Secured Data Acquisition System for Smart Water Applications using WSN

Ayaz Hassan Moon^{1*}, Ummer Iqbal¹ and G. Mohiuddin Bhat²

¹National Institute of Electronics and Information Technology, Srinagar - 191132,J & K, India; moonah@rediffmail.com, khan_ummer123@yahoo.com ²Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar-190006,J & K, India; drgmbhat@gmail.com

Abstract

Objectives: The paper presents a comprehensive system design and implementation of a prototype for secure data acquisition of water quality parameters in a real time basis using Wireless Sensor Network. Methods/Analysis: The design is based upon under-water sensors for measuring water parameters, interfaced to a Data Acquisition Board attached with a WSN mote. Layered architecture comprising of Mote Tier, Server Tier and a Client Tier has been employed. The system has been developed on TinyOS using TinyECC library and Matlab. Security service to provide data authentication employs a light-weight-key-generation scheme using ECC. A web based application facilitates visualization of sensor data. Findings: Following simulation in Tossim, the data acquisition application was ported to the WSN hardware with security primitives for data authentication. Field trials were carried out at World famous Dal Lake in Srinagar and data related to pH, Conductivity, ORP/Redox, Temperature, Turbidity and Oxidation was accessed remotely through the web application. For the purpose of recording the field location (Longitude and Latitude), a GPS sensor was also integrated to the WSN set-up. The water quality parameters acquired through the Data Acquisition System were correlated with the water quality test reports of standard labs. Energy and computational calculations were carried and benchmarked to ascertain the suitability of the system design considering the resource constraint nature of WSN. The product has the potential of becoming an important constituent of smart water applications as a requirement of smart city. Novelty/Improvement: The field deployable prototype serves as a generic model for monitoring the water quality of any water body like river ,lake, reservoir etc on a real time basis with the novel feature of employing sensor data authentication as a security service.

Keywords: Data Acquisition System, Key Generation, Real Time Monitoring, Smart Water, WSN

1. Introduction

Researchers have hitherto published numerous papers on environmental monitoring systems based upon WSN. However, complete system development and implementation details are obscured for one reason or the other. Moreover, Environmental sensing and monitoring applications based upon WSN have been developed without employing any basic security primitive in the overall system design. This could be attributed to resource constraint nature of WSN and the sensitivity of WSN applications, both of which have undergone a paradigm shift. In this paper a comprehensive design for developing a secured prototype for data acquisition of water quality parameters using wireless sensor network, which can become an important constituent of Smart City applications is presented. Draft Policy on Internet of Things brought out by DeitY envisions the resolve of the Govt. of India to develop 100 smart cities for which an expenditure of Rs 7,060 crores has been earmarked. This will Leverage developing smart environment, smart water¹, smart health, smart agriculture etc. thus leading to improved quality of life².

Lack of proper water quality monitoring system

^{*} Author for correspondence

prohibits a large populace to know about the quality of their drinking water. Technology intervention is required to provide appropriate solutions. In this case, WSN based water quality monitoring system shall be the most appropriate solution as it would leverage the advantages associated with WSN technology.

1.1 Related Work

Traditional methods of monitoring the water quality can be categorized into following:

- Manually collect the water samples and undertake subsequent lab analysis.
- Usage of hand held Instruments at the Site.

Both the methods have the disadvantage of being time consuming, Labour intensive and subject to Human error. A more sophisticated method involving use of remote sensing technology namely detecting the spectrum specifics of electromagnetic wave in a noncontacting method can also be used. However it provides low accuracy and not generally suitable for undertaking real time monitoring³. WSN based solutions are most appropriate in designing applications for monitoring of water quality parameters on real time basis in terms of ease of deployment/redeployment, wide coverage, accuracy, Scalablity etc.

Numbers of schemes are available on water quality monitoring system based on WSN. To the best of our knowledge none of the schemes implement any security primitive in their solutions. Moreover the number of sensors interfaced for monitoring water quality is generally restricted to 2 or 3. In⁴, the water quality monitoring system based on WSN has been designed for environmental protection using zigbee (CC2430) wireless transmission and TCP/IP for transmission of sensed data. In⁵, an integrated online water quality monitoring system has been designed for the measurement of pH parameters and dissolved oxygen. In^{6,7}, describes real time monitoring system for water environments based on WSN. Typical real time water environment monitoring systems are EMNET (by Heliosware-USA) FLECK (by CISRO Australia), Lakenet (by Notre Dame University, USA) and Smart Coast (Researchers from Ireland)⁸⁻¹²

1.2 Motivation

Security aspects of WSN based water acquisition systems concerning human life can no longer be ignored.

Therefore data needs to be accepted after exercising some basic security checks if not all. This was ignored previously primarily due to two reasons. One, the nature of the applications developed did not warrant any security safeguards with the exception of military and reconnaissance and the other, the issues involved in porting of the resource intensive security protocols into the resource constraint network that WSN was. Now with the technological advancements in MEMS, MIMO, MISO, SIMO¹³, Zigbee devices¹⁴ along with development of light weight security solutions based upon ECC, the security aspects may be embedded into the system design itself.

1.3 Challenge

It is more challenging to secure a WSN in comparison to conventional networks like WLAN, WPAN, mobile, adhoc networks (MANNET) and cellular networks due to inherent characteristics like energy constraints, small memory sizes, less computational power and small bandwidth^{15,16}. Most of the energy expended by sensor node is due to radio communication rather than data processing. Each bit transmitted in WSN consumes energy equivalent to executing about 1000 instructions¹⁷. With the stated constraints associated with WSN, the challenge is how to design and build WSN based robust and secure systems for example for smart cities. For example incorporating solar based energy management system for sensor nodes can drastically improve lifespan of WSN¹⁸.

2. System Development

2.1 Design Goals

The goal is to design a prototype which can serve as a generic secure data acquisition system for real time monitoring of water quality of any water body¹⁹. The overall system architecture is depicted in [Figure 1]. The system should be portable, mobile and secure besides having low power consumption, ease of deployment/redeployment along with supporting secure connectivity with the remote client location. The system can be used as one of the important sub-systems of building smart cities to track water quality of various water bodies including lakes, rivers reservoir etc.

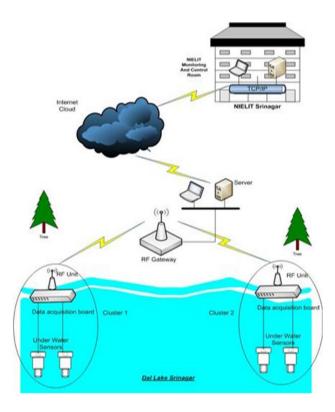


Figure 1. Overall System Architecture.

2.2 Design Methodology

A generic data acquisition system has different sensors interfaced via a signal conditioning unit to A/D converters. A communication unit integrated to the data sensing and processing unit transmits and receives the data emanating from the system or directed towards it. A generic block diagram is given in [Figure 2]. The design is based upon under-water sensors of Global Waters for measuring pH, Conductivity, ORP/Redox, Temperature, Turbidity, Oxidation levels²⁰. These sensors, which give current output proportional to the physical quantity which they sense, have been interfaced to Data Acquisition Board MDA300 of Memsic²¹. The board supports both analog and digital channels. The system architecture is organized in 3 Tiers. Applications have been developed in TinyOS²², an open source operating system for embedded systems and by making use of TinyECC library²³. Data sensing and communication application is capable of data packetization and routing it to the base station. Online and offline Sensor data can be accessed remotely through a web interface. A MATLAB based application has been developed for data analysis.

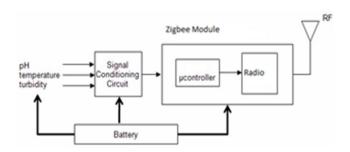


Figure 2. Block diagram of data acquisition system.

2.3 Architecture of Data Acquisition System

The layered architecture of Data Acquisition System as shown in [Figure 3] has been built on three-tier architecture comprising of Data Acquisition Tier, Server Tier and Client Tier. The Data Acquisition tier consists of cloud of sensor nodes formed by interfacing under water sensors to data acquisition board (MDA 300) attached with MicaZ mote²⁴. The server tier is an always-on facility that handles sensor data calibration and database logging. Client tier connects to the server tier for user visualization of sensed data.

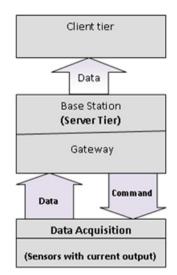


Figure 3. Layered Architecture of DAS.

2.4 Hardware implementation

Data Acquisition Tier has been built around host of underwater sensors sensing physical parameters like temperature, pH value, conductivity, dissolved oxygen to determine the water quality of a water body²⁵.

Hardware Devices Used in the System Design includes:

• Sensors (pH, Conductivity, Temperature, Turbidity,

Dissolved Oxygen, ORP/Redox)

- Data Acquisition Board (MDA300)
- Gateway (MIB 600/520)
- PC's
- Motes (MicaZ)

The platform has been developed around MDA300 data acquisition board with 8 single ended analog channels, 8 digital channels, counter channel, external sensor excitations, LEDs and power supply (VCC). Signals with dynamic range of 0 V to 2.5 V can be plugged to these channels.

2.4.1 Sensor Interface Circuit

The analog to digital converter has 12-bit resolution (N). The LSB value is given as below.

The LSB value = Full Scale Voltage range / $(2^{N}-1) = 2.5$ / $(2^{12}-1) = 0.61$ mv (1)

Where N is the no. of ADC bits. The sensor generates the current output of 4 to 19 mA corresponding to the value of physical quantity being measured. The output of ADC can be converted to voltage (v) equivalent to: $V= 2.5 * (ADC_reading / 4095)$ (2)

Scaling Resistors need to be added to properly scale the voltage levels of external analog sensors so that maximum voltage is clamped to 2.5 V DC at 19ma of sensor output current. A resistor value approximated to 125 Ohms (2.5v/19ma) was chosen while calibrating the signal conditioning circuit²⁶. The interfacing of two wire sensor with the data acquisition board is shown in [Figure 4]. Likewise three wire sensors have also been interfaced to the data acquisition board.

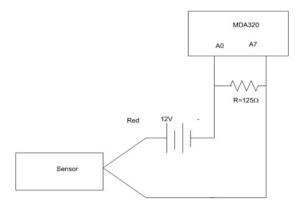


Figure 4. Two wire sensor interfacing with MDA 320.

2.4.2 Calibration of Sensors

The Sensors used for measuring pH(WQ201), Temperature(WQ101),ORP/Redox(WQ600), Conductivity (WQ-Cond), Turbidity(WQ730), Dissolved Oxygen(WQ401) were calibrated to obtain the correct values. The pH sensor (WQ-201) gives an output of 3.97 mA at 0pH and 19.01 mA at 14 pH. The conversion factor specified is 1.0743 mA/pH. Therefore the current output generated by X pH value solution is calculated as: $X_{pH value} = X^* 1.0743 + 3.97 mA$ (3) e.g 4pH = 4*1.0743 + .397 = 8.20 mA .Similarly other sensors were also calibrated as per the equations given in the.

Table 1. Calibration Equations

	1
Sensor	Equation (I _{out} is in mA)
Dissolved Oxygen	$DO(\%) = \frac{lout - 4.003}{0.15}$
	$DO(\%) = \frac{0.15}{0.15}$
ORP/Redox	$ORP(mV) = \frac{lout - 4.02}{0.015}$
	O(RP(mV)) = -0.015
Temperature	$Temp(0F) = \frac{lout - 4.1}{0.0877}$
	0.0877

2.4.3 Power Supply Circuit

The sensors are powered by 12 volt Lead acid battery delivering 10 volt regulated dc bus to different sensors. An excitation voltage of 5 volts is derived from the dcdc converter (boost converter) within MDA. This can be programmed to control the duty cycle of sensor supply voltage to prolong the battery life. Sensor power control circuit is built around two MOSFET switches and a regulator. The battery voltage along with the regulated output voltage after appropriate scaling, can be sensed remotely through VBATT_SENS and VREG_SENS pins respectively, that are available at MDA300. A3 second warm up time period is observed before the sampling is undertaken by MDA. The excitation voltage enable schematics for sensors is shown in.

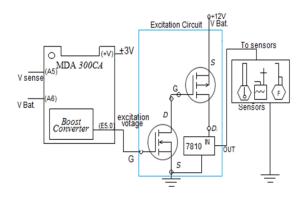


Figure 5. Excitation schematics for enabling supply voltage to sensors.

2.5 Software Implementation

The system comprises of the following set of applications as shown in the [Figure 6]:

- 1. Data Acquisition Tier Applications
- 2. Server Tier Application
- 3. Client Tier Applications

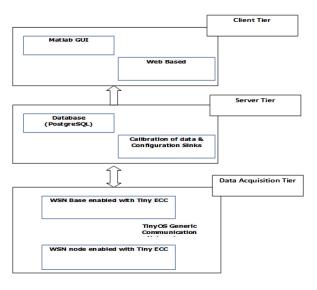


Figure 6. Software Representation of the System.

2.5.1 Data Acquisition Tier Applications

The motes in Data Acquisition Tier are programmed by two types of applications:

- Data sensing & transmitting application
- Gateway application

Data sensing & transmitting application is a NesC program capable of sampling the data in the data acquisition board and transmitting it over the network. The program samples the channels when the timer event occurs. The timer duration can be programmed as desired. For transmission and reception of radio packets, generic TinyOS messaging stack is used. Data sensing and transmitting application is enabled with Tiny ECC library for implementing security primitives like key exchange and authentication. The gateway application is primarily a generic TinyOS Base application with its configuration modified to enable TinyECC. The base application is also capable of data exchange on a serial link to the server through UART component. The wiring diagram of MDA300 is shown in the [Figure 7]. The SamplerC and TimerC module is utilized for sampling various analog and digital channels of MDA300 at fixed interval

controlled by TimerC module. The GenericComm module is used for transmitting and receiving generic TinyOS messages. NN.nc defines the interface NN, which provides big natural number operations. NNM.nc implements this interface. ECC.nc defines the interface ECC, which provides the basic and enhanced elliptic curve operations based on sliding window method and projective coordinate system. ECCM.nc implements this interface. The application has been wired with secp160r1 curve standard Similarly Base has also been programmed including framer and UART components used for relaying the packets received to the serial forwarder.

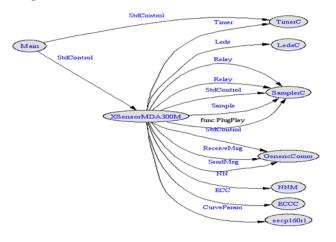


Figure 7. Wiring Diagram of NesC Program Fused in MDA300.

1.1.2 Server Tier Application

It is an application written in C for providing high level services like sensor data calibration and database logging. The application is capable of receiving packets over LAN or Serial Port depending upon the gateway being used. It provides features for displaying the received sensor data in raw, parsed and calibrated form. Raw option allows the packet to be seen in the stream of hex-decimal numbers which form the packet. Parsed option extracts the relevant data from the packet but displays it in the un-calibrated form. The database logging is handled by the application by inserting the data in the archival as well as live data tables created in a PostgreSQL database. The insertion operation in the tables is handled using database triggers.

1.1.1 Client Tier Application

The sensor data at client tier can be visualized either using a web based application or MATLAB. A web based

application has been developed for visualizing the offline and online sensor data. A MATLAB based application has also been developed for performing data interpretation of the received sensor data. The Matlab application can be connected with the server tier over VPN connection. [Figure 8] shows live data reading being collected from 2 sensor nodes. The Figure 10 shows the part of the environmental Data Packet. TinyOS supports a packet size of 54 bytes by default. This is inclusive of 7 bytes reserved for Generic Active Message Fields and rest for the payload. The packet payload structure has been customized as per the application and is shown in [Figure 9].

Connect to WSN DataBase Nam	task			User Nam	•	tele			Applica	ation	mda3	•1_00		
Password	tny			IP Addres	5	192.168.1	U.		Port		8080			Disconnec
	result,time	epoch	nodeid	parent	adell	Hdc1	Mic?	691	<i>6</i> 91	692	votage	humid	humtemp	
	2013-07	NaN	1	0	8.9599	59.3200	11.1900	1	1	1	492	1653	6817	-
GridView	2013-07	NaN	4	0	-3.6860	24.3700	24.5300	1	1	1	427	1827	6717	
Live														
Plot														_
	_												-	

Figure 8. Client interface for data viewing.

NadelD	Temp	pН	ORP/Redax	Cand	Turbidity	MAC
(1Byte)	(2 Bytes)	(20 Bytes)				

Figure 9. Part of Environmental Data Packet.

3. System Security

Environmental data is generally meant for public viewing hence there is no need for any confidentiality. In security parlance, it implies that sensor data need not to be encrypted. However the risk of injecting false packets (Sybil Attack)²⁷ by an adversary into the network would exist. This can result in disruption of environmental monitoring by raising false alarms or subverting a genuine alarm. Hence it makes a strong case for employing proper authentication and data integrity checks on sensor data before it is accepted.

Key Generation and exchange is the bed rock of all security primitives. For WSN based application, ECDH protocol is regarded as an effective protocol for symmetric key generation and distribution but is prone to manin-the-middle attack. This is because of the lack of any registration or authentication mechanism of the nodes prior to the key generation and distribution process^{28,29}. Thus before key generation and distribution, we run node initialization and registration protocols based upon ECC.

Base station generates an elliptical curve with the following sextuple domain parameters over F_p Р

$$Params = \{p, a, b, G, n, h\}$$
(4)

Where integer p specifying the finite field F_{n} , two elements $a,b \in F_n$ specifying an elliptical curve $E(F_n)$ defined by the equation:

$$E: y^2 \equiv x^3 + ax + b \pmod{p} \tag{5}$$

E is the elliptical curve, G is the generator point of E, a prime n which is the order of G and integer h which is the cofactor, $h = \# E(F_p / n)$. The notations used are tabulated in [Table 2].

Table 2. Symbol Table

Symbol	Notation
BS	Base Station
Fp	Prime Field
Sb	Random Number Chosen by BS
Pb	Public Key of BS
Id	Node ID
Sa	Random Number Chosen by Node
Pa	Public Key of Node

3.1 System initialization

(i) Base station (BS), chooses random number Sb ε F where F_{p} is the prime field of elliptic curve.

(ii) BS Computes Pb = Sb.G, as its public key and broadcasts it.

(iii) BS Computes and stores hash of each node Id, Hash(Id), which is in the network,

(iv) Data Acquisition Node (DAN) chooses a random number Sa ε F_n where F_n is the prime field of elliptic curve. It Computes $Pa = Sa^{-1}G$, as its public key

3.2 Node Registration

The node registration process involving 3 steps are shown in [Table 3]. After three exchanges if

 $X = (Hash(Id).Sa^{-1}.Pb \text{ computed by the Node is equal})$ to the Y = (Hash(Id).Pa.Sb) computed by the Base then the Node is registered by the BS. Hash(Id) is broadcasted by BS using its public certificate over a secured channel in the following manner: {(Hash(Id).SG), Hash(Id)}.Each receiving node can multiply Hash(Id) by public certificate of base station to verify the broadcast and then register the node 30 .

Table 3.	Node	registration
----------	------	--------------

Step	Node	Base Station (BS)
1	Compute Pa= Sa ⁻¹ .G and	
	send it to BS	
2		Compute Sb.Pa and Send
		it to Node
3	Verify Sb.Pa.Sa=Sb.	
	Sa ⁻¹ .G.Sa= Sb.G= Pb	
	(Pb is the public Certif-	
	icate of BS ,Hence BS is	
	authenticated by Node)	
4	Compute X =(Hash(Id).	
	Sa ⁻¹ .Pb) and send it to BS	
5		Compute Y= (Hash(Id).
		Pa.Sb)and verify if
		X==Y, Node is Registered
		with BS.

3.3 Key Generation using Hidden generator

The key exchange algorithm developed to overcome MIM attack, performs a sequence of steps as shown in [Table 4] to establish a shared key point Ga between Data Acquisition Node (DAN) and Base. By leveraging the strength of ECDLP the shared point is communicated to Base through a 3 exchange process³¹. DAN chooses a random numbers x and performs a scalar multiplication x.Ga .DAN embeds the x.Ga into the TinyOS message payload and sends it to the Base. Base receives x.Ga and performs a scalar multiplication of x.Ga with y where y is the random number chosen by Base. (x.Ga) .y is transmitted back to DAN. By applying the sequence of multiplicative inverse operations, Ga is established as a shared point between base station and the node.

Table 4.	Hidden	Generator	Key	Exchange.
----------	--------	-----------	-----	-----------

Step	Data Acquisition Node	Base
1	Generate a Random Num-	Generate a Random
	ber X	Number Y
2	Generate a Shared Key	
	Point G	
3	Compute X. G _a and send it	
	to Base	
4		Compute Y.(X. G _a) and
		send it to DAN
5	Compute (X ⁻¹ . (Y.(X. G _a	
))=Y. G_a and send it to Base	
6		Compute Y ⁻¹ . Y. $G_a = G_a$

3.4 Symmetric Key Generation

Ga(x,y) being a point on the curve will have x and y coordinates. Depending upon the curve chosen, the size of these coordinates can be 120, 160, 192 bits etc. x being a scalar number can act as a symmetric key between two parties, which can be used as a session's key for various purposes including distribution of public keys or for encrypting a session.

3.5 Sensor Data Authetication

Message Authentication Code $(MAC)^{32}$ which is key dependent, has been be generated using x co-ordinate of the common generated point Ga. The shared key (x) shall be used for generating key based MAC to authenticate the sensor data packet. DAN shall apply a MAC function, which is key dependent, to the Sensor data (P) which forms the payload of the packet and generates a Message digest (T) also known as MAC. DAN attaches the MAC authentication code (T) to the packet and transmits it to the Base Station.

$T = MAC_x(P)$

The base station applies the same MAC function while using the same key (x) to compute MAC of the received packet (T^*). On verification if $T=T^*$, the sensor data packet is accepted by the base station.

3.6 Security Analysis

The proposed Scheme provides a safeguard against MIM attack due to the factors listed as below.

- Node Registration is done in an authenticated way prior to the key generation.
- This method thwarts the man-in-middle attack as the intruder would not have any access to the generator point as it is not made public. This is unlike other ECC based key generation methods where the generator point is made public within the network. Moreover, the algorithm leverages the hardness of ECDLP as extracting Generator point from the scalar multiplicative terms during exchanges becomes a discrete logarithmic problem which has exponential time complexity.

3.7 Perytons Protocol Analyzer

TinyOS packet size by default is 54 bytes. A custom packet structure has been created for key exchange. The key exchange messages have been customized to active message AM type of 0x01. The payload structure has been modified so as to accommodate shared generator point G(x,y) where in x and y coordinates occupy 42 bytes i.e. 21 bytes each. The Node ID and Packet ID occupy 1 byte each thus creating an overall packet size of 44 bytes. The packet structure is shown in the [Figure 10].

Node ID	Packet	X-	Y-
(1 Byte)	ID	Coordinate	Coordinate
	(1 Byte)	(21 bytes)	(21 bytes)

Figure 10. Key exchange packet structure.

The Perytons Protocol Analyzer³³ is a professional suite for capturing and analyzing IEEE 802.15.4, ZigBee, 6LoWPAN, RF4CE, Thread, Bluetooth Smart, PLC-PRIME, G3-PLC and other wireless and wire-line traffic. The Traffic capured by Perytons Protocol Analyzer at MAC layer during key generation between MDA300 and Base is shown in the [Table 5] which validates the key

 Table 5.
 Traffic captured using Peryton Analyzer

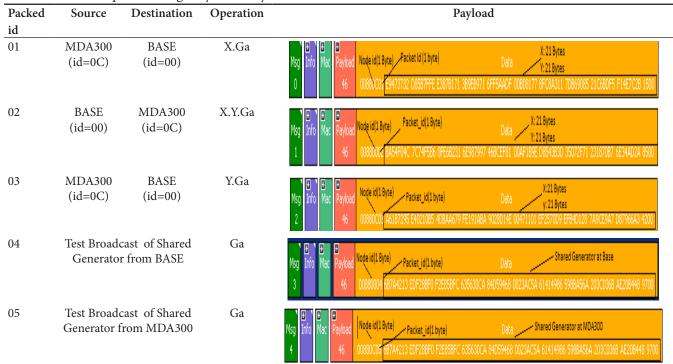
generation and exchange between Base and MDA300.

3.8 Performance Benchmarking

The performance benchmarking of the key exchange protocol involving hidden generator points would be based on the following parameters:

- 1. Energy Consumption
- 2. Memory Consumption
- 3. Computational Time

Energy Calculations would primarily depend on computational time taken for core ECC operations like Point Addition, Scalar Multiplication in addition to the voltage and current requirements. The number of ECC operations required to be performed have been indicated in [Table 6]. For calculation of energy we use $E = V^*i^*t$ (joules) where V and i stand for voltage and current drawn respectively, t is the execution time for each operation. MicaZ node using Atmel AT Mega 128 L is powered by 02 AA batteries. With a voltage of 3 V for 02



AA batteries, and a maximum load current of 19.7 mA, the energy calculations for each operation are indicated in the [Table 7]. For the purpose of capturing computational time of various key ECC operations like Point addition, Scalar Multiplication a basic setup was established using MicaZ, MIB520(programming board). A nesC program was developed for sending the time message to a TinyOS Serial Forwarder. These packets were sent on serial port through a MIB 520 programming board. The packets captured by the serial forwarder were transported to a java application. From [Table 6] it can be inferred that the proposed protocol offers protection against man-in-themiddle attack with energy consumption and execution time comparable to ECDH.

Protocol	No of Exchanges	Scalar Multiplication	Point Addition	Inverse Operation	ROM	RAM	Defense against
	0	1		1			MIM
1-hidden Generator Point	3	4	-	2	15482Bytes	1337Bytes	Yes
ECDH	02	4	-	-	1487Bytes	1208bytes	No

Table 6.Comparative analysis

Table 7. Energy Calculations

Operations	Avg Time Taken	1-hidden	Energy Consumption	ECDH	Energy
	(Seconds)	Generator Point	(1-Hidden Generator)		Consumption(ECDH)
			(milli Joules)		milli Joules
Scalar Multiplication	1.78	4*1.78= 7.14 secs	422.38	4*1.78= 7.14 secs	422.38
Inverse Operation	0.11	2*0.11=0.23 secs	14.06	Nil	Nil
Point Addition	1.787	NIL	nil	Nil	Nil
TOTA	AL	7.37 secs	436.44	7.14secs	422.38

4. Results

The prototype developed has 6 sensors to monitor the water quality. The range and accuracy of measurement of different sensors is indicated in [Table 8]. The field trials were conducted at the world famous Dal lake. The measurements were taken at different depths in the Dal lake owing to the flexibility in adjusting the length of marine grade cables. The prototype and the results of field trials are shown in the [Figure 11] and [Table 9].



Figure 11. Prototype design.structure.

Table 8.Range and	d Accuracy of S	ensors	
Sensor	Model	Range	Accuracy
рН	WQ201	0-14 pH	2 % Full scale
Temperature	WQ101	-50° to +50°C	$\pm 0.2^{\circ}$ F or $\pm 0.1^{\circ}$ C
ORP/Redox	WQ600	-500 to +500 mV	2% full scale
Conductivity	WQ-COND	0 to 200 µS/cm	+0.5% of reading
Turbidity	WQ730	0-50 NTU	+/- 1% of full scale
Dissolved Oxygen	WQ401	0 to 8 ppm	±0.5% full scale

Table 9.	Field Trails	conducted	at Dal L	ake Srinagar,	J &	ĸΚ
----------	--------------	-----------	----------	---------------	-----	----

Date	Time	Depth	PH	Temperature ⁰ C	ORP (mv)	DO (%age)			
2014-11-19	16:14:57.795	2 feet	7.8850	12.3409	249.3333	29.8888			
2014-11-19	16:16:46.029	4 feet	7.7667	11.7843	249.6587	29.8237			
2014-11-19	16:25:12.889	5 feet	7.4436	11.1350	251.9360	31.3528			
Latitude: 34.55 Longitude: 74.52Location: Near SKICC immediate turning after SKICC Jetty No. 6									

5. Conclusion

In this paper, a complete system design and implementation of a WSN based Data Acquisition System for real time

monitoring of water quality is presented. A generic field deployable prototype has been developed and field tested at Dal Lake Srinagar for monitoring of water quality parameters which include *pH*, *Conductivity*, *Turbidity*,

Temperature, ORP and *Dissolved Oxygen.* Security primitives related to authentication of sensor data has been in cooperated in the system design. Key generation has been achieved using a light weight protocol based upon ECC and hidden generator concept. The protocol is comparable to ECDH in terms of computational time and energy consumption; however it offers protection against MIM.A web based application facilitates the visualization of sensor data remotely. Future work shall be planned to improve upon the existing system design so as to enhance the utility of the product keeping in mind the requirements of WSN based Smart Environment systems for Smart Cities.

6. References

- 1. Kim DH, Suh J, Park KH. An empirical investigation on the determinants of smart water grid adoption. Indian Journal of Science and Technology. 2015; 1–9.
- Wooseung J, Kim TH, Choi K, Kang NG. Leakage Pattern Monitoring Method of CEP based Water Supply Block System. Indian Journal of Science and Technology. 2015 Oct; 8(27). Doi no: 10.17485/ijst/2015/v8i27/81054.
- 3. Jiang P, Xia H, He Z, Wang Z. Design of a water environental monitoring system based on wireless sensor network. Sensors. 2009; 9(8):6411–34. Doi: 10.3390/s90806411.
- He D, Zhang LX. The Water Quality Monitoring System Based on WSN. 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). 2012 Apr 21-23. p. 3661–64. Doi: 978-1-4577-1415-3
- Wiranto G, Maulana YY, Hermida IDP, Syamsu I, Mahmudin D. Integrated Online Water Quality Monitoring: An Application for Shrimp Aquaculture Data Collection and Automation. International Conference on Smart Sensors and Application (ICSSA). 2015. p. 1–4. Doi: 978-1-4799-7364-4.
- 6. Jiang P. Survey on Key Technology of WSN-Based Wetland Water Quality Remote Real-Time Monitoring System. Chin J Sens Actuat. 2007; 20:183–6.
- Jiang P, Kong Y. Design of Data Video Base Station of WSNs Oriented Water Environment Monitoring. Chin J Sens Actuat. 2008 Jul 29-31; 21:1581–85.
- 8. EmNetLLC Technology. Available from: http://www.he-liosware.com/technology.html. 16/01/2009.
- The CSIRO ICT Centre. Wireless Sensor Network Devices. Available from:http://www.ict.csiro.au/ page.pHp?cid=87. 16/01/2009.
- Seders LA, Shea CA, Lemmon MD, Maurice PA, Talley JW, LakeNet: An Integrated Sensor Network for Environmental Sensing in Lakes. Environm Eng Sci. 2007; 24:183–91.
- 11. O'Flynn B, Catala MF, Harte S, O'Mathuna C, Cleary J, Slater C, Regan F, Diamond D, MurpHy H. Smart Coast:

A Wireless Sensor Network for Water Quality Monitoring. 32nd IEEE Conference on Local Computer Networks, LCN 2007, Dublin, Ireland. 2007 Oct 15-18. p. 815–16.

- Yang X, Ong KG, Dreschel WR, Zeng K, Mungle CS, Grimes CA. Design of a Wireless Sensor Network for Long-Term, in-situ Monitoring of an Aqueous Environment. Sensors. 2002; 2:455–72.
- Islam MR, Kim J. Step-by-Step Approach for Energy-efficient Wireless sensor Network. IETE Technical Review. 2012 Jul-Aug; 29(4):336–45.
- Rasin Z, Abdullah MR. Water quality monitoring system using zigbee based wireless sensor network. International Journal of Engineering and Technology. 2012 May; 9(10):24–8.
- 15. Hsuech CT, Li YW, Wen CY, Quyang YD. Secure adoptive Topology control for wireless ad-hoc sensor networks. Sensors. 2010; 1251–78.
- 16. Kavitha T, Sridharan D. Security Vulnerabilities in Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security. 2010; 5:031–044.
- Hill J et al. System Architecture Directions for Networked Sensors. 9th int'l conf Architectural Support for Programming Languages and Operating Systems ACM Press. 2000. p. 93–104.
- Ashok J, Thirumoorthy P. Design Considerations for implementing an Optimal Battery Management System of a Wireless Sensor Node. Indian Journal of Science and Technology. 2011; 1255–9.
- 19. Chaamwe N. Wireless Sensor Networks for Water Quality Monitoring: A case study of Zambia. IEEE 4th International Conference on Bio-informatics and Bio-Medical Engineering (iCBBE); 2010 Jun.
- 20. Global Water User Manual; 2007.
- 21. Memsic. Xserve User Manual; 2007.
- 22. Levis P, Gay D. TinyOS Programming. Cambridge University Press; 2009.
- Ning LP et al. Tiny ECC: A Configurable Library for Elliptical Curve Cryptography in Wireless Sensor Networks. 7th International Conference on Information Processing in Sensor Networks SPOTS Track; 2008 Apr.
- 24. He D, Zhang LX. The Water quality monitoring system based on WSN. IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). 2012.
- 25. Moon AH, Khan UI et al. Practical implementation of WSN based data acquisition system with external connectivity. IEEE Conference on ICMIRA. 2013. p. 77–81.
- 26. Walters JP, Liang Z, Shi W, Chaudhary V. Wireless sensor network security: A Survey. Security in Distributed Grid and Pervasive Computing. CRC Press; 2001.
- 27. Moon AH, Shah NA, Ummer I, Adil A. Simulating and Analyzing Security Attacks in WSN Using Qualnet. IEEE Conference on ICMIRA. 2013. p. 68–76.
- 28. Kishore R, Budwa HS. High Performance Scalar Multiplication for ECC. International Conference on Computer Communication and Informatics. 2013.

- 29. Choi K, Kim M, Chae K. Secure lightweight key distribution with ZigBee pro for ubiquitous sensor networks. International Journal of Distributed Sensor Networks. 2013; 8. Article ID 608380.
- Hong WW, Bing LY, Chen et al. The Study and Application of Elliptic Curve Cryptography Library on Wireless sensor Network. 11th IEEE International Conference on Communication Technology Proceedings. 2008. p. 785–88.
- Kodali RK et al. Implementation of ECC with Hidden Generator Point in Wireless Sensor Network. 6th IEEE International Conference on Communications Systems and Networks. 2014. p. 131–36.
- 32. Chang Q, Zhang YP et al. A node Authentication Protocol based on ECC in WSN. International Conference on Computer Design and Application. 2010; 2. p. 606–09.
- 33. Perytons TM Protocol Analyzer User Manual. 2011.