



Study on Different Encoding Mechanism to Perform Secure Network Communication

Yashu¹ & Smita²

¹Research Scholar, ²Associate Professor,
Department of Computer Science and Engineering,
PDM College of Engineering for Women, Bahadurgarh, Haryana, India

Abstract: Network security can be achieved in different ways in a communication system. To achieve the security against different attacks, one approach is to send the encoded information over the network. The encoded approaches not only provide the information security but also decrease the communication size without adding the overhead. In energy critical networks such as sensor network, this kind of encoded communication approach is more effective. In this paper, some of the most common encoding approaches are discussed. The approaches considered in this work are RS Encoding, Convolution Codes and Hamming Codes.

Keywords: Convolution, Hamming Code, Information Security, WSN

I. INTRODUCTION

A sensor network is one of the most common network architecture defined under the energy constraints. Different operations associated with sensor network include the communication over the effective route. As the communication is performed over the specific route, each participating node consumes some amount of energy. To perform the energy effective communication some optimized routing approach is required. Another way to reduce the energy consumption is to reduce the communicating data over the network. As the communication will be reduced, the energy consumption will also get reduced. To reduce the size of communicating data over the network some encoding technique can also be adapted. The encoding technique is also effective to provide the effective mechanism to detect the error over the network and to provide the effective communication. In this paper, a study on all these aspects of network communication is discussed. The aspect discussed in this paper includes the routing approach as well as the encoding mechanism adapted to reduce the communication. The possibilities to improve the energy effectiveness in sensor network are shown in figure 1.

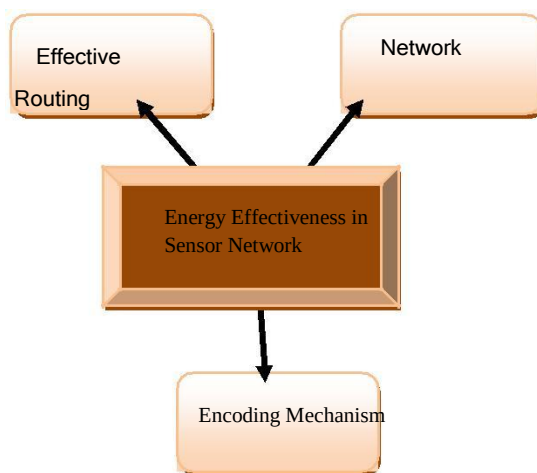


Figure 1: Energy Effectiveness in Sensor Network

In this section, Routing in sensor network is discussed. Routing in sensor network is performed using two main approaches called unicast routing and multicast routing approach. Global routing and Maze routing are also some of popular routing approaches adopted by sensor network. These routing approaches are discussed in this section.

A. Unicast Routing

Unicast routing is about the generation of single path between single source and destination node. The challenge in such routing is to obtain the QoS while performing the effective utilization of bandwidth and the buffer space. The state path generation under the bottleneck problem is also a challenge for communicating network. Unicast

routing is also1, which is the bandwidth of the bottleneck link (i, j). For these QoS metrics, two basic routing problems can be defined. One is called link-optimization routing. An example is the bandwidth-optimization routing, which is to find a path that has the largest bandwidth on the bottleneck link. Such a path is called the widest path. The other problem is called link-constrained routing. An example is the bandwidth- constrained routing, which is to find a path whose bottleneck bandwidth is above a required value [2]. For other QoS metrics such as delay, delay jitter and cost, the state of a path is determined by the combined state over all links on the path. For example, if the delay of path $s \rightarrow i \rightarrow j \rightarrow t$ is 10, which is the total delay of all links on the path. Two basic routing problems can be defined for this type of QoS metrics. One is called path-optimization routing. An example is the least-cost routing, which is to find a path whose total cost is minimized. The other problem is called path-constrained routing. An example is the delay-constrained routing, which is to find a path whose delay is bounded by a required value. [2].

B. Multicast Routing

There are several well-known multicast routing problems. The Steiner tree problem is to find the least-cost tree, the tree covering a group of destinations with the minimum total cost over all links. It is also called the least-cost multicast routing problem, belonging to the tree-optimization routing problem class. The constrained Steiner tree problem is to find the least-cost tree with bounded delay. It is also called the delay-constrained least-cost routing problem, belonging to the tree-constrained tree-optimization routing problem class [2].

C. Global and Detail Routing:

During global routing, complex design rules are abstracted away and a design is divided into a regular grid. Routes are created for each net that connect adjacent grid cells. Capacities are assigned to pairs of adjacent grid cells to model limited routing resources between the cells. Since different metal layers may use distinct wire pitches, routing capacities at each layer may differ to reflect this. A global routing solution is legal if all nets are connected and all capacity constraints are satisfied. Detail routing takes a global routing solution with a small number of capacity violations (overflows), or none at all, and assigns wires to routing tracks while enforcing spacing constraints and more sophisticated design rules. Starting with slightly illegal global routes can make detail routing considerably more difficult, therefore a global router must minimize violations and wavelength, seeking to avoid violations entirely when possible [4].

D. Maze Routing

It connects pairs of terminals on the routing grid using standard search techniques such as BFS and Dijkstra's algorithm. The maze router ensures that the least cost route (according to the cost function) is found. More than 50% of nets in modern designs connect only two pins. BFS can find the shortest path between a source location and a target location, if one exists, but cannot handle routing segments with non-trivial weights [4][8].

In this paper, a study on the encoding techniques in sensor network is defined. The work has covered the routing mechanism in sensor network. In this section, some of different routing approaches adapted in sensor network are defined. In section II, the work done by the earlier researchers is discussed. In section III, some of the effective encoding techniques are discussed. In section IV, the conclusion obtained from the work is defined and presented.

II. ERROR DETECTION TECHNIQUES

Several schemes exist to achieve error detection. The general idea is to add some *redundancy*, i.e., some extra data, to a message, that enables detection of any errors in the delivered message. Most such error-detection schemes are *systematic*: the transmitter sends the original data bits, and attaches a fixed number of *check bits*, which are derived from the data bits by some deterministic algorithm. The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a "non-systematic" code, such as some raptor codes, the original message is transformed into an encoded message that has at least as many bits as the original message. In general, any hash function may be used to compute the redundancy. However, some functions are of particularly widespread use, due to their simplicity, or their suitability of detecting certain kinds of errors, such as the cyclic redundancy check's performance in detecting burst errors. Other mechanisms of adding redundancy are repetition schemes and error-correcting codes. Repetition schemes are rather inefficient but very simple to implement. Error-correcting codes can provide strict guarantees on the number of errors that can be detected.

A. Repetition schemes

Variations on this scheme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send "1011", we may repeat this block three times each. Suppose we send "1011 1011 1011", and this is received as "1010 1011 1011". As one group is not the same as the other two, we can determine that an error has occurred. This scheme is not very efficient, and can be susceptible to problems if the error occurs in exactly the same place for each group (e.g. "1010 1010 1010" in the example above will be detected as correct in this scheme).The scheme however is extremely simple, and is in fact used in some transmissions of numbers stations

B. Parity schemes

Parity bit: A simple parity bit is an error detection mechanism that can only detect an odd number of errors. The stream of data is broken up into blocks of bits, and the number of 1 bits is counted. Then, a "parity bit" is set (or cleared) if the number of one bits is odd (or even). (This scheme is called even parity; odd parity can also be used.) If the tested blocks overlap, then the parity bits can be used to isolate the error, and even correct it if the error affects a single bit: this is the principle behind the Hamming code. There is a limitation to parity schemes. A parity bit is only guaranteed to detect an odd number of bit errors (one, three, five, and so on). If an even number of bits (two, four, six and so on) are flipped, the parity bit appears to be correct, even though the data is corrupt.

III. ENCODING TECHNIQUES

The next process of the system is to perform the channel coding. In this work we have defined three different encoding schemes listed below.

A. Convolution Codes

A convolutional code is a type of code in which each k -bit information to be encoded is transformed into an n -bit symbol. A convolutional code introduces redundant bits into the data stream through the use of linear shift registers as shown in (Figure1). The inputs to the shift registers are information bits and the output encoded bits are obtained by modulo-2 addition of the input information bits and the contents of the shift registers.

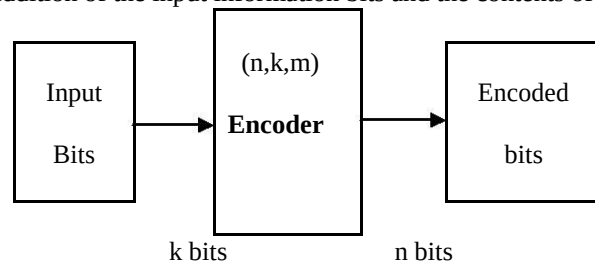


Figure 1: Encoding Mechanism

B. Convolution Code Encoder

A convolutional encoder is made up of a fixed number of shift registers. Each input bit enters a shift register and the output is derived by combining the bits of the shift register. The number of output bits depends on the number of modulo 2-adders used with shift registers.

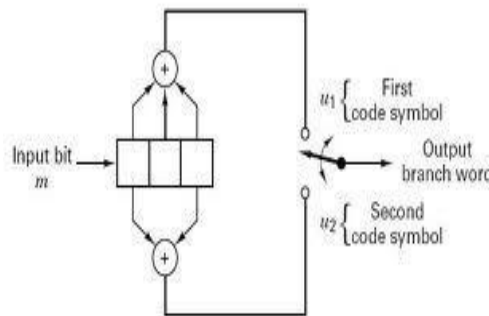


Figure 2: Convolution Code Encoder

Convolutional codes are primarily described by three parameters (n,k,m) where,
 n = number of output bits k = number of input bits
 m = number of memory registers

A convolutional encoder is characterized by two parameters, namely code rate (r) and constraint length (K). The code rate is defined as the ratio of the number of message bits(k) to the number of encoded bits (n).

$$r = k/n$$

The convolutional code's structure is easy to draw from its parameters. First draw m boxes representing the m memory register. Then draw n modulo-2 adders to represent the n output bits. Now connect the memory registers to the adders using the generator polynomial. This is a rate $1/3$ code. Each input bit is coded into 3 output bits. The constraint length of the code is 2. The 3 output bits are produced by the 3 modulo-2 adders by adding up certain bits in the memory registers. The selection of which bits are to be added to produce the output bit is called the generator polynomial (g) for that output bit. For example, the first output bit has a generator polynomial of $(1,1,1)$. The output bit 2 has a generator polynomial of $(0,1,1)$ and the third output bit has a polynomial of $(1,0,1)$. The output bits just do the sum of these bits.

$$v_1 = \text{mod}2 (u_1 + u_0 + u_{-1})$$

$$v_2 = \text{mod}2 (u_0 + u_{-1})$$

$$v_3 = \text{mod}2(u_1 + u_{-1})$$

The polynomials give the code its unique error protection quality.

C. Hamming codes

Hamming codes are block codes, so coded vectors, c , of length n coded bits are formed from a data sequence, d , of length k information bits, and generator matrix, G , as follows:

$$[c] = [G] [d].$$

$$n \times 1 \quad n \times k \quad k \times 1$$

There are specific possible sizes of G for hamming codes based on a parameter, m . $n = 2^m - 1$, $k = n - m$. So, for $m = 3$, $n = 7$ and $k = 4$. This is called the (7,4) Hamming code.

D. RS Encoding

Reed Solomon encoding is a block encoding scheme. The system implemented in this study was a (255,223) system, in which (n,k) denotes an output codeword length of n and an input word of length k , as shown in Figure 1. It has a symbol size, s , equal to 8. The decoder has a correcting capability of t symbol errors in the code word, with $n - k = 2t$, in this case, $t=16$.

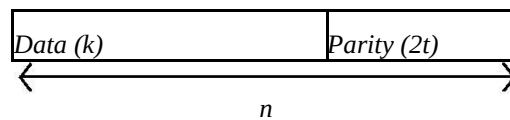


Figure 3: typical RS codeword

The encoder forms a code word $x^{n-k}m(x) + r(x)$ by means of the following equation:

$$\frac{x^{n-k}m(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

The divisor, $g(x)$ is known as the generator polynomial. It is a polynomial of degree $(n-k)$ and which is a factor of (x^n+1) . To maximize the minimum distance between codes, the roots of this polynomial should all be consecutive. This is a direct consequence of the BCH bound, which states that the minimum distance is always larger than the number of consecutive factors of $g(x)$. The system used adapted a generator polynomial with roots from 1 to ^{32} .

V. CONCLUSIONS

In this paper, a study on different encoding filters is defined. While performing the communication in network, some mechanism is required that will reduce the communication efforts as well as provide the effective communication in term of security. The paper has discussed three main encoding techniques called Convolutional Filters, RS Filter and Hamming encoding.

REFERENCES

- [1] Juejia Zhou, "A Kind of Application-Specific QoS Control in Wireless Sensor Networks", Proceedings of the 2006 IEEE International Conference on Information Acquisition 1-4244-0529-7/06©C2006 IEEE
- [2] Haifeng Hu, "The Study Of Power Control Based Cooperative Opportunistic Routing In Wireless Sensor Networks", Proceedings of 2007 International Symposium on Intelligent Signal Processing and Communication Systems 1-4244-1447-4/07 ©2007 IEEE
- [3] Paulo Sergio Sausen, "Energy Efficient Blind Flooding in Wireless Sensors Networks".
- [4] Peng Ji, "A Power-aware Layering Optimization Scheme for Wireless Sensor Network", 978-1-4244-3693-4/09 ©2009 IEEE
- [5] Parvaneh Rezayat, "A Novel Real-Time Routing Protocol in Wireless Sensor Networks", 978-1-4244-5757-1/10 ©2009 IEEE
- [6] Kritchai Witheephanich, "On The Applicability of Model Predictive Power Control to an IEEE 802.15.4 Wireless Sensor Network", ISSC 2009.
- [7] Djamel Djenouri, "Traffic-Differentiation-Based Modular QoS Localized Routing for Wireless Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING 1536-1233/11@ 2011 IEEE
- [8] A. Chehri, "QoS Aware Green Routing Protocol for Wireless Sensor Networks", 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) 978-1-4673-1433-6/12 ©2012 IEEE
- [9] Prof. Arun Biradar, "Dual Channel Based Multi-Objectives Genetic Routing Protocol for Ad-Hoc Networks and Optical Networks Using Power Aware Clustered Topology", 2012 International Conference on Optical Engineering (ICOE) 978-1-4673-2463-2/12 © 2012 IEEE
- [10] Nirmala.S, Nallusamy.R, "An Energy-Efficient and enhanced QoS aware of MAC application specific protocol in the distributed Wireless Sensor Networks", IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University 978-1-4673-5584-1/12@2012 IEEE
- [11] Mohammad Arifuzzaman, "An Intelligent Hybrid MAC With Traffic-Differentiation-Based QoS for Wireless Sensor Networks", IEEE SENSORS JOURNAL 1530-437X © 2013 IEEE
- [12] Diogo F. Lima Filho, "TCNet: Trellis Coded Network - implementation of QoS-aware routing protocols in WSNs".
- [13] D. F. L. Filho, "TCNet: Trellis Coded Network - Implementation of QoS-aware Routing Protocols in WSNs", IEEE LATIN AMERICA TRANSACTIONS
- [14] Irfan Al-Anbagi, "An Adaptive QoS Scheme for WSN-based Smart Grid Monitoring", IEEE International Conference on Communications 2013: IEEE ICC'13 - 3rd IEEE International Workshop on Smart Communication Protocols and Algorithms (SCPA 2013) 978-1-4673-5753-1/13 ©2013 IEEE
- [15] Luis Marques, "Fighting Uncertainty in Highly Dynamic Wireless Sensor Networks with Probabilistic Models", 2013 IEEE 32nd International Symposium on Reliable Distributed Systems 1060-9857/13© 2013 IEEE