Compressive Sensing in Data Loss Recovery using Wireless Network
M. Tamilarasan¹ K. Ramsundar² M. Sankara Narayanan³ G. Shunmuga Priya⁴
¹,²,³ Department of Electronics & Communication Engineering
¹,²,³,⁴ S. Veerasamy chettiar college of engineering, Puliyangudi

Abstract— In wireless sensor network data loss is the major problem which occurred during the transmission of data between sensor nodes over the network. The loss of data should affect the communication between source and destination so, to minimize or to reduce the data loss, data loss recovery scheme called as “compressive sensing” based data loss recovery mechanism is proposed. Compressive Sensing technique can be embedded into smart wireless sensors and effectively increases wireless communication reliability without retransmitting the data and also to reduce communication time and power savings. According to the theory of CS, the raw signal can be effectively reconstructed from the received incomplete transformed signal given that the raw signal is compressible in some basis and the data loss ratio is low. To secure the communication data by using cryptography standard mechanism. It is used to save the confidentiality of transferred between source and destination.

Key words: Compressive Sensing technique, Wireless Sensor Network Formation, Compressive sensing

I. INTRODUCTION

Wireless sensor network is interconnected with sensor nodes which is to communicate data without traffic. Wireless data transmission is particularly susceptible to packet loss. The reliability of wireless transmission highly relies on the communication Radio interference, i.e., other devices operating on the same frequency. Weather problems such as, Rain and Lightning, Poor Installation, Antenna Orientation, Maximum transmission distances, Obstructions, Hardware Problems, etc. Reactive retransmission in which the sender is notified to retransmit the lost data packets until all data is received at the destination. Less sparse signals can also be effectively reconstructed provided that data loss ratio is lower. The data reconstruction performance drops with the decreasing scarcity of acceleration signal and the increasing data loss ratio. station. Our proposed system is a CS-based lost data recovery approach for smart wireless accelerometers used in SHM. The basic idea of this CS-based approach is that, instead of transmitting the raw acceleration signal, a transformed signal which I a transformed signal which is created by projecting the raw signal onto a random matrix, is transmitted. Some data loss may happen during the transmission of this transformed signal. However, according to the theory of CS, the raw signal can be effectively reconstructed from the incomplete transformed signal given that the raw signal is compressible in some basis and the data loss ratio is relatively low. While this work shows great promise of CS to improve the reliability of wireless transmission, implementation on a wireless sensor platform has yet to be realized. Researchers have proposed various methods to cope with the data loss issue in wireless transmission. Reactive retransmission, in which the sender is notified to retransmit the lost data packets until all data is received at the destination, has popularly been applied. However, retransmission based methods generally suffer from communication delay and significant bidirectional traffic (NACK/ACK 3 messages) that makes them less efficient in many scenarios. Despite the possible inefficiencies, link-layer retransmission is still widely employed by researchers for wireless SHM. All adopt such an approach to enhance the data transmission reliability of their respective wireless sensor systems.

Though a complete framework of data loss compensation for wireless smart sensor has been established as described above, embedding the framework into a wireless sensor platform requires several important issues to be addressed. Because this study does not attempt to compress the raw data using the CS algorithm, a square sampling matrix with m equal to n is adopted for the transmission. A larger n is desirable in the sense that the acquired data tends to have a higher sparsely ratio when data is longer, which in turn, accommodates more data loss, especially when continuous data loss occurs. A sampling matrix with n equaling to 3,000 was employed by the entries of the matrix are independently and randomly generated from an identical Gaussian distribution.

Fig. 1:
The data transformation and recovery are performed segment by segment, the data loss per segment, not the overall data loss ratio, bounds the reconstruction performance. Therefore, data loss statistics mainly deals with the mean, minimum and standard deviation of segment-wise data loss. Data transmission is reliable up to 100 meters with an almost perfect average received data ratio. The minimum received data ratio per segment is above 90% for all measurement distances within 120 meters. A sharp decrease of communication performance is observed when communication distance reaches above 140 meters. The average received data ratio drops to around 80%. Some data segments are almost completely lost at 150 meters. Reliable recovery of such data segments is impossible.

II. SYSTEM ANALYSIS

In this project, the various similar projects of compressive sensing based data loss recovery systems used were surveyed and a better system is proposed. This chapter includes the existing system and the outcome of this project. The existing system framework should analyze the connection efficiency of wireless sensor network with limited number of nodes. Communications over wireless networks are particularly vulnerable to data loss due to the broadcast nature of the wireless medium.

To protect confidential message transmission, physical layer security has been developed as a promising mechanism which provides the protection at the physical layer by exploiting the random and noisy nature of the wireless propagation channels. The data transmission is possible at limited range of base station coverage.

In which we investigate the effects of user cooperation on the secrecy of broadcast channels by considering a cooperative relay broadcast channel. The proposed system should construct the wireless sensor network with sensor nodes. Then each node is connected to the base station by using their unique id. The base station should establish the connections of each sensor nodes within the coverage range. Based on the coverage range the sensor nodes can transmit their data over the wireless network. The route between the source and destination should be established by the Dynamic source routing protocol. Each nodes transferred their packets through the shortest path which is used to reduce the transmission data of each sensor nodes and save the energy of each nodes. If the packets are mishandled by third parties, their confidentiality should be affected that will produce packet loss at destination nodes. In order to reduce the packet loss, the packet retransmission mechanism is developed and in which loss of data are retransmit by intermediate nodes. Here the energy of the source node should be saved.

The compressive sensing algorithm provides such a data loss recovery technique. This technique can be embedded into smart wireless sensors and effectively increases wireless communication reliability without retransmitting the data. Also confidentiality of the data should be secured by using the cryptographic standards.

A. Encryption:

Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice.

B. Compressive Sensing:

Our proposed a CS-based lost data recovery approach for smart wireless accelerometers used in SHM. The basic idea of this CS-based approach is that, instead of transmitting the raw acceleration signal, a transformed signal which is created by projecting the raw signal onto a random matrix, is transmitted.

C. Decryption:

Decryption is the reverse process of converting encoded data to its original un-encoded form.

III. SYSTEM ARCHITECTURE

A. Wireless Sensor Network Formation:

Wireless sensor network is an interconnection of Sensor Nodes to Transmit and Receive Information over the wireless media. This kind of network consists of base station and Nodes (Sensors). The base station should control the entire networks. It also provides the private and public key for every node whenever involved in data transmission.

B. Establishment of Connection between Source and Destination:

The base station should establish the connection between the source and destination whenever the nodes are connected to the network. Before the establishment of connection the base station should verify the identities of the nodes.

C. Transmission of Data through Intermediate Nodes:

The base station should establish the routing between the source and destination using Dynamic Source Routing Protocols. This protocol is used to govern the data communication over the network depends on the distance between the source and destination of the network.

D. Dynamic Source Routing:

Routing protocols determine the best path to each network, which is then added to the routing table. One of the primary benefits of using a dynamic routing protocol is that routers exchange routing information whenever there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths if there is a link failure to a current network. Compared to static routing, dynamic routing protocols require less administrative overhead. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice.

E. Compressive Sensing:

Our proposed a CS-based lost data recovery approach for smart wireless accelerometers used in SHM. The basic idea of this CS-based approach is that, instead of transmitting the raw acceleration signal, a transformed signal which is created by projecting the raw signal onto a random matrix, is transmitted.
If the distance is maximum, the data should be forwarded through the intermediate nodes depending on the energy and coverage area.

**F. Data Recovery Scheme Implementation:**
The data should be traveled on the routing path of source and destination while the data loss occurs due to the interference of the network environment. As the result of data loss, the destination does not receive the data from the source node. So the communication between the source and destination should be meaningless. To avoid this kind of data loss, “Compressive Sensing” technique with temporary buffer this used to store the data temporarily until the success full transmission is achieved.

**G. The Data Confidentiality through Cryptography Standards:**
The confidentiality of the data should be maintained until it reach the destination from source node along the routing path is an important during each and every transmission over the transmission media. So implementation of the cryptography mechanism to avoid illegal access of data over the transmission path and is performed and also it maintained the confidentiality of transformed data, security of network environment.

**IV. RESULT AND DISCUSSION**

**A. Wireless Sensor Network Formation:**
Wireless sensor network is an interconnection of Sensor Nodes to Transmit and Receive Information over the wireless media. This kind of network consists of base station and Nodes (Sensors). The base station should control the entire networks. Also provide the private and public key for every node whenever involved in data transmission.

**B. Establish The Connection Between Source And Destination:**
The base station should establish the connection between the source and destination whenever the nodes are connected to the network. Before the establishment of connection the base station should verify the identities of the nodes.

**D. Data Recovery Scheme Implementation:**
The data should be traveled on the routing path of source and destination while the data is loss due the interference of
the network environment. As the result of data loss the destination does not receive the data from the source node. So the communication between the source and destination should be meaningless. To avoid this kind of data loss using Compressive Sensing technique with temporary buffer this used to store the data temporarily until the success full transmission.

E. Improve The Data Confidentiality Through Cryptography Standards:
The confidentiality of the data should be maintained until reached the destination from source node along the routing path is an important during each and every transmission over the transmission media. So implement the cryptography mechanism to avoid illegal access of data over the transmission path and also maintained the confidentiality of transformed data, security of network environment.

V. CONCLUSION
Our implementation of a Compressive Sensing (CS)-based framework for data loss recovery into a wireless smart sensor platform using NS2 is proposed. To overcome the constraints of limited onboard resources of wireless sensor nodes, a method called compressive sensing is employed to provide memory and power efficient construction of the random sampling matrix. The data reconstruction performance drops with the decreasing scarcity of acceleration signal and the increasing data loss ratio. In the developed CS-based wireless transmissions can be used effectively for acceleration signals that have a segment spectral sparsity ratio above 0.85 and a maximum segment data loss ratio below 0.2. The data reconstruction process is shown to largely improve the signal quality from incomplete data for stationary signal that results from the data transmission medium. The confidentiality of data through cryptography standards is achieved. The data loss ratio achieved is 10%.

VI. REFERENCE PAPER

REFERENCES