International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

An Effective Scheme to Detect and Prevent Tampering on the Physical Layer of WSN

Mbeng Atemson Enow*

College Of Computer Science and Technology, Shanghai University of Electrical Powers, Shanghai, China
Email: mbengatemson@yahoo.com

Abstract

This experiment "Using a Pressure (smart) wireless sensor to Detect and Prevent Tampering on the Physical Layer of WSN", has as main purpose to show how smart sensors especially pressure sensors can be used to detect attacks on the physical layer of wireless sensors network. This is to prevent tampering and possible intrusion on the physical layer. We build a device to mimic a smart meter or a wireless sensor device and to it we add a pressure sensor and an Arduino motherboard to interpret and execute instructions. The information or readings collected from the sensor will indicate if the device has been tampered or not. (This can be observed from a change in pressure state from high to low). This change in pressure level from high to low will indicate the level and degree to which the smart wireless device has been tampered. We can therefore conveniently conclude depending on pressure level that the use of smart pressure sensors can effectively detect tampering in the physical layer of WSN.

Keywords: Tampering; FSR; Physical Layer; WSN; Arduino; Security; Attacks and Detection; PCA.

1. Introduction

Wireless sensor networks form an infrastructure-less wireless network where nodes are independent and self-organizing.

---

* Corresponding author.

Such networks provide an emerging technology that helps solves both environmental and social challenges through monitoring and data collection related to the applications which uses them (the advantage being that their network can be set without infrastructure, ideal for the non-reachable places such as across the sea, mountains, rural areas or deep forests and flexible if there is ad-hoc situation when additional workstation is required. Implementation cost is cheap [10]. In recent years WSNs have become widely used in almost all devices which contain smart sensors to make life easy for users. The development of WSNs was motivated mostly by military applications such as battlefield surveillance, but today they have various uses such as: Industrial process and monitoring, Machine monitoring, monitoring the environment, Health-care, Home automation, Traffic control etc. Unfortunately it is important to note that this devices or WSNs are susceptible to all kind of attacks and security is a great concern same like classical networks, WSNs if not secured they can be attacked and the whole system compromised [10]. Some disadvantages of WSNs are:

- Less secure because hackers can enter the access point and get all the information, lower speed compared to a wired networks.
- More complex to configure than wired networks.
- Easily affected by surroundings. These attacks can either be outside attacks (passive eavesdropping, DoS attacks) or inside attacks (physical layer attack, DoS etc).

This paper is structured as follows. In section 2, we discuss some recent works and research in this field. In section 3 we describe the system models; we further introduce some requirements and materials. In section 4 we give experimental results and analyses.

2. Recent Works

One of the solutions for physical layer tampering as earlier discussed include using magnetometer sensors (to detect powerful magnetic fields which affect meter readings in current transformer-based electricity meters), tilt sensors which detect removal or physical tampering of meters from authorized locations[1], usage of tampering algorithms as part of firmware that helps ensure billing is continued, and anti-tamper switches that can be placed on the casing of the meter to trigger a tamper when the casing is opened.

There are many works on security of WSNs physical layer which all try to solve security issues in WSNs especially that of physical layer, the following are recent works by some researchers;

Reference [11], 2015 in his paper described that the emergence of smart meters has both created additional opportunities for theft as well as enabled a broader set of sophisticated tamper-detection mechanisms. Specialized energy-metering system-on-chip (SoC) devices such as the Analog Devices ADE7763, Maxim Integrated 71M654xT, and STMicroelectronics STPM01/10 integrate energy measurement and metrology functionality with additional capabilities on a single chip. Using these devices, engineers can create sophisticated metering designs with few additional components. Without special precautions, however, these sophisticated smart-meter designs are no less inherently susceptible to tampering than their earlier mechanical counterparts. As with their earlier mechanical counterparts, however, smart meters still depend on external

sensors for measuring energy usage. Current-transformer (CT) sensors in particular typically used in metering applications present a point of vulnerability to attacks using strong magnets. Placed near the current sensor, the external magnet introduces measurement errors by saturating the core of the CT device or otherwise distorting its output. Meter designers can mitigate this type of tampering by using magnetic shields or additional sensors to detect the presence of a strong external magnetic field. Alternatively, engineers can turn to less susceptible sensors based on shunt resistors or Rogowski coils such as the Pulse Electronics PA32XXNL series. Although the specific choice between these alternatives depends on metering requirements, both sensor types are immune to magnetic fields and so offer an attractive approach for mitigating this type of tampering.

Ben Smith [12], 2014 paper proposed ways of preventing physical layer attacks by tampering. He illustrated that at a minimum, devices that purport to be secure should be *tamper resistant*. That is, the designer and manufacturer of the device should take at least minimal steps to deter the curious and the casual hacker. These steps include virtual barricades in the hardware, including using nonstandard fasteners, plastic or metal welds in construction, or glue in assembly. This means, of course, that servicing the device can also become more complicated, but remember that the focus here is on security.

But ultimately it does not matter how difficult you make it to pry open a product. A determined opponent will find a way in. When that happens, there are four possible responses to a tamper attack, all directly related to the value of a secure device and its protected data.

- Destroy the device.

This may be the best and most straightforward option, particularly if the device is inexpensive but the data it contains has great value. For example, if a credit card terminal detects that its case is being opened, it may rapidly destroy any secret information inside, including the cryptographic keys that decrypt its operating software. Then, when next turned on, it will not be able to function because its encrypted code store is useless without access to the keys required to decrypt it. Any device that destroys its own ability to function when it senses a tamper event is about as close to being *tamper proof* as it can be.

To “repair” the damage, one must replace the device, but presumably at a relatively modest cost compared to the recovery cost if sensitive material had been lost.

- Send a notification.

If a device is connected to a network, a message is launched to a supervisory computer on the network at the first sign of a security breach. The supervisory computer then notes the device’s identity and removes it from the list of active devices. This kind of device is called *tamper evident*: it cannot prevent a tamper event, but it can certainly make a network manager aware of the tampering.

- Activate a physical indicator.

If a device requires physical interaction with a person to do its job, an automatic indicator can alert the user that

the device is no longer trustworthy. For example, there are tamper-evident seals on medical supplies that provide inexpensive but effective security. If broken, they alert the user (i.e. the medical professional) that the device's integrity has been compromised and that it should be discarded.

- Do nothing.

It may seem strange sometimes to allow outsiders access to our secret information. In fact, in the right circumstances not everything has to be locked down tightly. If device's value is low and if the consequences of losing control of its data are minimal, the simplest reaction may simply be to do nothing. Absent a financial incentive to tamper, attacks against low-value targets often stem from curiosity or accidental damage, and do not warrant recording or action.

Reference [13], in his article review he proposed Tamper-proofing the node's physical package as one of the defenses to this attack.

Jeff McCullough [14], in his paper proposed the following: - Detection techniques internal to the revenue meter itself, such as the outage or blink count, have limitations. Blink counts infer theft by detecting that a meter has been de-energized more often than its neighboring meters, thereby implying that the customer has removed the meter to tamper with it or to install jumpers around the meter base. A limitation of blink counts is that they cannot detect a common theft technique involving live tapping of the customer service drop wires ahead of the meter.

Remote detection and measurement of electricity theft is one of the challenges that inspired Elster to develop transformer meters such as the Elster Low Voltage (LV) transformer AGInode™ device. The LV AGInode device is designed for secondary outputs of pole- and pad- mounted distribution transformers.

These types of devices have been especially effective in detecting theft associated with marijuana-growing operations in residential Premises. For some electric utilities, such operations Account for 99 percent of electricity theft. This more definitive theft detection technique uses such devices as the AGInode to measure the full energy output of a distribution transformer and then compare that metric to the sum of the energy consumption registered in the meters supplied from that transformer.

After factoring in secondary distribution line losses and any unmetered loads, such as streetlights, the full output of the transformer should roughly equal the consumption of customer meters. Missing energy is direct proof that one or more customers are stealing. With transformer meters and energy inventorying, theft can be positively identified and isolated down to the distribution transformer serving the offending customer. Regardless of how the theft is attempted — meter tampering, meter inverting, jumpers around the meter, tapping in ahead of the meter — transformer measuring will detect the missing energy that represents theft.

By comparing location data with other incidental evidence such as blink counts or unusual consumption patterns, the utility can easily narrow down the list of accounts to be investigated before sending a technician into the field.

Table 1: Comparison in-terms of time, cost and implementation between other methods and our proposed method

	Time consuming	Cost effective	Ease to implement
Nonstandard fasteners plastic or metal welds	slow	expensive	complicated
Tamper proofing the nodes	fast	expensive	easy
Using magnetic shields and sensors	fast	expensive	Not easy
Installed jumpers around the meter base and blink counts	fast	expensive	Not easy
Using force resistant sensors	Real time	Relatively cheap	Relatively easy

Comparing the different solutions from other researchers to secure physical layer we noted more needs to be done, it is for this reasons we decided to propose another method, easy and cost effective to secure WSN physical layer from tampering attacks. Based on this we decided to carry out an experiment that would prove that we can also use pressure sensors to detect tampering in WSN devices such as smart meters and other appliances etc. The said experiment is based on ways to secure the smart meter from attacks such as tampering which is one of the most basic attacks on WSN's physical layer. Theoretically the solution consists of integrating smart sensors to monitor the state of the physical layer, this sounds easy, and our task consists of introducing a smart wireless sensor to these devices. Many researches on ways to prevent attacks on the physical layer of WSN by tampering mechanism are ongoing. Our first experiment is building a prototype for implementing security measures to keep the physical layer more secure. The experiment consists of linking devices such as: Bluetooth, pressure sensor, Arduino motherboard, LED (light emission diode), adapter, capacitor etc.

3. System Models, Requirements and Design Goals

3.1. Simple Circuitry (Architecture)

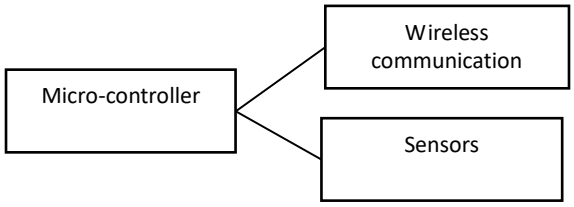

Figure 1: architecture (circuit Model)

Devices such as sensors, and wireless communication channels such as Bluetooth devices are connected to a smart processor whose main objective is to process and collect information it receives from the sensors and other nodes in real time, and to send this information to a base station or command station.

3.2. Components and Materials Needed for the Experiment (Basic Requirements)

Firstly, we started the experiment by obtaining and gathering materials we need to achieve the expected results. The following devices are primordial for this experiment:

- Arduino: It is a micro-controller use for building digital devices and interactive objects that can sense and control objects in the physical world [8, 9]. One of its main advantage is that it is very easy to use and setup, designed to make applications, interactive controls or environment and easily adaptive. The hardware consists of a board designed around an 8-bit micro-controller, or a 32-bit ARM.
- Force Sensitive Resistor: A resistor that changes with time. Even though there are various types of force sensors, the force sensing resistors are having several advantages such as thin size (less than 0.5mm), very low cost and are also good shock resistance. The only disadvantage of FSR sensors is low precision, there will be approximately 10% or more difference in measurement results [15].
- Bluetooth HC-05/HC-06: Is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs) [16].
- Breadboard: A breadboard is construction base for prototyping electronics circuiting. 7.5KOhm&221KOhm Resistors: A resistor is a passive two terminal electrical components that implements electrical resistance as a circuit element [7].

- LED: A light diode which is used to give an indication.
- Android device or system: An android device is needed such as a cell phone or tablets etc. a Bluetooth application or software is downloaded from the phone store and later install on the android phone, this will help facilitate communication between the micro-controller and the FSR.

3.3. Methods, Circuits and Connections (Bluetooth Circuitry)

Our method to solve tempering (mostly on the physical layer) in WSN devices consist of introducing a FSR to the physical layer of WSN, this FSR is a sensor which is sensitive to a very minute change in pressure or force hence making it a suitable choice for this experiment. Added to this is a micro-controller specifically Arduino and these components are interconnected to one another.

The circuit connection was a simple one; we first established communication channels between the Bluetooth and the Arduino motherboard; we then linked our android device to the Arduino motherboard with the help of the Bluetooth connection. The specific pin combination is summarized in the Table 2 below.

Table 2: Showing Pin connection between Arduino and Bluetooth device

Arduino Pins	Bluetooth Pins
RX (Pin 0)	TX
X (Pin 1)	T RX
5V	VCC
GND	GND

Connect a LED negative to GND of Arduino and positive to pin 13 with a resistance valued between 220Ω – 1KΩ. And you're done with the circuit Bluetooth Pins.

The devices are interconnected one to another in a simple circuit. Then codes for both the Bluetooth and FSR are uploaded to the Arduino motherboard.

4. Results and Analysis

The results for this experiment was to verify if sensors (pressure/force) could be used to protect the physical layer against attacks such as tampering which are mostly physical and very difficult to detect, HC 05/06 works on serial communication. Here the android application is designed sending serial data to the Bluetooth module when Pressure is exerted on the Force sensitive resistor when it is pressed. The Bluetooth module at other end receives the data and send to Arduino through the TX pin of Bluetooth module (RX pin of Arduino). The Code fed to Arduino checks the received data and compares. If received data is 0 or less than 100 the LED turns OFF.

The experiment proved that a force sensor can detect tempering on physical layer of WSN devices due to the change in force or pressure difference on the FSR, we conducted further experiments and built a prototype device in which we inserted a Force sensitive sensor (pressure sensor) on its lid. A change of pressure from 0 to a higher value helps us know if at a given point the device has been tampered. A high pressure indicates the device has not been tempered while a low pressure indicates the device has been tempered. Hence meaning this technique can be effectively used to bring some level of security to the physical layer by acting as a warning whenever an intruder tries to get into a smart meter physically.

NOTE: The pressure exerted on the Force sensitive sensor when the lid is closed and when it is open is different. As such tempering on the physical layer of the WSN can easily be detected.

The FSR changes its resistance with force. It ranges from near infinite when not being touched, to under 300ohms when pressed hard. So, we can measure that change using one of the Arduino analog inputs. But to do that we need a fixed resistor that we can use for the comparison (We are using a 10K resistor). This is called a voltage divider and divides the 5v between the FSR and the resistor. The analog read on your Arduino is basically a voltage meter. At 5V (its max) it will read 1023, and at 0v it will read 0. So, we can measure how much voltage is on the FSR using the analog Read and we will have our force reading. The reading from the

FSR will help us know if there was intrusion or tampering on the physical layer.

4.1. Data Analysis (Detail Analysis)

We use **PCA** (Principal Component Analysis) to analyze how long it takes in terms of time for the force to change from a high value which means secure to a low value which means tampered, in this analysis we estimated that it takes a total of 0.00001micro seconds to change from one pressure value to another. A portion of the data analysis is as follows:

In Table 3 below we considered three forces F1, F2, F3 with random values representing the forces exerted at a given constant time T.

Table 3: sample data (random Pressure values) for PCA analysis

F1	F2	F3	Time(T)
0	20	1000	0.00001
300	5000	4	0.00001
10	600	1	0.00001
50	0	90	0.00001
1000	0	0	0.00001
100	5	2000	0.00001
500	1	50	0.00001
100	0	10	0.00001
50	100	800	0.00001
0	600	0	0.00001
20	1	500	0.00001

4.2. Summary Statistics(Supplementary Observations)

Table 4: detail summary

Variable	Observation	Obs. With missing data	Obs. Without missing data	Minimum	Maximum	Mean	Std. deviation
F1	10	0	10	0.000	1000.000	208.000	321.517
F2	10	0	10	0.000	5000.000	622.700	1557.879
F3	10	0	10	0.000	2000.000	365.500	660.371

Table 5: Supplementary observations

Variable	Observation	Obs. With missing data	Obs. Without missing data	Minimum	Maximum	Mean	Std. deviation
F1	1	0	1	50.000	50.000	50.000	
F2	1	0	1	100.000	100.000	100.000	
F3	1	0	1	800.000	800.000	800.000	

Table 6: correlation matrix (Pearson (n))

Variable	F1	F2	F3
F1	**1**	0.047	-0.271
F2	0.047	**1**	-0.240
F3	-0.271	-0.240	**1**

4.3. Principal Component Analysis (PCA)

4.3.1. Eigen values

Table 7: Eigen values

	F1	F2	F3
Eigen value	1.387	0.953	0.660
Variability (%)	46.219	31.779	22.002
Cumulative (%)	46.219	77.998	100.000

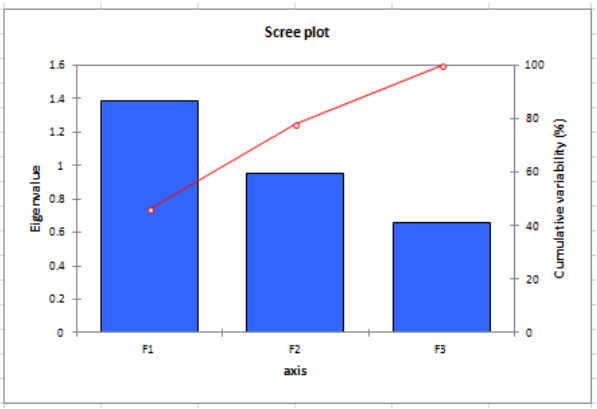

Figure 2: Eigen value / cumulative variable

4.3.2 *Eigenvectors*

Table 8: Eigenvectors

	F1	F2	F3
F1	-0.540	-0.661	0.521
F2	-0.491	0.750	0.444
F3	0.684	0.016	0.729

Table 9: factor loading

	F1	F2	F3
F1	-0.636	-0.646	0.423
F2	-0.578	0.732	0.360
F3	0.805	0.016	0.593

Table 10: correlation between variables and factors

	F1	F2	F3
F1	-0.636	-0.646	0.423
F2	-0.578	0.732	0.360
F3	0.805	0.016	0.593

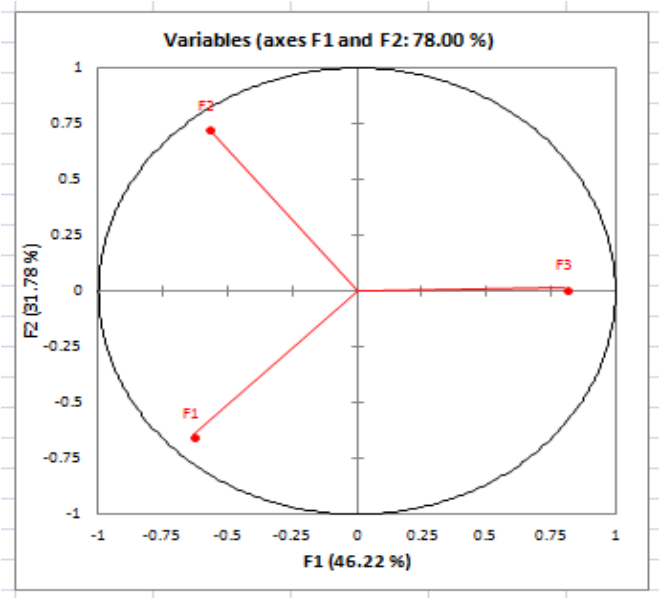

Figure 3: F1 / F2 variables

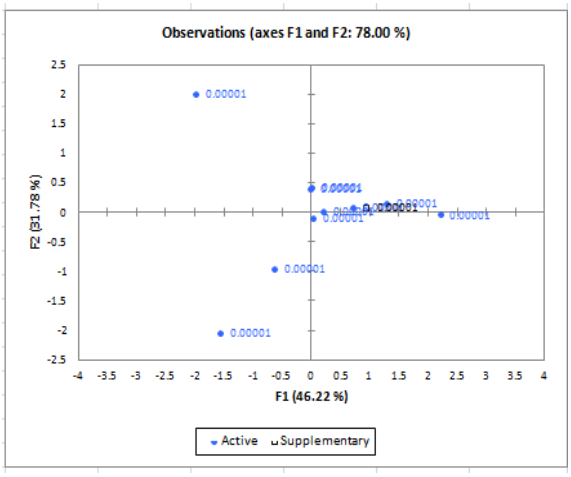

Figure 4: F1 / F2 observations

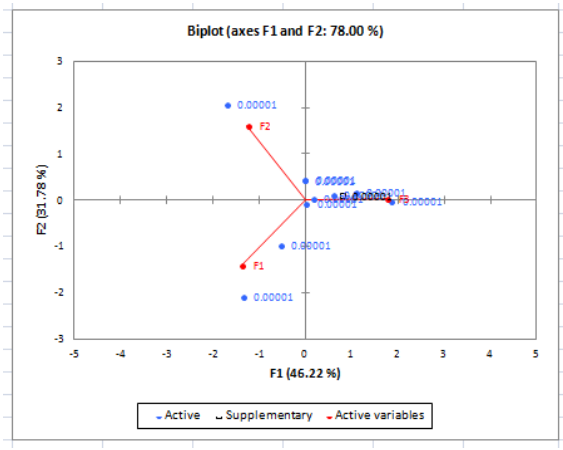

Figure 5: F1 / F2 Biplot

Table 11: Contribution of the observations (%)

	F1	F2	F3
0.00001	11.467	0.274	0.622
0.00001	29.166	42.476	16.701
0.00001	0.012	1.749	8.966
0.00001	0.248	0.004	9.157
0.00001	18.320	43.760	8.300
0.00001	34.297	0.014	35.605
0.00001	3.092	9.601	0.046
0.00001	0.001	0.087	9.340
0.00001	0.004	1.939	9.396
0.00001	3.394	0.096	1.867

Table 12: squared cosines of the observation

	F1	F2	F3
0.00001	**0.959**	0.016	0.025
0.00001	0.440	**0.440**	0.120
0.00001	0.002	0.219	**0.779**
0.00001	0.054	0.001	**0.946**
0.00001	0.350	**0.575**	0.075
0.00001	**0.669**	0.000	0.331
0.00001	0.318	**0.679**	0.002
0.00001	0.000	0.013	**0.987**
0.00001	0.001	0.229	**0.770**
0.00001	**0.780**	0.015	0.204
0.00001	**0.984**	0.009	0.007

The results corresponding to the supplementary observations are displayed in the second part of the table. Values in bold correspond for each observation to the factor for which the squared cosine is the largest. The bold values mean the pressure is high; hence the device has not been tampered.

5. Conclusion

In this study of detecting and preventing tampering attacks on physical layer of Wireless Sensor Networks, we have contributed by proposing another method to prevent and detect tampering attacks on WSN devices. We compare other methods to our method in table1 and we discuss already existing solutions to this problem. There are many other methods or ways to detect and prevent tampering in WSN's physical layer for example, Using magnetic shields and sensors to detect powerful magnetic fields which affect meter readings, Nonstandard fasteners plastic or metal welds in construction, or glue in assembly, Tamper proofing the nodes, Install jumpers around the meter base and outage or blink counts, we proposed the use of force resistant sensors to secure physical layer from tampering attacks. Some advantages over existing methods are: tampering attacks are detected in real time; it is cheap, reliable and very easy to implement. In the course of our research we discovered that our method is not only cost effective but also can conveniently detect tampering or intrusions on WSN physical layer.

6. Recommendations

For future test and experiments we intend to increase the communication range of the WSN devices. We can note that the Bluetooth device linking the wireless devices for communication has a limited range.

Acknowledgments

I want thank my supervisor Wen Mi (Phd) for always setting me in the right direction, New Era Technology for providing conditions necessary for effective laboratory work and Experiments and to all those who helped me to achieve my set goals and objectives.

References

[1] Steven Berber and Nuo Chen. "Physical layer design in wireless sensor networks for fading mitigation", 2013.

[2] Dr.Shahiriar .M. And Hossein jadidoleslamy. "A comparison of physical attacks on wireless sensor networks". Vol.2.No.2, 2011.

[3] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", IEEE, 2010..

[4] Anitha S.Sastry, Shazia Sulthana and Dr. S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", International Journal of Advanced Networking and Applications", Vol.04 Issue 04, pp. 1657-1661, 2013.

[5] Yansha Deng. "Physical layer security in three-tier wireless sensor networks: a stochastic geometry approach".

[6] Jonathan Oxer, Hugh Blemings. "Practical Arduino: Cool Projects for open Source Hardware".

[7] Ladyada, "Force Sensitive Resistor", 2013.

[8] John Boxall. Arduino workshop "A hand-on introduction with 65 projects"

[9] Massimo Banzzi. Getting started with arduino. 2nd edition

[10] Debnath B, Tai-hoon and Subhajit Pal. "A comparative study of wireless sensor networks and their Routing Protocols". sensor 2010,10,10506-10523;doi:10.3390/s101210506.

[11] Stephen Evanczuk. 2015. "Employing Tamper Detection and Protection in Smart meters".

[12] Ben Smith. "Fundamentals of Electronics Security: Tampering with the easy the target". 2014, APP 5937.

[13] Murat Dener. 2014. "Security analysis in wireless sensor networks". Vol 2014, article ID 303501.

[14] [14] Jeff McCullough. "Deterrent and detection of smart grid meter tampering and theft of electricity, water, or gas".

[15] Adam Meyer. "Force Sensitive Resistor + Arduino".

[16] Alasdair Allan. 2011. "iOS Sensor Apps with Arduino".