International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 9, September 2016)

Secure Data Aggregation in Farming Application Using Wireless Sensor Networks

Shivaraj
Department of Telecommunication Engineering
Dayananda Sagar College of engineering,
Bangalore, India,
ssajjan10@gmail.com

H. C. Srinivasaiah
Department of Telecommunication Engineering
Dayananda Sagar College of engineering,
Bangalore, India,
hcsrinivas@gmail.com

***Abstract*— This paper deals with development of a Java applet for Data-Aggregation (DA) in farmland through simulation of Wireless Sensor Network (WSN). This applet is developed on Java/eclipse platform. It provides simple user interface in the form of Graphical-User-Interface (GUI) for DA in WSN and its analysis in the farmland application. The implementation has 4 modules namely: Service-Provider (SP), Router, Base-Station, and Intrusion-Detection-System (IDS) manager. The end sensor nodes (SNs) senses the farmland soil attributes such as: temperature, pH-value, pressure, humidity and wind velocity, in accordance with this implementation, whose values are aggregated securely and communicated to the end user using the above modules. In this process, energy and delay parameter while packet transmission are very important for the lifespan of the SNs. The maximum and minimum simulated network transmission delays are 109.38 µs and 15.63 µs, respectively. The simulated maximum and minimum energies consumed during this transmission are 17.5 milli-Joules and 1.04 mili-Joules, respectively.**

Key Word: **Data aggregation, Service provider, Router, Intrusion detection system manager, and Base station.**

I. Introduction

Wireless networking is a method by which homes networks, telecommunication networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunication networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. A wireless sensor network is a spatially distributed autonomous sensor to monitor physical or environmental conditions, such as temperature pressure, sound etc., and to cooperatively pass their data through the network to a main location. The WSN [1] is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting device. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust. The cost of sensor node similarly varies, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communication bandwidth. A WSN typically consists of a sink node sometimes referred to as a Base Station (BS) and a number of small wireless sensor nodes. The base station is assumed to be secure with unlimited available energy while the sensor nodes are assumed to be unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensor information. Sensor information is communicated to the Base Station through various means of transmission media. To conserve energy this information is aggregated at intermediate sensor nodes by applying a suitable aggregation function on the received data.

Data aggregation [2,3,4,5,6] is any process in which information is gathered and expressed in a summary form, for purposes of statistical analysis. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes.

The outline of this paper is as follows. In the section 2, an overview of the WSN is presented in the context of the secure DA in the farmland application. Section 3 provides an overview of the implementation of this application software in Java/Eclipse platform [7]. The section 4 provides the prototype simulation results of secure DA in farming application using WSN. The conclusion based on the implementation and the simulation results are drawn in section 5 of this paper.

II. Proposed Block Diagram

The wireless sensors (labelled as s1-s28, 28 in number) are assigned to read specific attributes namely temperature, pH-value, pressure, humidity, and wind velocity. These sensors collect the data and send them to the SP, and then the SP sends the same data to the BS through the Router. During the information being sent it is also checked by the IDS [8] manager to provide the security to the system. Later once it is received to the BS, the end user can access the information. During the sending of the information from sensors to SP, in-Network aggregation [1,9] method is followed [2]. Various objects involved in the implementation are shown in Figure 1, whose descriptions are given subsequently.

2.1 Service Provider

In this module of this (Java) applet, the SP [9,10,11] activates all the sensors and assigns temperature, humidity, pH level, pressure and wind-velocity to the SN objects, and their backup will be stored, and uploaded to the particular BS. Meanwhile the data is extracted by the IDS manager for the security purposes.

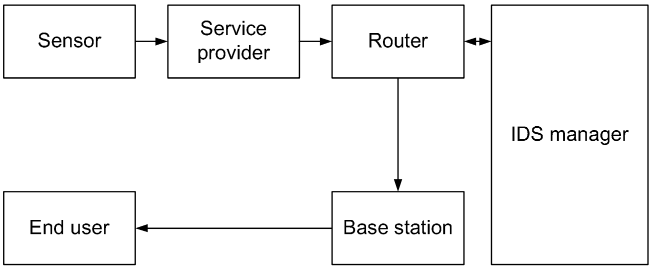


Figure 1: Proposed block diagram of the secured DA application

Temperature

A temperature is a comparative measure of hot or cold. Here the temperature is been assigned from sensor node s1 to s5. The range is between 25^{o}C to 30^{o}C assigned to these SNs during the simulation using the developed Java applet.

pH level of soil

The pH stands for potential of hydrogen, which is a measurement of the hydrogen ion concentration in the soil of the farmland in this application. The total pH scale ranges from 1 to 14, with 7 considered to be neutral. A pH less than 7 is said to be acidic and solutions with a pH greater than 7 are basic or alkaline. The optimal pH range for most plants is between 5.5 and 7.0. In the work of this paper the SN-devices s6 to s10 as pH sensors.

Pressure

A pressure sensor measures pressure as force per unit area (Newton/Square meter), typically of gases or liquids. This device is used to measure the pressure of environment, of farmland. The pressure voltage signal acquired by the pressure sensor in farmland environment is amplified and then changed into digital signal representation by Analog-to-Digital-Converter (ADC). Finally, the digital pressure data is manipulated and analyzed by Supply-Chain-Management (SCM) program is sent to a computer through serial port. In this way the system can detect and monitor pressure parameter of agriculture environment in real time. The SNs - s11 to s15 are pressure sensors.

Humidity

Humidity is the amount of water vapour (in percent) in the air. The water vapour is the gaseous state of water and is invisible. Humidity indicates the likelihood of precipitation of dew or fog. The water is taken in by the roots and evaporated through the leaves into the air. This process cools the plant. The relative humidity in the air can affect the flow of water through the plant. The higher the relative humidity, the more slowly transpiration occurs. The SNs s16 to s20 are humidity sensors as per this work.

Wind velocity

Wind flow velocity is fundamental atmospheric quantity. Wind speed is caused by air moving from high pressure to low pressure, usually changes due to change in temperature. Its unit is meter per second (or hour). The SNs s21 to s28 are used as wind sensors.

Router

In this module, the predicate count query is used to determine the total number of nodes whose sensor readings have some property in the network. And it is responsible for delivering the sensor readings to the BS. Before sending any file to receiver, the data will be verified and then sent to particular BS. In a router we can view the sensor details and the corresponding sensory data and clear it, if required.

IDS Manager

The IDS Manager is responsible to identify the intrusion in the network. Basically it has two types (sets) of data, one set of data taken from service provider and the other set of data from the router. If the data is not matched, it sends an acknowledgement that so and so data from the respective sensor is not matched and the same will be retrieved again from the corresponding sensor. Then the IDS Manager is responsible for capturing the fake data and the respective attacker. The IDS Manager will make an attacker list and then all attackers are stored with tags such as, attacker name, attacked node, and modified sensor data details of a SN, attacker IP address, time and date.

Base Station

The BS module collects all sensor data from the nodes: s1, s2, s3, etc., and computes aggregation results. The in-network-aggregation allows sensor readings to be aggregated by intermediate nodes, which efficiently reduces the communication overhead. The BS used for checking the status and to verify the results through reliable random sampling is achieved by data communication and interactive proofs.

In-network aggregation

In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption, in particular energy thereby increasing network lifetime. There are two approaches for in-network aggregation:

a. With size reduction
b. Without size reduction.

1) With size reduction

In-network aggregation with size reduction refers to the process of combining and compressing the data packets received by a node from its neighbors in order to reduce the packet length to be transmitted.

2) Without size reduction

In-network aggregation, ‘without size reduction’ refers to the process of merging the data packets received from different neighbors into a single data packet but without processing this data for compression.

III. IMPLEMENTATION

The implementation procedure includes the following steps to realize the 4 modules built into the applet. They are:

Service Provider

The SP module activates all the sensors and assigns a range of values of data, randomly to the sensor node, and backup will be stored. It uploads their data to the particular BS. The SP can view the attacked file by the IDS manager. It can replace the injected fake temperature to the SN.

Router

The router module predicate count query is used to determine the total number of nodes whose sensor readings have some property in the network. And it is responsible for delivering the sensor readings to the BS. If it is founds fake readings then it transfer the flow to IDS Manager. Before sending any file to receiver temperature will be verified, then send to particular BS. In a router we can view the sensor temperature details and clear this detail.

IDS Manager

The IDS manager module is responsible to identify the intrusion in the network. If the router finds fake temperature readings, then it transfers the flow to IDS Manager. Then the IDS Manager is responsible for capturing the attackers. The IDS Manager will make an attacker list and then all attackers are stored with tags such as: attacker name, attacked node, and modified temperature of SN, attacker IP address, and time and date.

Base Station

The BS collects the data from all sensor nodes: s1, s2, s3, etc., and computes aggregation results at the BS. In-Network aggregation allows sensor readings to be aggregated by intermediate nodes, which efficiently reduces the communication overhead. The BS is used for checking the temperature status and to verify the results through reliable random sampling achieved by data communication and interactive proofs with the BS.

IV. Results

A prototype of the applet for secure DA in farming application is implemented as a software model of the farmland WSN, using Java/Eclipse platform. Various (virtual) objects such as SNs, SP, routing device, IDS manager, and BS (modules) are created by coding. The communication between various objects is accomplished through their ports. For the simulating the sensor attributes, the built-in Java label function, class, object, etc., features are used.

1) Simulation of Service Provider

The below screen in Figure 2 is snapshot of SP which helps to give command such as ‘Read temp’, ‘view backup’, ‘send’ and ‘clear data’. Basically all the sensors are inactive which is shown in black color. Once the “Read temp” command is clicked, each sensor gets activated and turns to green color which shows the sensor is in active state and reads the respective allotted reading. Second command is the “view backup”, by clicking it we can see the newly allotted data to all the sensors. Third command is the “send” command which helps us in sending the data to the BS through routing device. Fourth command is the “clear” command which helps in clearing the previous data.

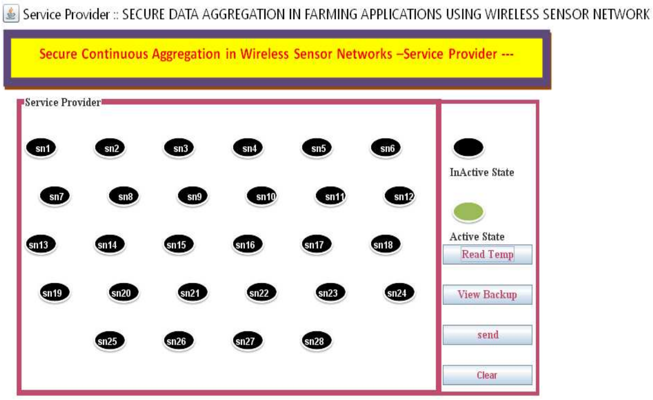

Service Provider :: SECURE DATA AGGREGATION IN FARMING APPLICATIONS USING WIRELESS SENSOR NETWORK
Secure Continuous Aggregation in Wireless Sensor Networks –Service Provider ---
Service Provider
sn1 sn2 sn3 sn4 sn5 sn6
sn7 sn8 sn9 sn10 sn11 sn12
sn13 sn14 sn15 sn16 sn17 sn18
sn19 sn20 sn21 sn22 sn23 sn24
sn25 sn26 sn27 sn28
InActive State
Active State
Read Temp
View Backup
send
Clear

Figure 2: Screenshot of SP

2) Simulation of WSN routing device

The Figure 3 below is the screen shot taken for routing device which is implemented for transferring data from SP to BS. In this section we have two commands viz., ‘view details’ and ‘clear details’. Firstly the ‘view details’ helps us to view the data that has come from the SP by which we can also verify whether arrived data is same as the one sent by the SP or not. Second command helps in clearing the previous data.

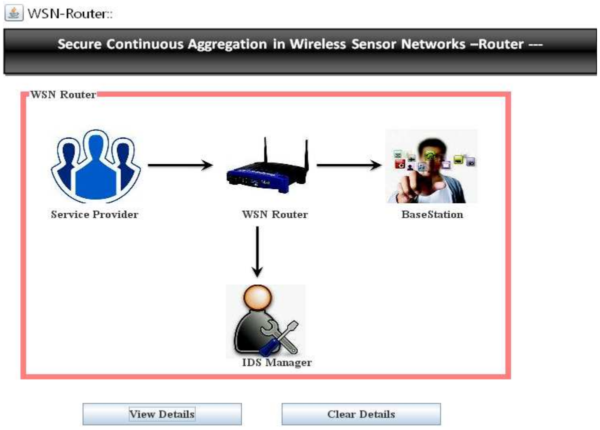
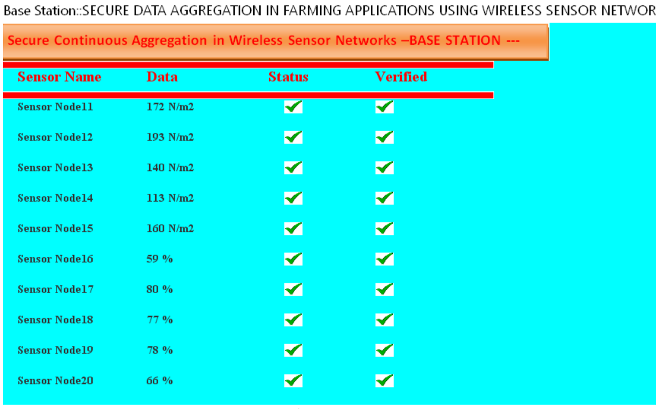


Figure 3: Screenshot of WSN routing device

3) Simulation of Base Station

Figure 4 shows the screenshot of the BS. Here the data being received at the BS as an end user can be viewed. There are four columns viz., ‘Sensor Name’, ‘Data’, ‘Status’, and ‘Verified’. The ‘Sensor Name’ is given from s1 to s28. Second column that is ‘Data’ displays the respective data allotted from the respective sensor. Third column ‘Status’ tells about the status whether the data received from SP to Routing device is same or not; while the “Verified” column tells about the data received from routing device to BS is same or not. Hence there will be two right clicks shown during the execution of the (applet) program. In the screenshot of figure, five sensed attributes namely temperature, pH-level, pressure, humidity, and wind-velocity are shown recorded. As this screenshot displays only ten values at a time of all the sensed values corresponding to 28 sensors, they are also written into a spreadsheet of Table 1 during this simulation for convenience. Table 1 shows the values of the sensor attributes for each of the 5 sensor types. Note that sensed values at the SP and the values in this table are same. The values that are sent to BS are correspondingly equal, verifying the objective of this applet (project) implementation. Also each SN is assigned with a MAC address against it and its sensed attribute value, during the simulation. In conclusion this (applet) provides the implementation of secured DA in farming application using WSN. As this is prototype model, it requires a thorough analysis before adopting this model for a realtime field implementation. This work provides modeling of a realtime farmland scenario, saving enormous cost that would otherwise be incurred due to lack of initial knowledge.


Base Station::SECURE DATA AGGREGATION IN FARMING APPLICATIONS USING WIRELESS SENSOR NETWOR

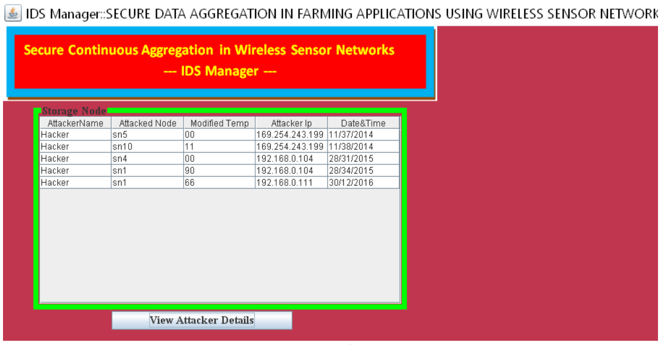
Secure Continuous Aggregation in Wireless Sensor Networks –BASE STATION ---

Sensor Name	Data	Status	Verified
Sensor Node11	172 N/m2	✓	✓
Sensor Node12	193 N/m2	✓	✓
Sensor Node13	140 N/m2	✓	✓
Sensor Node14	113 N/m2	✓	✓
Sensor Node15	160 N/m2	✓	✓
Sensor Node16	59 %	✓	✓
Sensor Node17	80 %	✓	✓
Sensor Node18	77 %	✓	✓
Sensor Node19	78 %	✓	✓
Sensor Node20	66 %	✓	✓

Figure 4: Screenshot of Base station with data shown

4) Imulation of IDS Manager

Figure 5 shows the snapshot of the IDS manager window. The IDS manager gives details about the node whose data being manipulated. In IDS manager there is only one command that is 'View Attacker Details'. It displays the attacker name to the respective node, what data has been changed of that particular node and lastly we can see the date and time of attack. Any data of a SN, if changed by the external interface or by any intruder, details can be seen and further action can be taken in order to provide more security to data at the end user. In an extended scenario, the IDS manager can also detect any active attack on the SN itself from being manipulated, by a proper tracking (which would be a course of future work).


IDS Manager::SECURE DATA AGGREGATION IN FARMING APPLICATIONS USING WIRELESS SENSOR NETWORK

Secure Continuous Aggregation in Wireless Sensor Networks
--- IDS Manager ---

Storage Node

AttackerName	Attacked Node	Modified Temp	Attacker Ip	Date&Time
Hacker	sn5	00	169.254.243.199	11/37/2014
Hacker	sn10	11	169.254.243.199	11/38/2014
Hacker	sn4	00	192.168.0.104	28/31/2015
Hacker	sn1	90	192.168.0.104	28/34/2015
Hacker	sn1	66	192.168.0.111	30/12/2016

Figure 5: Screenshot of IDS manager

Table 1: The complete set of readings for all 28 SNs corresponding to five attributes under consideration (mph –miles per hour).

Service			
Field1	**Data**	**Mac**	**Node**
Temp	26 °C	3f817cdcd8a37623a1bb0399deccf8cc27658428	sn1
	27 °C	-d9bfb34eca74417f7553539b64574e1c377fcd5	sn2
	25 °C	-59d56ffa3de755c1dd6fcb2940b2c35919b04e52	sn3
	25 °C	-59d56ffa3de755c1dd6fcb2940b2c35919b04e52	sn4
	25 °C	-59d56ffa3de755c1dd6fcb2940b2c35919b04e52	sn5
pH	7	-6fd45c325e77c7fea6b491e4bad86f33ac6b7026	sn6
	8	-1a244315a3181d67747396430202176fb5543e1	sn7
	9	ade7c2cf97f75d009975f4d720d1fa6c19f4897	sn8
	9	ade7c2cf97f75d009975f4d720d1fa6c19f4897	sn9
	7	-6fd45c325e77c7fea6b491e4bad86f33ac6b7026	sn10
Pressure	124 N/m2	4b6c87178a477a03fa06f9f116aa2cfd62deb3df	sn11
	184 N/m2	-ef3425bff848bb43fa6f9a3a98848842df22948	sn12
	180 N/m2	23dfd578a6dacbede537935bad97996db97d99cc	sn13
	153 N/m2	-25b12f87849fde4b6dd688afd771917d566f31b1	sn14
	152 N/m2	2e24288c3ffa41609f4da2446c7dc1a1e6e0ca9b	sn15
Humidity	58 %	508a6173812 19d8ceadf36eab95c5079996e57b2	sn16
	68 %	6c485d1715dccd26f06a964a1579bb79d973991c	sn17
	77 %	-51cc7dd590c80152c40146afa9c59e0b624a0342	sn18
	58 %	508a6173812 19d8ceadf36eab95c5079996e57b2	sn19
	67 %	ee4c3a0a7f015458fbe2be94a036456448f58b	sn20
Wind velocity	26 mph	-55ac05a6d29e069b575f34557cbf2cca2356f69b	sn21
	23 mph	-5691a87d2a03ac91e5b2fef1fb05496b67812cc0	sn22
	20 mph	59c204d71852aa33b442afabe871569ff3f18d58	sn23
	24 mph	-5002327953593ba8a53a166fa76bca9ac0dce0ec	sn24
	16 mph	-6e5fa18bb181af7f8712bc317d348425c5693499	sn25
	18 mph	-7d18e3bd5453bfb1de5dae0e22bb808976c40f65	sn26
	25 mph	-5971439f51596456a7b67a35ca9878c82838937d	sn27
	21 mph	798bab45db1fb765867361af9a699efa66e71e2c	sn28

5) *Transmission - delay and energy*

Figure 6 shows the graph of delay (left y-axis) and energy (right y-axis) as function of SN number along x-axis. The delay (microsecond - µs) refers to the transmission time and the energy refers to energy consumed (in milli-Joules – mJ) during the transmission of each message (packet) of sensed attribute data. The amount of the energy consumed and the transmission delay are random depending on the sensed attribute and the network conditions, which is simulated internally by Random-Number (RN) generation. The energy values E1 to E28 corresponds to the SN 1 to 28, respectively. Based on the calculation of the energy consumption for each (message) slot we can have overall idea of how much energy has been consumed from the battery. The maximum energy consumed is 17.5 mJ (for pH-value attribute) and the minimum energy is 1.04 mJ (for pressure attribute), both found by simulation.

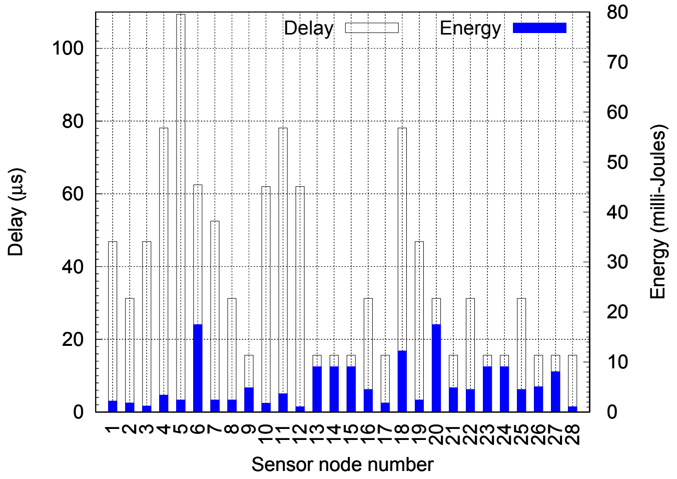


Figure 6: Delay and energy bar graph for the 28 sensor nodes

Energy Calculation: The amount of energy (mJ) consumed by the system is given by the formula:

Energy = (message content/time delay)*1024 bytes, in Joules.

The simulated delay values are T1 to T28 (µs) corresponding to the SN, 1 to 28, respectively as shown in Figure 6. The maximum and minimum network transmission delays are 109.38 µs (for temperature attribute) and 15.63 µs (for pH-value and pressure attributes), respectively both found by simulation.

Time Delay calculation: The time taken by the packet (or message) to transmit data from source - SP to the destination - end user is given by:

Time delay = Start time – End time, in seconds. Note: the delay and energy parameters are tabulated in µs and mJ, respectively for convenience.

V. Conclusion

In the work presented in this paper, a prototype of Java applet is developed to model a WSN for implementing in farmland for secure DA, with an objective of monitoring the soil attributes such as - temperature, pH-value, pressure, humidity, and wind-velocity for an optimum yield. This applet is developed on Java/Eclipse platform. The simulation using this applet validates our scheme of implementation of secure DA in WSNs for implementation in farmland. A security mechanism is also proposed to protect the sampling procedure in the form of IDS manager, incorporated into this simulated WSN. By exploiting the spatial correlation among the 28 SNs labeled - s1 to s28 considered in this case study in close proximity, a proper conclusion can be drawn towards the soil quality. From the functioning and lifespan - perspective of the SNs and hence the WSN, the DA and its transmission over the network is very vital. Each one of the soil attributes has their own delay and energy consumption in its process of sensing and transmission. The maximum delay found by simulation is 109.38 µs for the temperature attribute; and a minimum of 15.63 µs for - pH-value, pressure, humidity, and wind-velocity. The simulated maximum and minimum energy, consumed are 17.504 mJ (for pH-value) and 1.04 mJ (for pressure). The function of the IDS manager in this prototype version of the applet is made simple for convenience, but in future work it is planned to address all types of attacks, in view of farmland application.

VI. Acknowledgment

Authors convey special thanks to the Management of Dayananda Sagar Group of Institutions (DSI) for all its support and constant encouragement for this project work. Authors also convey special thanks to Visvesvaraya Technological University (VTU), Belagavi, Karnataka, for all its direct or indirect support for this work.

References

[1] A Swami, Q Zhao, YW Hong, L Tong, "Wireless Sensor Networks: Signal Processing and Communications", Wiley, 2007.

[2] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," in proceedings of ACM First international conference Embedded Networked Sensor Systems (SenSys), pp. 255-265, 2003.

[3] A. Manjhi, S. Nath, and P.B. Gibbons, "Tributaries and Deltas: Efficient and Robust Aggregation in Sensor Network Streams," in proceedings of ACM SIGMOD international conference Management of Data, pp. 287-298, 2005.

[4] S. Madden, M.J. Franklin, J. Hellerstein, and W. Hong, "Tag: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," in proceedings of Fifth symposium on Operating Systems Design and Implementation (OSDI), 2002.

[5] Lei Yu, Jianzhong Li, Siyao Cheng, Shuguang Xiong, and Haiying Shen, "Secure Continuous Aggregation in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, VOL. 25, No. 3, March 2014.

[6] K.-W. Fan, S. Liu, and P. Sinha, "On the Potential of Structure-Free DA in Sensor Networks," in proceedings of IEEE INFOCOM, pp. 1-12, 2006.

[7] Herbert Schildt, "The Complete Reference: Java", McGraw-Hill, Seventh Edition, 2007.

[8] William Stallings, "Cryptography and network security: Principles and practice", Pearson, 6th edition

[9] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," in proceedings of ACM 13th conference Computer and Comm. Security (CCS), pp. 278-287, 2006.

[10] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-By- Hop DA Protocol for Sensor Networks," in proceedings of ACM MobiHoc, pp. 356-367, 2006.

[11] B. Frikken and J.A. Dougherty IV, "An Efficient Integrity- Preserving Scheme for Hierarchical Sensor Aggregation," in proceedings of ACM First conference Wireless Network Security (WiSec), pp. 68-76, 2008.