Development of Fishplate Tampering Detection System for Railway Security based on Wireless Sensor Network

Krishnendu Ghosh,
Student Member, IEEE
Department of Electronics and Telecommunication Engineering,
Bengal Engineering and Science University, Shibpur
Howrah, West Bengal,
India

Ashish Singhi
Department of Electronics and Telecommunication Engineering,
Bengal Engineering and Science University, Shibpur
Howrah, West Bengal,
India

Chirasree RoyChaudhuri
Member, IEEE
Department of Electronics and Telecommunication Engineering,
Bengal Engineering and Science University, Shibpur
Howrah, West Bengal,
India

ABSTRACT

Intelligent sensors with cognitive ability when wirelessly networked can be deployed in a wide range of applications. This paper reports a novel fishplate tampering detection system for railway security based on wireless sensor network. Fishplates are tampered when the nuts and bolts are loosened so that the railway lines wouldn't remain perfectly aligned, leading to derailment of trains. The existing efforts use long length fibre optic cables which are complex to install and expensive. The smart system with cognitive wireless sensors proposed in this paper employs sensitive, cost effective and flexible piezoresistive pressure sensors which show large changes in resistances as soon as the nuts and bolts of the fishplates are loosened. These changes are processed with a MSP430 microcontroller and transmitted through the CHIPCON CC2500EM at a frequency of 2.4 GHz. Further, power saving schemes have been adopted to minimize the consumption of power along with other safety precautions. Thus the system sends early warning messages to the nearest control room whenever an unforeseen tampering act is attempted.

General Terms

Application of Wireless Sensor Network in Railway Security which is a part of Urban Development.

Keywords

Fishplate Tampering, Railway Security, Wireless Sensor network, Flex-piezoresistive sensor, Low-power mode.

1. INTRODUCTION

India has the third largest railway network after the USA and China. Rail track security is naturally a concern for the authority (more so after the recent Jnaeshwari express accident). The most common act in tampering of rail lines is the removal of the integral fish plates that join the two rails. A fish plate is an indispensable component of track lines. It's a mechanical component, a flat piece of iron that joins one length of the railway line to another. On removing this, the lines wouldn't be perfectly aligned, leading to derailing of trains. Hence, to stop this wicked act of tampering we propose the idea of a security system, which detects the tampering and reports to the nearest railway cabin.

There has been an attempt by a group at Vellore Institute of Technology in 2005 to prevent tampering of fishplates using fibre optics [1,2]. They used long cables along the tracks which are complex to install and also quite expensive. Additionally no power saving scheme has been incorporated in the report which is a necessity for a field deployable system. Moreover, the existing relay system [3] uses heavy wires which are difficult to install; the EIS (Electronic Interlocking System) is based on wireless concept but still uses copper cables [3]. Few countries use imaging to detect micro cracks on tracks [4]. If we use this same technology for detection of tampering of fishplates it will give false signals always when trains will pass over the track. None of them have deployed wireless sensor network with cognitive ability for the railway security. Such sensor network not only detects the signal but also have capabilities to collate and analyse the data to flag out any anomalies if required [5, 6].

In this paper, we deploy sensitive piezo-resistive sensors [7] networked wirelessly to detect the tampering act. As soon as somebody tries to loosen the nut and bolt which keeps the fishplates attached to railway track a change in pressure would be obtained which would be detected by the sensor network. The output of the pressure sensors will be processed by an intelligent controller to estimate whether any nut loosening of the fish plate has occurred and depending on the decision, a security code will be generated and transmitted to the receiver placed in the nearest railway cabin indicating the identity of the tampered fish plate. The battery status is also monitored at frequent intervals to avoid any misinformation due to improper electrical connection or low voltage. Further, we have incorporated a power saving scheme to reduce the average power dissipation.

2. PROPOSED SOLUTION

The scheme that would be followed to meet these specifications in the project is shown in Fig.1:

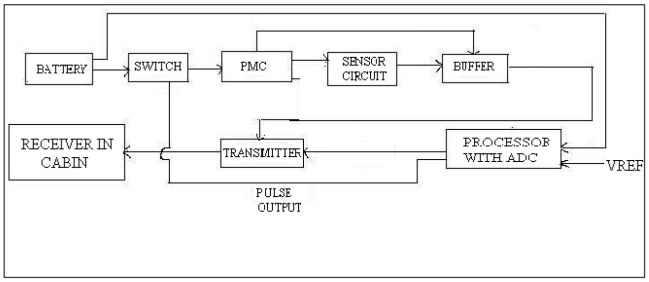

Fig.1: System Block Diagram

.

In this scheme, the main detector device is the piezo-resistive sensor whose resistance varies with pressure applied. The piezo-resistive sensor in the form of a flexible strap is placed in between the fishplate and the nut. The Flex Sensor is based on resistive carbon elements. As a variable printed resistor, the Flex Sensor achieves great form-factor on a thin flexible substrate. When the substrate is bent, the sensor produces a resistance output correlated to the bent radius-the smaller the radius, the higher the resistance value [7].Two holes drilled just below the bolt through the fishplate carries two wires from the sensor, which connects, to the rest of the circuit implanted between the fishplate & the tracks.

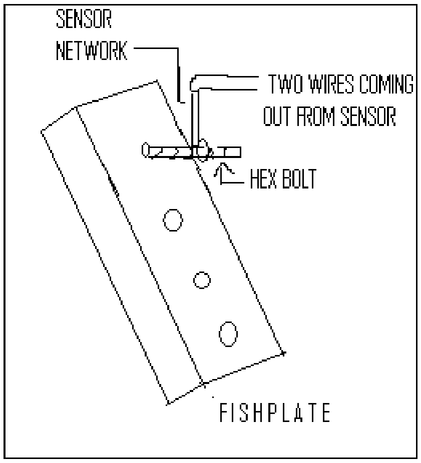

Fig.2: Arrangement of the circuitry behind the fishplate

When the nuts are loosened a change in pressure would be observed. This change is detected by Flex Sensor and the corresponding output serves as an input (via a buffer to avoid loading effect due to mismatch in impedance) to the MSP430 [8]. The output of the Microcontroller is a bit stream. This bit stream signifies any change in sensor output and hence reports whether there is any attempt to tamper the fishplate. Whenever the nuts are in their normal positions a fixed voltage is being sent to the controller which produces a standard bit stream. Now whenever there is any tampering in the fishplate a change in voltage is obtained. This changed voltage is compared with a threshold voltage in the controller to ascertain that the change in voltage is due to fishplate tampering. The microcontroller then generates a different bit stream acting as the alarm code which is transmitted wirelessly to the receiver placed in nearest railway cabin. For multiple sensors placed along the railway tracks, there will be transmitted signals from each of them, hence at the receiver side, time division multiplexing scheme needs to be incorporated to identify the tampered fishplate. To identify which fishplate is tampered we can pad a few extra bits with the sent signal. Suppose if there are N fishplates under the control of a particular cabin then we will pad log$_2$N bits to identify which particular one among those N fishplates is tamperded.

Inspite of using a continuous dc power supply we produced a pulsating voltage of 50% duty cycle to reduce power consumption. We are using a power management chip in our design which operates in the low power mode. Also our software coding technique contributed towards saving power. The pictorial representation of the placement of sensor is shown in Fig 2. Also the controller checks the battery status frequently to avoid any false information.

3. ALL SENSOR SIGNAL CONDITIONING UNIT

The circuit schematic for individual sensor signal conditioning unit has been drawn in the eagle software for simulation. This software is very efficient since it not only allows us to draw our schematics but also allow us to design our own PCB design. Fig. 3 shows our schematic drawn in Eagle Software which helped to design our PCB.

The first block is a switch (SN74CB3Q3306A) whose input is controlled by a periodic signal of 50% duty cycle generated by the micro controller. So the output of the switch is also a same periodic signal which goes to the input pin of the Power Management Chip (TP63020) which provides biasing voltage to other IC like buffer and the sensor network as well. The output of the sensor network goes to the input of MSP430 via a buffer (OPA832). The CC2500 EM [9] present at the USART peripheral pins of MSP430 transmits a signal according to the sensor output. The circuit is driven by a voltage source of 3.3Volts.

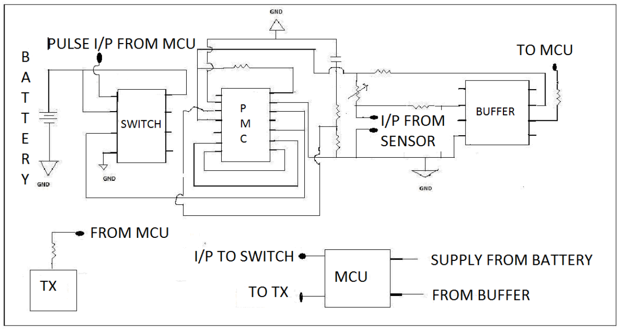

Fig.3: Schematics drawn in Eagle Software

- In case of sudden power cut the Switch [10] inhibits backward flow of current and hence saves the system from getting damaged. Low on state resistance of the selected switch SN74CB3Q3306A gives less propagation delay.
- The PMC chip (TP63020) [11] at low current (as in our case) operates in power save mode to give better efficiency. Voltage divider bias is used to get the exact desired output voltage from it. It is used to drive the sensor network and the amplifier.
- The Buffer chip (OPA832) [12] eliminates loading effect due to mismatch in impedance between sensor network and microcontroller and also provides protection against sudden noise-signals.

We started our simulation portion with the Software TINA which helped us to choose our IC to be used in the design. We analysed the characteristics of IC which we deemed fit for our design. For example we studied the Characteristics of TPS63002 and decided to go for Power Management Chip with enhanced features which is currently in market and ended up with TPS63020. Similarly all other IC's chosen were based on our simulation done in TINA. We got the desired value of divider resistor used in PMC to be 1.3 MΩ to get our desired output 3.3 V to drive MSP430 from Fig.3.

4. COMMUNICATION PROTOCOL

The sensor units are equipped with RF transceivers for two way communication. The receiver at the nearest control station polls the sensor units at regular intervals and gathers the status of the fishplates. The low power consuming CHIPCON CC2500EM is used by the sensor nodes which operates at a frequency of 2.4 GHz and is capable of data transmission at a baud rate of 9600 pulses per second. To make the communication between the sensor nodes and the receiver rigid, error checking has been implemented to check the validity of the transmitted data. The software algorithm is shown in Fig.4 and 5. The algorithm is completely customizable and can be configured depending on the situation.

In our actual design first of all the control signal of the switch is generated by a simple code, so that its power consumption is controlled and is considerably low.

- For transceiving purpose, we used interrupt-driven code [13] to ensure further power saving. In case of any tampering, when input to MCU gets on (Fig 9) the main function calls the interrupt subroutine and operates in LPM3 mode. In this mode the internal DCO clock operates (with the help of auto calibration of FLL+ circuitry) at a baud rate of 9600 Hz for proper transmission with the USART. The USART transmits in SPI (Serial Peripheral Interface) mode.
- In normal condition when the fishplate is not tampered, no transmission is required; hence the microcontroller operates in sleep mode (LPM0 mode) saving the power which would have been consumed due to the operation of DCO clock.

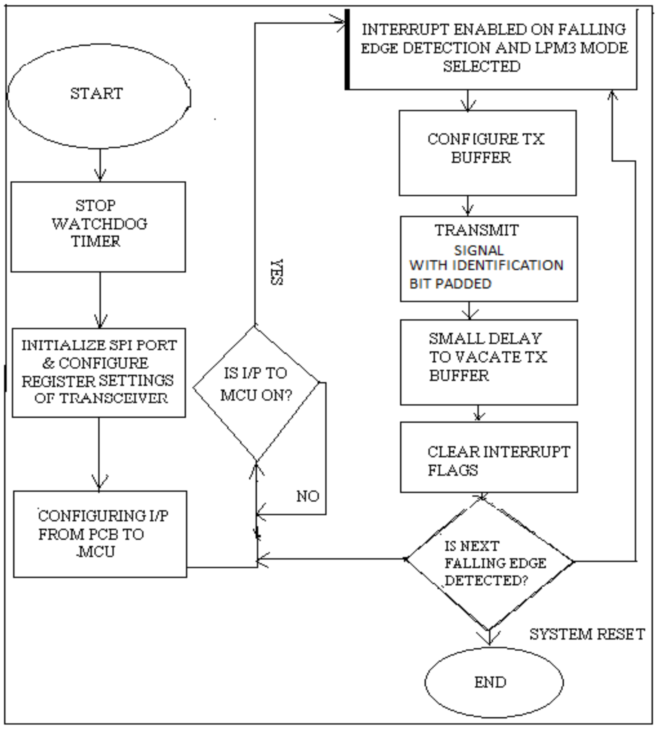
START
STOP WATCHDOG TIMER
INITIALIZE SPI PORT & CONFIGURE REGISTER SETTINGS OF TRANSCEIVER
CONFIGURING I/P FROM PCB TO MCU
IS I/P TO MCU ON?
YES
NO
INTERRUPT ENABLED ON FALLING EDGE DETECTION AND LPM3 MODE SELECTED
CONFIGURE TX BUFFER
TRANSMIT SIGNAL WITH IDENTIFICATION BIT PADDED
SMALL DELAY TO VACATE TX BUFFER
CLEAR INTERRUPT FLAGS
IS NEXT FALLING EDGE DETECTED?
SYSTEM RESET
END

Fig.4: Flowchart of transmitter algorithm

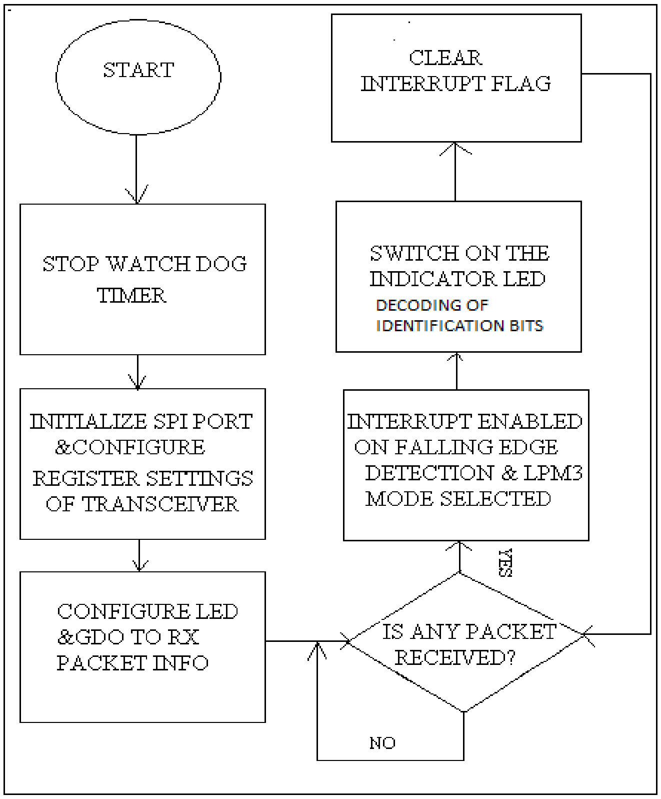
START
STOP WATCH DOG TIMER
INITIALIZE SPI PORT &CONFIGURE REGISTER SETTINGS OF TRANSCEIVER
CONFIGURE LED &GDO TO RX PACKET INFO
IS ANY PACKET RECEIVED?
NO
YES
INTERRUPT ENABLED ON FALLING EDGE DETECTION & LPM3 MODE SELECTED
SWITCH ON THE INDICATOR LED DECODING OF IDENTIFICATION BITS
CLEAR INTERRUPT FLAG

Fig.5: Flowchart of receiver algorithm

5. RESULTS

When in normal position (nuts in their tight position i.e. fishplate connected to tracks):

- Resistance across the sensor network: of the order of 100 kΩ
    - Corresponding voltage across the sensor network (which goes as input to MSP430): of the order of Microvolt.
    - Input to the microcontroller remains high.
    - No transmission takes place.

When tampered (nuts are loosened i.e. fishplates detached to tracks):

- Resistance across the sensor network: of the order of 5MΩ
- Corresponding voltage across the sensor network (which goes as input to MSP430): a square wave of peak voltage 3.7 volt and 50% duty cycle. (Fig. 7)
- Input to the microcontroller goes low and the falling edge wakes up the interrupt subroutine.
- Transmission occurs from the transceiver module at a frequency of 2.4GHz using USART port in SPI mode.
- Glow of LED on the receiver.

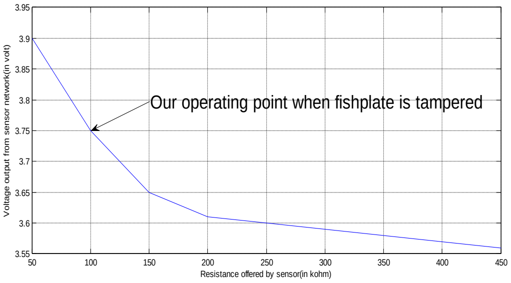

Fig.6: Showing the Voltage output characteristics of the Sensor Network v/s Pressure Applied calibrated in terms of resistance.

The photograph of the PCB is shown in Appendix.

A. *Power consumption without pulse mode*

- Power dissipated in switch per cycle = $V_{CC}I_{CQ}$=0.825mW
- Power dissipated in PMC per cycle = $V_{CC}I_{CQ}$ =2.497mW
- Power dissipated in Buffer per cycle = $V_{CC}I_{CQ}$ = 128.7mW
- Power dissipated in MSP430 = $V_{CC}I_{CQ}$ = $AV_{CC}I_{CQ}$ = 1.02 mW
- Total DC power consumed = 133.042 mW

B. *Power consumption with pulsed mode of operation*

We used pulses of 50% duty cycle. A less amount of duty cycle than this would have saved more power but bandwidth requirement of the buffer limits from reducing it beyond 50%.

- Power dissipated in switch per cycle = (1/2) $V_{CC}I_{CQ}$ =0.4125 mW
- Power dissipated in PMC per cycle = (1/2) $V_{CC}I_{CQ}$ =1.249 mW
- Power dissipated in Buffer per cycle = (1/2) $V_{CC}I_{CQ}$ = 64.350 mW
- Power dissipated in MSP430 = $V_{CC}I_{CQ}$ = $AV_{CC}I_{CQ}$ = 1.02 mW (1/2 factor does not come here because the microcontroller dc current is always present)
- Total DC power consumed = 67.03 mW

Power Saved (per cycle): (133.04 – 67.03) mW = 66.01 mW
Percentage Power saved (per cycle): 49.6%

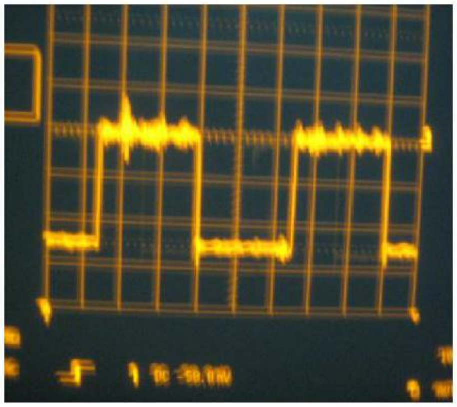

Fig.7: Digital Storage Oscilloscope showing the output of the sensor when fishplate is tampered.

Battery Checking Option: There is a separate subroutine written to monitor the battery voltage, in case it drops or the battery becomes invalid the MCU will send another signal to the nearest cabin. This subroutine is based on a direct comparison between the battery voltage and a reference voltage of 2 volt.

6. OVERALL COST ESTIMATION

We used several hardware and software components to give our design a real face. Some of the software (all during free trial version) we used to finally complete our design are:

1. EAGLE.
2. IAR Embedded Workbench.
3. Smart RF Studio.
4. TINA.
5. MATLAB.

The hardware components we used are shown in Table.1 below:

Serial number	Name of the Component	Cost per Component	Quantity	Total Cost (in$)
1	**Switch**	**$ 0.55/1ku**	1 pc	negligible

2	**Power Management Chip**	**$ 2.9/1ku**	1 pc	negligible
3	**Buffer**	**$ 0.55/1ku**	1pc	negligible
4	**MSP430 FG4618**	**$ 10.77**	2 pcs	$21.54
5	**CC2500 transmitter module**	**$ 1.5**	2 pcs	$3
6	**Flex Sensor**	**$ 5**	1 pc	$5

Approximate total cost of the project = $29.54

Table.1: Estimation of total cost

Whereas, cost of fibre optic cable per foot is about $35 [14]. So to set up the security system with fibre optic cable, expenses will be much higher compared to our proposed scheme as the former will demand for miles of cable to communicate with a distant railway cabin.

7. CONCLUSION

A railway security system through detection of fishplate tampering using wireles sensor network has been reported. The system uses sensitive piezoresistive pressure sensors which produces stable, reproducible changes when the fishplates are tampered. It has also been observed that by using pulsed bias of operation instead of continuous power supply, we are able to save around 50% of power consumption needed for processing the signal throughout the entire transmitting circuitry. The present system also avoids false signals due low battery voltage. The sensor strips are so flexible that they can be mounted such that they are almost invisible to the user. Further the use of low power miniaturized SMT chips will enable the packaging system to be compact and robust to safeguard it from natural calamity.

8. ACKNOWLEDGMENT

We would like to mention the name of Prof. D.V. Gadre who took a seminar at IIT Chennai organized by TI. His seminar played an important role regarding completing our PCB design. Last but not the least our entire ETC Department encouraged us and helped at proper time without which the successful completion of our project would have never been possible.

9. REFERENCES

[1]. Abhijeet Kshirsagar, B.R.Sujoy Kurup, S.Akshay Singan, E.James Jebaseelan Samuel:"Optical Fibre Enabled Track Security System." Swasti, VIT Newsletter, Issue March'05.

[2] Mr. Thomas P. Smithberger, David C.Kelly, Alfred E.Shaw:"Railroad Track Structure System Design." http://www.trb.org/publications/millennium/00095.pdf

[3] Railway Signaling using Wireless Sensor Networks**:** http://railprofessionals.net/blog/?p=244

[4]. United States Department of Transportation Federal Railroad Administration FinalReport'08. available: http://www.fra.dot.gov/Public affairs/final_reort_May_2008

[5] Anuroop Gaddam, Subhas Chandra Mukhopadhyay, and Gourab Sen Gupta*,* "Elder Care Based on Cognitive Sensor Network", IEEE SENSORS JOURNAL, VOL. 11, NO. 3, MARCH 2011, pp. 574-581.

[6] A. Lim, "Distributed services for information dissemination in self organizing sensor networks," Journal of Franklin Institute, vol. 338 no. 6, pp. 707-727, Sep. 2001.

[7]. Flex Sensor: http://devices.sapp.org/component/flex

[8] MSP430 details available**:** http://www.ti.com/MSP430

[9] Chipcon Transceiver details: www.ti.com/swrs040c.pdf

[10] Switch details: scds113d.pdf

[11] PMC details: slvs916.pdf

[12] Buffer details: sbos266e.pdf

[13] MSP430 interface to CC2500/1100: http://www.ti.com/slaa325a.pdf & slaa325a.zip

[14] Cost of fiber optic cable: http://www.isp-planet.com/business/fiber_price_bol.html

10. APPENDIX

10.1 Photo Gallery:

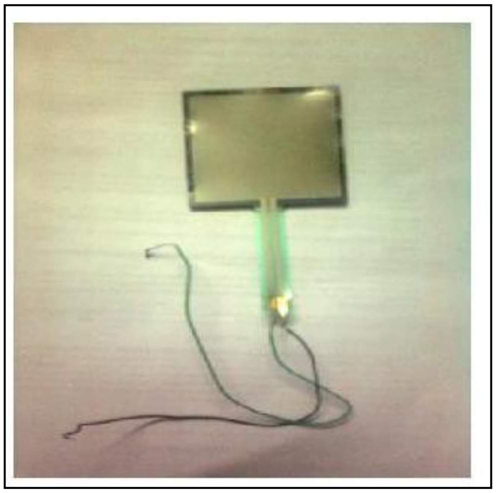

PHOTO 1: Piezo-resistive sensor
PHOTO 2: Chipcon Transceiver Module, CC2500 (at bottom) along with its antenna (at top)
PHOTO 3: Our self-made printed Circuit Board which generates the input signal to the MCU
PHOTO.4: The entire system with transmitter at left and distant receiver at right.