ISSN:0975-9646

Adaptive Fault Free and Secured Path Selection in Wireless Sensor Networks

Deepali Virmani[a], Pranav Gupta[b]

[a]*Department of IT,Professor&Head,*
Bhagwan Parshuram Institute of Technology,New Delhi110085,India
[b]*Department of IT, UG Student,*
Bhagwan Parshuram Institute of Technology,New Delhi110085,India

Abstract -Wireless sensor networks is a time honoured and has unbounded range of applications. . Nodes are prone to fail due to energy depletion, hardware failure, malicious attack and so on. Distributed storage systems for large clusters typically use replication to provide reliability. This paper introduces a adaptive fault free and secure routing in wireless sensor network and reliability is achieved by introducing a family of packet erasure codes based on Reed-Solomon codes which allow for fast encoding and decoding for large block lengths and provides load balancing, dynamic swapping of components and power saving.[1]

1. INTRODUCTION

Wireless sensor networks are small subset of wireless networking and is just now reaching the maturity level necessary to make it commercially viable. These sensor networks are made of low cost spatially distributed sensor nodes with limited computational power and memory.WSN have environmental applications, medical monitoring, home security, surveillance, military applications, air traffic control, industrial and manufacturing automation, process control, inventory management, distributed robotics, etc [2]. In this paper we are proposing a data storage system using forward error correcting codes (erasure codes) in order to provide reliability and fault tolerance in the system by providing backup node and link, more than that the recovery of the lost data over a lossy channel is proposed using Reed Solomon codes. Remainder of paper is organised as follows, section 2 briefly states the related work. Section 3 describes the proposed algorithm. In section 4 simulation results and comparison is shown. In section 5 conclusion and advantage of the proposed algorithm is presented and section 6 shows list of references.

2. RELATED WORK

In[3], Yuanming Wu et. al. discussed security vulnerabilities of watchdog mechanism and trust mechanism and also examined how inside attackers could exploit them. Their trust mechanism involved three stages: 1) node behaviour monitoring, 2) trust measurement, and 3) insider attack detection.

In [4], Ung-Jin Jang et. al. discussed fault-tolerant time synchronization algorithm for wireless sensor networks that requires a short time for synchronization, achieves a guaranteed time synchronization level for all non-faulty nodes, accommodates nodes that enter suspended mode and then wake up, is computationally efficient, operates in a completely decentralized manner.

In [5], Alexandros g et. Al. implement new codes in Hadoop HDFS and compare to a currently deployed HDFS module that uses Reed Solomon codes. Our modified HDFS implementation shows a reduction of approximately 2_ on the repair disk I/O and repair network.

In [6], Jian yin et. al. proposed a hierarchal secure routing protocol against black hole attack which used symmetric key cryptography to discover a secure route against black hole attacks. For detection of cooperative black hole attack a randomized data acknowledgement scheme is proposed.

3. PROPOSED SYSTEM

3.1 *Distributed store and retrieve operation*

Our distributed store and retrieve operation is straight forward application of MDS codes to WSN. Suppose that we have n nodes. For store operation, we encode a block of data of size d into n symbols. Each of size d/k, using an (n,k) MDS array code. We store one symbol per node. For a retrieve operation, we collect the symbols from any k nodes and decode them to obtain original data. This data storage scheme has many attractive features. Firstly, it provides reliability. The original data can b recovered from n-k nodes failures. Secondly it provides dynamic reconfigure ability and hot swapping of components. We can dynamically remove and replace up to n- k nodes. In addition the flexibility to choose k nodes out of n nodes permits load balancing ,we can select k nodes with the smallest load, or in case of wide area network k nodes which are geographically closest.

3.2 *Proposed FAULT RECOVERY in WSN*

The node memory is divided into two sections:

1. Data memory.
2. Redundant memory.

The storage and recovery of encoded data if performed within redundant memory of node.

3.2.1 Store operation:

1. Encoding :'d' sized block into 'n' symbols each of size 'd/k' using (n,k) MDS array codes.
2. Then store each symbol per node. Every node communicates with every other node to pass on the encoded data. This is a centralised system initiated after every fixed interval if time by the base station.

3.2.2 Retrieve operation:

1. Decoding: collect all symbols from any k nodes and decode to get original data.
2. When data is lost the base station collects data from any k nodes and decodes using XOR operation.

3.2.3 Decoding at receiver:

An error correction and detection system is also introduced to detect the transmission error in the packet and correct them. The block codes like Reed- Solomon codes are used which are highly efficient and have high throughput. It is the most efficient and require low computation as well as energy.

Proposed Algorithm

1. All nodes broadcast energy to every other node after every cycle.
2. Cluster head is assigned dynamically based on residual energy by the base station.
3. Every node lives in either of 3 states according to power limitations.
   - Sleep = it turns off the radio for energy saving.
   - Discovery = broadcast discovery message to neighbouring node. Can receive information but can't send.
   - Active = broadcast discovery message and communicates by sending and receiving information.

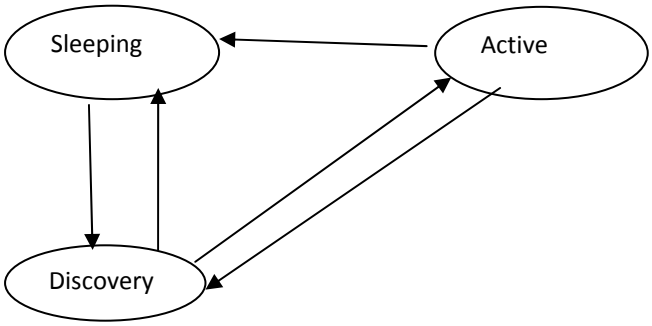


Figure 3.1: interstate transitions.

These states consider the energy used in both sending and receiving the information by the nodes in the WSN. Let E_n be the energy of the nodes and threshold energies are as follows.

Threshold energy for active state – T_1

Threshold energy for receiving data – T_2

1. For sleep state:
   $E_n <= T_2$ (1)
2. Discovery state:
   $T_2<E_n<T_1$ (2)
3. Active state:
   $E_n >= T_1$ (3)
4. Data storage and recovery by fault management uses redundant memory. Two operations are performed. Firstly, store and then retrieve using MDS coding technique.
5. Error detection and correction at receiver node using RS codes.

Proposed algorithm

1. Select CH by centralised broadcasting of energies.
2. Initialise timer T_e.
3. BS calculates T_1 & T_2 /* threshold energies*/
4. Assign S ,A or D. /*states to each node*/
5. If ($E_n <= T_2$)
6. State = s
7. Else if($T_2<E_n<T_1$)
8. State = D
9. Else
10. State = A
11. Store states in redundant memory of each node.
12. Create recovery. /*using (n,k) MDS array codes*/.
13. Encode data. /*using (n,k) block codes */
14. Store data in each nodes.
15. At receiver decode data to detect error and correction. /* using Reed-Solomon codes*/.
16. If(data loss)
    Select any 'k' nodes.
    Start recovery.

END

4. RESULTS AND COMPARISONS.

4.1 *Reed Solomon Error Probability*

Reed Solomon codes are mainly used for burst error correction. However the code has its own error correcting capability. So, the error probability plays a crucial role in saving our time detecting and correcting the error. Let us assume that the code can correct 4 error symbols in an (255,251) RS code. A maximum of 32 bits of error can be corrected. So, if we can calculate the bit error rate properly and then manage the syndrome calculation part as if the decoder calculates more than 32 bits of error, then send a signal that decoder cannot correct. Therefore plotting the bit error probability (P) against the SNR will help. We can have a range of SNR for which the error can be corrected. However the range will include many parts like the percentage of probability that the signal will get detected. Figure 4.1 shows the plot between bit error probability and SNR. The code is for a random of about 255 symbols where each symbol contains 8 bits being transmitted. These 255 symbols form a code word. And there are about 500such code words. However the range estimation for different capability of correcting errors can be calculated.

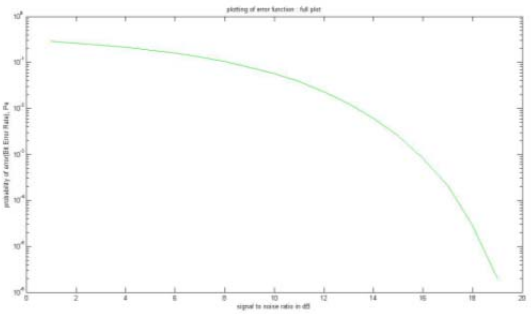


Fig 4.1 :Graph between SNR and Bit error rate (BER)

To analyse the error probability graph, 255 symbols corresponds to m=8, therefore each symbol will contain 8 bits. And for different error correcting capability different range of SNR can be deduced. So, for different error correcting capability the number of error bits can be found out from the graph. For example for 2t=4; t=2 16 error bits can maximum be corrected. So a range of SNR can be found out using the graph. Similarly for 2t=8; t=4 at maximum 32 bits can be corrected. This range of SNR would be quite bigger than the last range. This result helps us to find out whether the decoder can correct the received signal or not which saves our lot of time and efforts.

4.2 ***Simulation results***

Our main aim for simulating the same in MATLAB was to understand the phenomenon as how the signal is being transmitted, what would happen if the signal has some error and up to what extent, the decoder can detect and correct errors. In MATLAB, a random symbol of integers was taken as input. These random symbols were then encoded using RS encoder. And some random symbol noise was added to the input, these symbols were then received at the decoder end. Now at the decoder end, the decoder can correct up to 2t symbols. Our basic aim was to see if any error would have occurred in the parity symbols then what result comes out. The reed Solomon decoder actually corrects symbols up to 2t symbols from the n number of symbols. It never matters to him whether the errors are in parity symbols or the information symbols. After correcting the error, however the decoder takes the redundant bits out which were generated while encoding the symbols. An output with errors in parity symbols (first one parity symbol error and then two parity symbol error) will be shown in the results. However a comparison between the decoded and received data and the encoded data structure will be shown in figures. This comparison will be shown in RS (255,251) code. The analysis was done using RS (15,7) because it is easy to produce an error in an parity symbol in a 15,7 code than in an 255,251 code. Figure 4.2 shows the comparison between the encoded data and the message symbols which shows that 251 information symbols are the same as the old one while the 4 parity symbols are added in the encoded data. And the Figure 4.3 shows the comparison between the decoded data and the message symbols when the errors are corrected.

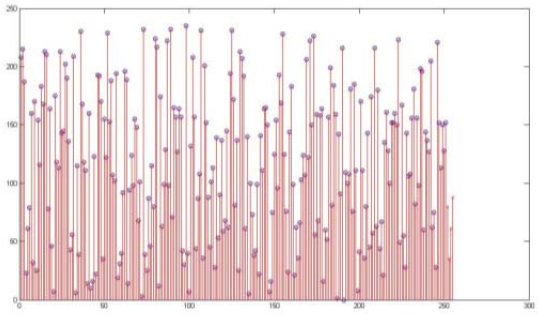


Fig 4.2: comparison of encoded and message symbols

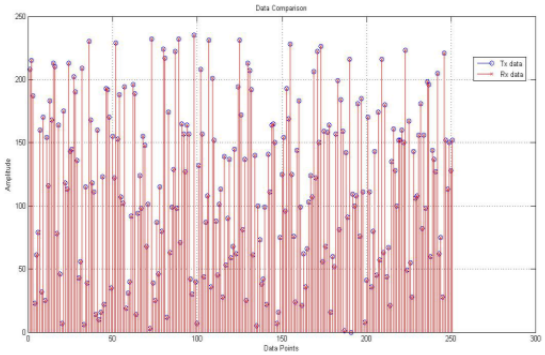
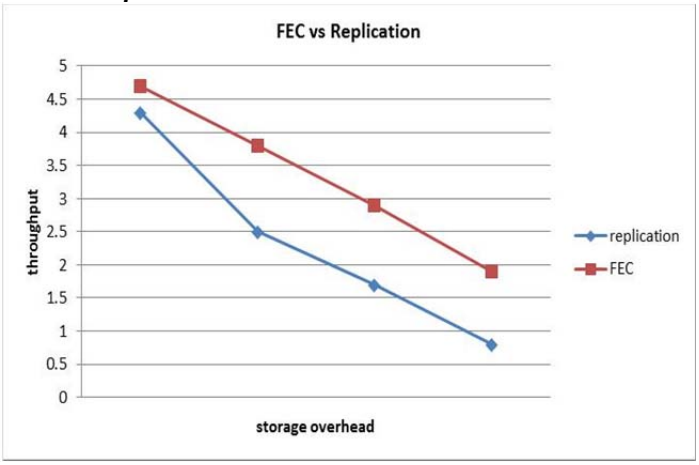


Fig 4.3: comparison of decoded and input data

4.3 Comparison of FEC codes and data replication technique.



5. ADVANTAGES

1. Fault tolerance by providing backup nodes in active and discovery states and resilient data aggregation which is made robust in presence of any adversary.
2. Load balancing by broadcasting energies and heterogenous system enables in providing link hetroginity and computational hetrogenity.
3. Data storage in any of the k nodes and checking data plausibility using Reed- Solomon codes .
4. Recovery of lost data from any k nodes using MDS array codes.
5. Energy saving and dynamic swapping of the system components .

REFERENCES

[1]. J.P. Walters, Z. Liang, W. Shi, V. Chaudhary, "Wireless Sensor Network Security: A Survey", *Security in Distributed, Grid and Pervasive Computing*, pp.3-5, 10-15, 2006.

[2]. Clustering in Wireless Sensor Network using K-MEANS and MAP REDUCE Algorithm.

[3]. V. Katiyar, N. Chand, S. Soni, "A Survey on Clustering lgorithms for Heterogeneous Wireless Sensor Networks" Int. J. Advanced Networking and Applications Vol. 02, Issue: 04, pp. 745-754, 2011

[4] Ung-Jin Jang, Sung-Gu Lee, Jun-Young Park, Sung-Joo Yoo " fault-tolerant time synchronization algorithm for wireless sensor networks'' doi:10.4236/wsn.2010.210089 October 2010 (http://www.SciRP.org/journal/wsn/) Copyright © 2010 SciRes.

[5] Alexandros G. Dimakis University of Texas at Austin XORing Elephants: Novel Erasure Codes for Big Data

[6] A. Perrig, J. Stankovic, D.Wagner, "Security in Wireless Sensor Networks", *Communications of the ACM*, 2004, pp.53-57.