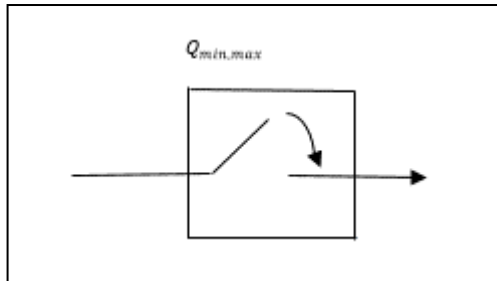


Figure 3. Minimax Sampler

Assuming the number of samples obtained after minimax sampling is

$$N_{min,max}$$

The capacity loss or excess capacity, $L_s Q_{min,max}$ after minimax sampling will be given by

$$L_s Q_{min,max} = f_{max} - N_{min,max} \quad (3)$$

Capacity loss or excess capacity is the difference between maximum capacity of a uniformly sampled signal and capacity of a minimax sampled signal [11]. From equation 3 we can obtain the Excess capacity, given the number of samples (capacity) resulting from uniform sampling at different frequencies for a duration of 10 seconds. Figure 4 shows the MATLAB simulation of minimax sampling. From Figure 4, the number of samples obtained after minimax sampling for a duration of 10 seconds is 13 samples.

Since we know, $N_{min,max}$ we can calculate Excess capacity at different frequencies to obtain table 2. Assuming 1 sample needs 1 bit per second of memory. From table 2 we obtain a plot of sampling frequency verses capacity loss or Excess capacity as shown in figure 5.

From figure 5, we can deduce that, as the sampling frequency increases, the excess memory size increases and vice versa. This implies that sampling frequency is directly proportional to the capacity or memory usage. Area A, circled on figure 5, shows the minimax sampling operating region in terms of memory usage during key agreement generation.

The proposed minimax sampling results in reduced number of samples, resulting in reduced memory usage in the WSN node. The minimax sampling thus improves

memory management in the WSN due to its higher signal compression rate. With minimax sampling, very few samples that are maximums and minimums are considered during key agreement generation resulting in considerable memory saving as compared to conversion sampling methods employed for the similar purpose.

The sensor to communicate with the sink node (master node) uses the signal of the parameter being measured to generate the key to be exchanged with the sink node. The signal of the measured parameter is fed to the minimax sampler, whose output is fed to the Quantizer. The quantized output is then fed to an encoder using Run-Length Encoding

(RLE) scheme to further minimize memory usage in the WSN node. The output of the encoder is fed into the Generator matrix in order to obtain a fixed length code of 128 bits. The obtained code is then encrypted using an appropriate commitment scheme or encryption algorithm for onward transmission to the sink node for authentication. This research concentrates on memory management in WSN nodes during key agreement and did not look at the commitment scheme to be used during key agreement exchange. Figure 6 shows the implementation model using minimax sampling method during key agreement generation in WSN nodes.

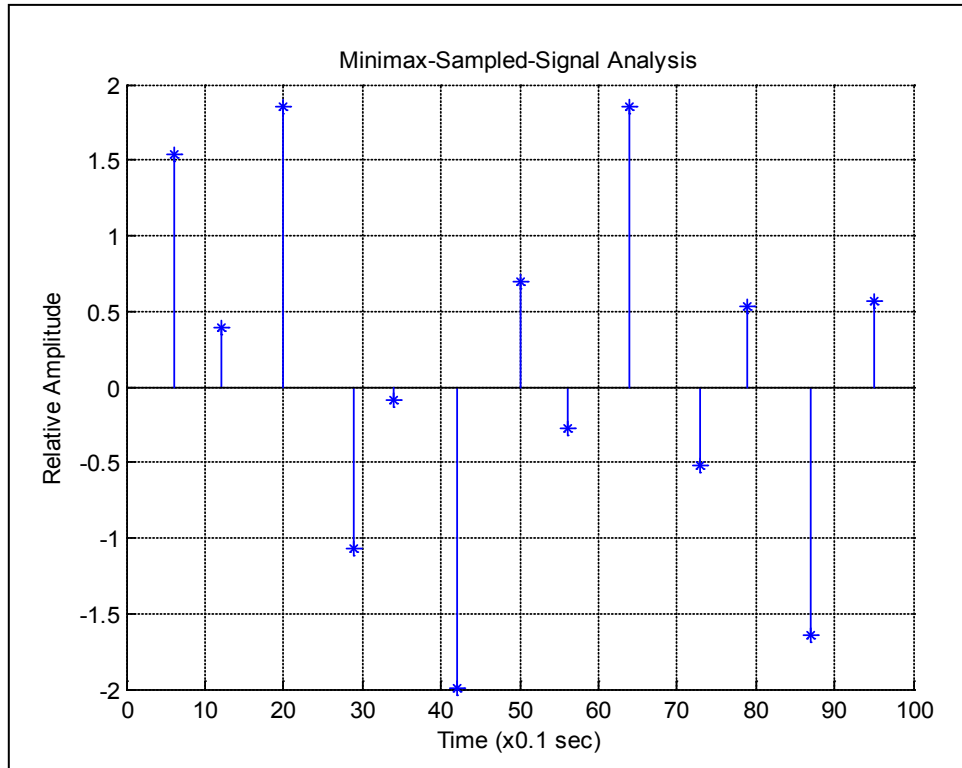


Figure 4. Signal after Minimax Sampling

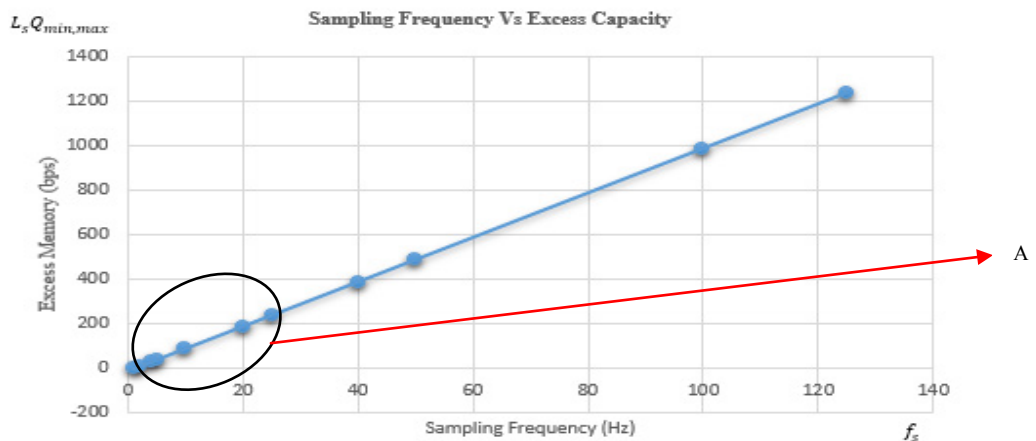
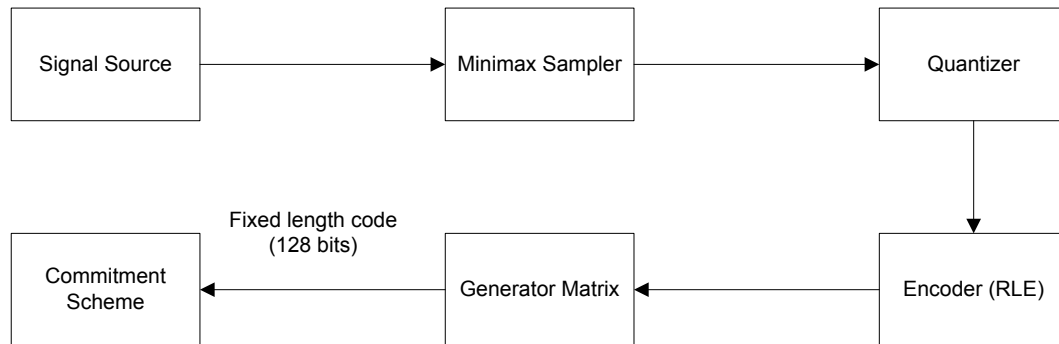


Figure 5. Plot of Sampling Frequency Vs Excess Capacity4. Implementation Model

Table 2. Sampling Frequency verses Excess Capacity

$f_s(Hz)$	1	2	4	5	10	20	25	40	50	100	125
$L_s Q_{min,max}(bps)$	-3	7	27	37	87	187	237	387	487	987	1237

**Figure 6.** Implementation model

4. Conclusions and Future Work

The research objectives are achieved using minimax sampling. The proposed minimax sampling results in higher signal compression as demonstrated from graphical interpretation of the results obtained when the signal was sampled at different frequencies. The minimax sampling uses very few samples for key generation because only the samples occurring at minimum and maximum points are considered. Future research should concentrate on the practical implementation of minimax sampling in WSNs during key agreement generation.

ACKNOWLEDGEMENTS

Special thanks go to my supervisor Dr. Simon Tembo for his support and encouragement during the research. I wish to thank my wife and children for the support during this period. And most of all God almighty for the strength and good health during the course of study.

REFERENCES

- [1] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. Leung, "Body Area Networks: A Survey," in *Mobile Networks and Applications (MONET)*, Springer Netherlands, 2010, pp. 1-23.
- [2] H.-j. Kim, R. D. Caytiles and T.-h. Kim, "Design of an Effective WSM-Based-Interactive u-Learning Model," *International Journal of Distributed Sensor Networks*, vol. 2012, 2012.
- [3] I. F. Akyildiz and I. H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351-367, 2004.
- [4] I. Homjakovs, M. Hashimoto and T. Onoye, "Signal-Dependent Analog-to-Digital Conversion based on MINIMAX Sampling," *IEEE, Osaka*, 2011.
- [5] S. Almowuena, "An Efficient Key Agreement Scheme for Wireless Sensor Networks using Third Parties," *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, vol. 4, no. 4, 2013.
- [6] S. Cherukuri, K. Venkatasubramanian and S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," *Proc. IEEE Int. Conf. on Parallel Processing Workshops*, pp. 432-439, 2003.
- [7] S. Mesmoundi and M. Feham, "BSK-WBSN: BIOMETRIC SYMMETRIC KEYS TO SECURE WIRELESS BODY SENSOR NETWORK," *International Journal of Network Security & Its Applications*, vol. Vol.3, no. No.5, pp. 155-166, 2011.
- [8] M. Pathak, "An Approach to Memory Management in Wireless Sensor Networks," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 4, no. 8, pp. 1171-1176, 2013.
- [9] M. Li, W. Lou and K. Ren, "DATA SECURITY AND PRIVACY IN WIRELESS BODY AREA NETWORKS," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51-58, 2010.
- [10] E. Billauer, "Peakdet," 20 July 2012. [Online]. Available: www.billauer.co.il. [Accessed 23 April 2015].
- [11] C. Yuxin, G. Andrea and E. Yonina, "Minimax Universal Sampling for Compound Multiband Channels," in *International Symposium on Information Theory (ISIT)*, Istanbul, 2013.
- [12] V. Khanna, *Digital Signal Processing, Telecommunications*, New Delhi: S.Chand, 2003.