Turbo Coding Based High Performance Technique to Minimise Privacy and Safety Issues in RFID

M Vijaya Deepti[*], M N V S S Kumar[**], L Ganesh[***] and S Deva Prasad[**]
([*]Department of Computer Science, Stratford University, Virginia, USA)
([**]Department of Electronics and Communication Engineering, Andhra University College of Engineering, India)
([***]Department of Electronics and Communication Engineering, Chaitanya Engineering College, India)

ABSTRACT

Radio Frequency Identification (RFID) technology is playing a very crucial role in tracking objects and their location, individuals, for the purpose of identification. The RFID system is an emerging technology widely used in various fields including the circulation, military affairs, health care, medicine etc. In this technology a RFID tag is attached to a person or an object to be tracked or identified which emits RF signal. Now-a-days RFID tags are being used almost everywhere and customer might be carrying these tags knowingly or unknowingly. The signal from tag is read by a remotely located RFID reader to identify or track the object. This signal can be read by any reader in the vicinity and retrieve the information, the tag contains. The data can be easily tracked by a third person other than original reader. So there may be probability of losing the object and data to a person who might be a threat to the privacy concern of an individual. There is also lack of safety by using these RFID tags. This is a grave issue in the fields of military, banking, medicine etc. So in this paper a Turbo Coding based method is explained to overcome the problem using RFID. In this method the information to be transmitted from a tag is encoded. The complete analysis is done based in MATLAB simulink.

Keywords- **RFID, Turbo Coding, Bit Error Rate**

I. INTRODUCTION

Radio Frequency Identification (RFID) is a method of identifying objects, people or animals by means of radio waves. RFID device is physically attached to the object to be identified or tracked. This device continuously emits radio waves which are received by a RFID reader. These radio waves contain the information like details of the object. RFID enables identification from a distance, and unlike earlier bar-code technology, it does so without requiring a line of sight.

RFID tags uses a larger set of unique IDs than bar codes and can incorporate additional data such as manufacturer, product type, and even measure environmental factors such as temperature. Furthermore, RFID systems can discriminate many different tags located in the same general area without human assistance. RFID tags can be broadly classified into three types based on the power source active, passive and battery assisted passive tags. Active RFID tags have their own internal power source, which is used to power the integrated circuits and to broadcast the response signal to the reader. Passive RFID tags have no internal power supply. Battery assisted passive tags, also called semi-active tags, are more or less like active tags in that they have their own power source, but the battery is only used to supply the power to the microchip only but does not power the broadcasting of a signal. The table 1 shows different types of RFID.

Active or passive	Other Classifications
Passive (no battery) Smaller, Lighter Shorter range (<3m) Smaller data storage Lower cost	Data storage (Programming) Read Only Write once Read/write
Active (with battery) Larger, Heavier Longer range (up to 100m) Larger data storage Higher cost	Frequencies Low –135 kHz VHF –13.5 MHz UHF –860MHz Microwave –2.4 GHz

Table 1 RFID Types

There are so many applications using RFID like food traceability, Asset tracking, process control, personal identification, counterfeiting prevention, luggage tracking, animal identification, banking, military etc. Inspite of all these applications RFID has some limitations like range limitation, safety, collision of signals at reader etc. Among these limitations safety and privacy plays a crucial role. RFID signal from a object can be read by any reader in the vicinity and retrieve the information the tag contains. The data can be easily tracked by a third person other than original reader. So there may be probability of losing the object. There is lack of privacy and safety by using these RFID tags. This is a grave issue in the fields of military, banking, medicine etc. So in this a Turbo Coding based method is analyzed. Before going to Turbo Coding method various encoding methods like convolution, trellis code are investigated. In all these methods performance of each method is determined based on Bit Error Rate. Among all these Turbo Code finds better BER. In general every RFID device transmits a RF wave which can be retrieved by any reader. So one would know what RF wave contains i.e., information of the object. This is a big issue in case of banking, military etc. So it is very important to hide the information from hackers. Before the device is transmitting the signal it should be encoded so that no one can extract the information of the target. This encoding is done using Turbo Coding. This is very secure than other encoding techniques. This encoded signal cannot be hacked by any person as it is a significant method and it is unique to only that particular tag and reader. To this encoded signal a separate ID is given so that whenever a reader reads the ID it retrieves the particular encoding method and can read the information regarding the object.

II. TURBO CODING

The Turbo codes are designed by using two or more Convolutional Coders and interleaver which gives various configurations. These configurations therefore could be parallel, multiple parallel, serial and hybrid configurations. The main difference in respect of the Parallel Concatenated Convolutional Code (PCCC) and Serial Concatenating Convolutional Coding (SCCC) encoders is based on their arrangements and in respect of the decoders. It is based on the use of the output of the 'A Posteriori Probability' (APP) Decoder wherein the PCCC decoder does not make use of the output of the 'A Posteriori Probability' (APP) Decoder related to the updated likelihood ratios of the coded symbols, whereas the SCCC does. Since these codes have been providing superior performance, these schemes are therefore being implemented in many real life applications. Multiple parallel and Hybrid configurations show variation in the arrangements of the Convolutional Coders. It has been established that the Turbo codes can give the performance close to Shannon's limit by using the simple Convolutional Coders and the interleaver of large size. The Turbo codes are designed by using two or more Convolutional Coders and the decoding is performed by the decoder having the less complex structure and making use of the iterative decoding algorithm. Therefore for developing the efficient Turbo codes, the efforts therefore have been primarily on designing better and better interleavers and designing better and better Convolutional Coders.

III. CONVOLUTIONAL CODER

Depending on the arrangements of the constituent encoders and the interleaver, the turbo codes are designated as either PCCC or SCCC. In this paper, we have concentrated only on the Convolutional encoder as the constituent encoder of the Turbo Coding Scheme. The most typical form of a Convolutional encoder is the non recursive non systematic convolutional (NSC) encoder. An example of NSC encoder is shown in Fig. 1. The input to the encoder at time t is a bit d_k, and the corresponding code word is the bit pair (u_k, v_k), where

$$u_k = \sum_{i=0}^{K-1} g_{1i}\, d_{k-i}$$
$$v_k = \sum_{i=0}^{K-1} g_{2i}\, d_{k-i}$$

The g_{1i} and g_{2i} can take the values of either '0' or '1'.

$G_1 = \{g_{1i}\}$ and $G_2 = \{g_{2i}\}$ are the code generators, generally expressed in octal form, and d_k is represented as a binary digit. It can be seen that since the encoder is nonsystematic in nature, it has got the finite impulse response (FIR).

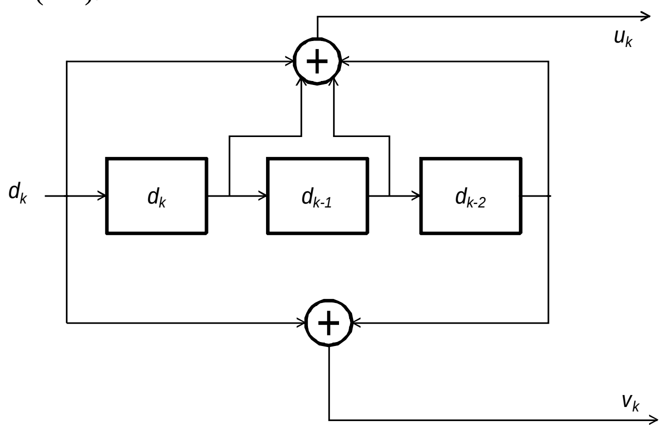

Fig. 1 An example of a nonsystematic Convolutional encoder

It has been observed from the literature that the BER of a NSC code is lower than that of a Systematic code (SC) at high signal-to-noise ratio if the constraint length is kept same. In general at low SNR, the performance of NSC and SC are reversed.

IV. ROLE OF THE INTERLEAVER

In the Turbo coding design the minimum distance is not decided by the constituent encoder but by the design of the interleaver, however designing of such interleaver still remains a challenge. The design of the interleaver affects the overall performance of the code and an interleaver which interleaves the data in a random fashion provides better performance in comparison to the block interleaver. Therefore the research has been concentrated on the design of the interleaver which permutes the data in the random fashion.

V. SCCC TURBO ENCODER

A SCCC encoder is similar to the serial concatenated codes. The main difference is that an interleaver is located between the output of the outer encoder and the input of the inner encoder. Serial concatenation of Convolutional codes is a straight forward extension of conventional turbo codes. A serial turbo code C is also an (M_b,K_b) linear block code (where M_b is the length and K_b the dimension). It results from the serial concatenation of two convolutional encoders Encoder I and Encoder II as depicted in Fig. 2.

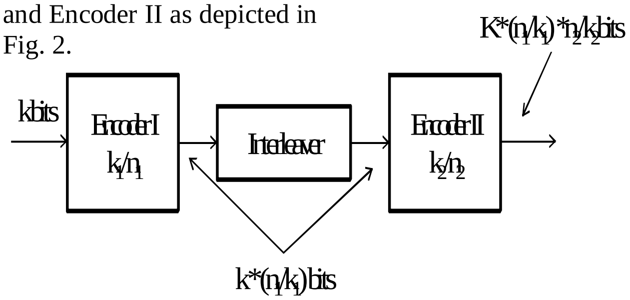

Fig. 2 SCCC Encoder

Encoder I is called the outer code and Encoder II is called the inner code. The trellis of both codes starts and ends at the zero state after K_b /k_1+T_1 trellis transition for encoder I and N/k_2 + T_2 for Encoder II. The outer code can be chosen as either systematic or not, but the inner code must be recursive systematic so as to make the iterative decoding work efficiently. The K_b information bits are encoded by encoder I to produce N= K_b /R_1 bits x', which are interleaved by [PI] and encoded by Encoder II to produce M_b =N/R_2 coded bits c. Since encoder II is systematic, c contains the permuted version of x. The rate of the serial turbo code C without taking the trailing zeros is R = R1*R2. By taking the trellis ending into account the rate becomes

$$\frac{K_b}{M_b+n_1T_1+n_2T_2} = \frac{R_1R_2}{1+(n_1T_1+n_2T_2)\frac{R_1R_2}{k}}$$

VI. SCCC TURBO DECODER

The received symbols x and y are fed into the decoder MAP (Inner). At the first iteration the extrinsic information z_0 is set to zero. After decoding, the output extrinsic information $\Lambda_c x^i + z_i'$ is deinterleaved and input into the outer decoder as apriori information $\Lambda_c x^o + z_i$. After decoding we have output $z_i + \Lambda_c x^o + z_o'$. $z_i + \Lambda_c x^o$ is subtracted from the output of the second decoder and interleaved before input to the inner decoder as extrinsic information for the next iteration. For the last iteration, a hard decision is made on the output of the outer decoder $z_i + \Lambda_c x^o + z_o'$. Fig. 3 shows the decoder structure for an SCCC with the log MAP algorithm as the constituent decoder. Note that the decoding order of each CC is fixed since the outer code is encoded before the inner code. Therefore the inner code must be decoded first before the outer code can be decoded.

VII. DESIGN APPROACH OF TURBO ENCODER

The performance of the Turbo Coding scheme depends on the constituent encoders. In this paper, the approach that has been followed is to design the convolutional encoders in respect of the fading channel and then use these convolutional encoders for designing the turbo codes by serially concatenating them.

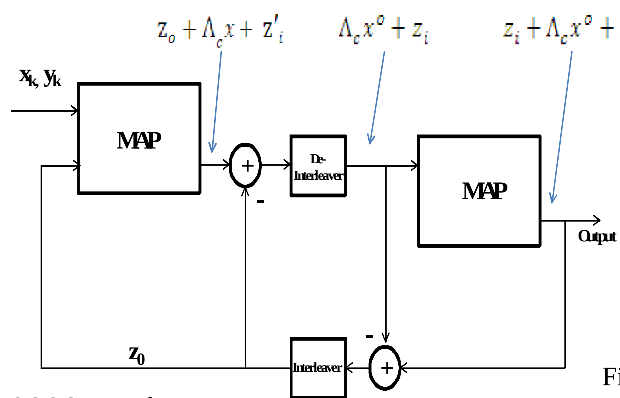

Fig. 3 SCCC Decoder

For undertaking the performance analysis of the turbo codes, there are only two approaches. One is the theoretical approach which is much more complicated and complex and the second approach are through computer simulations. In this, the second approach has been followed and the performance analysis has been undertaken using computer simulation. In the next section, the various Turbo coding schemes that have been designed and developed is presented. The block diagram for simulation in respect of Turbo Coding is shown in Fig. 4. The Turbo encoder is based on serial concatenation of two convolutional encoders separated by an interleaver. The parameters of the function poly2trellis within the convolutional Block have been changed as per the design parameters.

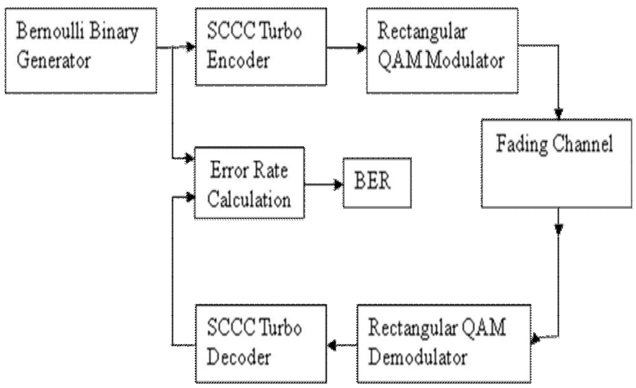

Fig. 4 Simulation in respect of Turbo Coding Scheme

VIII. RESULTS AND DISCUSSION

Performance analysis of code rate 1/3 for different FEC schemes

For code rate 1/3, 8-state, 8PSK

Fig. 5 shows the performance analysis in respect of Turbo Coding Scheme based on Serially Concatenated Rate 1/3, 8 State Convolutional Codes for Fading Channel. The poly2trellis (4, [10 3 15]) has been used in Simulink.

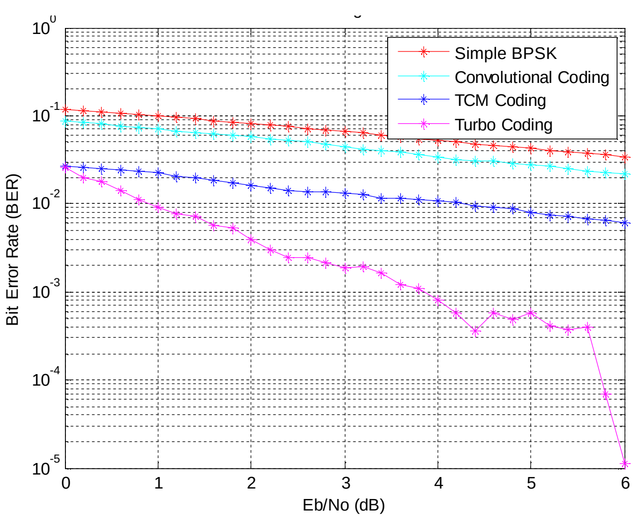

Fig. 5 Performance analysis of Turbo Coding Scheme based on Serially Concatenated Rate 1/3, 8 State Convolutional Codes

The graph is plotted between E_b/N_0 in the range 0 to 6dB and BER in the range 10^{-5} to 1. The Turbo scheme shows better BER performance when compared to the other schemes and this improvement is more pronounced at higher values of E_b/N_0. The performance of the uncoded BPSK, Convolutional, TCM and Turbo schemes is tabulated in table 2 for the 1/3, 8-state coding rate for different values of Eb/No in the interval 0 to 6dB in steps of 1dB.

Eb/No	BER of Uncoded BPSK scheme	BER of Convolutional coding scheme	BER of TCM coding scheme	BER of Turbo coding scheme
0	0.119729	0.086499	0.027017	0.025601
1	0.099092	0.071389	0.022628	0.009069
2	0.080762	0.057991	0.016155	0.003919
3	0.066333	0.044709	0.013084	0.001879
4	0.05255	0.033448	0.010883	0.000805
5	0.04307	0.027814	0.008015	0.000585
6	0.034514	0.022153	0.006001	1.11×10^{-5}

Table 2 Performance analysis of different coding schemes for the 1/3, 8-state coding rate

IX. CONCLUSION

As mentioned above in the earlier section, safety and privacy are the main concerns in RFID technology. To make the technology of RFID more efficient, Turbo Coding technique is analyzed in this paper. In this method the data is encoded more securely using interleavers and convolution encoders. The Turbo coding technique is a powerful coding scheme capable of giving the data rate close to the Shannon's limit. Therefore the work is undertaken with regards to the development of Turbo Coding techniques optimized for fading channels. The design of the Turbo coding scheme for 1/3 code rate based is presented. In this, the performance analysis of the designed Turbo scheme is presented in comparison with the existing Coding Schemes. After encoding data to be radiated is appended with a message ID so that whenever a reader reads the ID it retrieves the particular encoding method and can read the information regarding the object.

REFERENCES

[1] Hyangjin Lee, Jeeyeon Kim, "Privacy threats and issues in mobile RFID"*Korea Information Security Agency.*

[2] Bahl L. R., Cocke J., Jelinek F., and Raviv J., "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate", IEEE Transactions on Information Theory, March 1974, Vol. 20, No. 2, pp. 284-287.

[3] Barbulescu A. S. and Pietrobon S. S., "Interleaver design for turbo-codes," Electronic Letters, Vol. 30, No. 25, Dec. 8, 1994, pp. 2107.

[4] Benedetto S., Divsalar D., Montorsi G. and Pollara F., "A Soft-Input Soft-Output Maximum A Posteriori (MAP) Module to Decode Parallel and Serial Concatenated Codes," The Telecommunications and Data Acquisition Progress Rep. 42-127, November 1996, Jet Propulsion Lab. Pasadena, California.

[5] Benedetto S, Divsalar D., Montorsi G. and Pollora F., "Serial Concatenation of interleaved codes: Performance analysis, design, design, and iterative decoding", IEEE Trans. Inform. Theory, Vol. 44, May 1998, pp. 909-926.

[6] Benedetto S, Divsalar D., Montorsi G., and Pollara F., "Serial concatenated trellis coded modulation with iterative decoding", IEEE International Symposium on Information Theory, Ulm, 1997, pp. 8.

[7] Benedetto S., Turbo Codes, ICC'96 Tutorials, Dallas USA, June 23 – 25, 1996.

[8] Benedetto S., Divsalar D., Montorsi G., and Pollara F., "Serial concatenation of interleaved codes: performance analysis, design and iterative decoding", IEEE Transactions on Communications, Vol. 44, May 1998, pp. 909-929.

[9] Benedetto S., Divsalar D., Montorsi G., and Pollara F., "Soft-output decoding algorithms in iterative decoding of parallel concatenated convolutional codes", Proceedings of 1996 IEEE International Conference On Communications, Dallas, Texas, Vol. 1, June 1995, pp. 112-117.

[10] S. L. Garfinkel, A. Juels and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, vol.3, pp34-43, May/June 2005.