I J C T A, 9(20), 2016, pp. 33-41

A Secure WSN Based Forest Fire Prediction System

Ummer Iqbal*, Adnan Manzoor and Arsalan Mustafa*****

ABSTRACT

Forest Fire is a predominant natural disaster which requires modernization for early detection and prevention. The technology of Wireless Sensor Networks (WSN's) has shown substantial promise in pre-determination of the forest fires. In this paper,the design of a system based on WSN for predicting and detecting Forest fires has been discussed.The focus is towards security aspects of such systems as less work has been done in that direction. Using Elliptical Curve Cryptography (ECC) protocols have been proposed for providing a secure base-to-node and node-to-base communication. The protocols have been, developed using nesC language,simulated on Tossim,and also tested on MicaZ motes.The security analysis of developed protocols has also been carried out.

Keywords: Wireless Sensors Network, Forest Fire, ECC, ECDLP, TinyOS

1. INTRODUCTION

Forest fires or wildfires are uncontrolled fires that occur in wild areas and cause substantial natural, monetary, and human loss. Early exposure and pre-determination of possible fires is the only plausible way to minimize the damage and casualties. Thus the most critical issue in a forest fire detection system is an immediate response. For this purpose constant and calibrated surveillance of the forest conditions is required. A recent revolution in the field of Wireless Sensor Networks[1] has made it possible to use this technology in Early Forest fire detection. Based on the various studies that have been conducted towards this end, it can be observed that the adoption of WSN for Forest Fire detection and prevention is more prudentthan traditional techniques.

Kechar et al [2] presented the usage of WSN for reliable forest fire detection.They studied the Canadian and Korean Fire detection techniques for Energy and data efficiency, and using real-time simulations concluded that the Canadian Fire Weather Index was more plausible in WSN systems for Forest Fire detection. Lloret et al [3] suggested usage of Wireless Sensor Network of fire detectors connected to Cameras withI.P's. Hafeeda et al [4], in 2008 proposed the use of Canadian Fire Weather Index to measure the rate of spread of the forest fire. Aslan [5] discussed in detail a plausible network Framework of WSN used in Forests for Fire detection and proposed Energy efficient inter-cluster and intra-cluster protocols.

Forest fire prediction systems are data-centric applications. Security primitives which include authentication,integrity, and freshness are of paramount importance in such systems. Based on the data sent by various sensor nodes, alarms and actuators are employed, thus it becomes imperative to address the critical security primitives.Although many designs for such systems have been proposed, the security of the misless addressed. As these systems involve low power devices, traditional security mechanisms cannot be employed.

This paper proposes a secure forest fire detection system based on WSN, enabled with a light weight security framework. The Security solution leverages the low computational overheads associated with

* National Institute of Electronics and Information Technology, Srinagar, J & K, India, *Email: khan_ummer123@yahoo.com*

** Hans Raj College, University of Delhi, New Delhi, India, *Email: adnan904@gmail.com*

*** Hans Raj College, University of Delhi, New Delhi, India, *Email: arsalanali09@gmail.com*

Elliptical Curve Cryptography (ECC).The proposed framework has been simulated on Tossim and tested on MicaZ motes. The security analysis has also been carried out.

The rest of the paper is organized as follows: Section 2 presents the proposed Forest Fire prediction system. Section 3 highlights the security requirements of the proposed system. Section 4 presents the security framework using ECC. Section 5 provides the implementation details. Section 6 gives the security analysis of the proposed scheme. Section 7 concludes the paper.

2. PROPOSED FOREST FIRE PREDICTION SYSTEM

The basic schematics of the proposed system is shown in figure 1. The system divides a Large Forest area into various cluster regions. All these clusters are interconnected through a multi-hop routing protocol.The sensors deployed in a cluster will send the collected data to their respective cluster heads using a Multi-Hop network. The Sensors primarily used in the forest fire detection system include Temperature, Humidity, Rainfall, and Wind Speed. In general, the output of all the sensors is between 4-20 mA. These Sensors are to be integrated with a data acquisition board like MDA300[6].MDA300 is a multi-function direct user interface and flexible data acquisition board. The board in itself acts as a sensor and detects temperature and humidity changes in the environment. MDA 300 has 7 single-ended or 3 differential ADC channels, 4 precise differential ADC channels, 6 digital I/O channels with event detection interrupt, 2.5, 3.3, 5V sensor excitation and a low-power mode. The MDA300 data acquisition board is sandwiched with MicaZ Motes through I2C bus(51-pin connector).These motes are programmed using TinyOS [7] Operating System. The cluster heads shall be placed at strategic locations in the large forest area within their respective clusters such that they too connect to each other through multi-hop routing. The closest of these cluster heads to the base station (BS) shall relay the received data to the BS. This data will finally be collected at the Database server in large amounts. As an enormous amount of data is being generated over certain periods of time, an effective data management technique for well-organized data storage and retrieval using Big Data concept can be employed.

Based on the conclusion drawn by Kechar et al[2] that the Canadian Fire Weather Index (FWI) was more plausible in WSN systems for Forest Fire detection, the proposed system would make use of the Canadian Fire detection method.

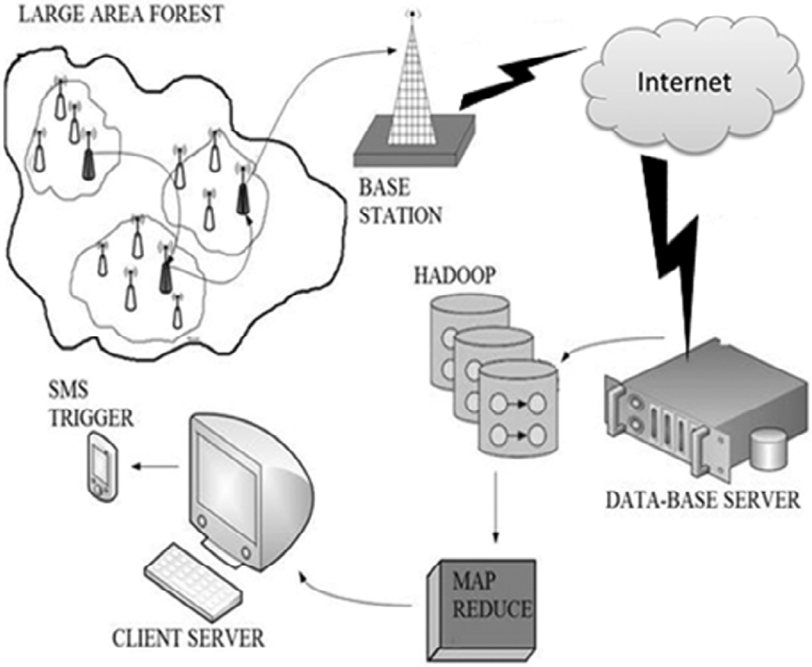


Figure 1: Basic Schematics of the Proposed System

The Canadian method is based on Fire Weather Index (FWI). The FWI takes into consideration the temperature, relative humidity, wind speed and rain readings. These observations help us in predicting the highest burning conditions at about 1600hrs LST (Local Standard Time) during the day.The FWI is made up of six components. The first three components may be classified as primary components which in fact are fuel moisture codes and monitor the moisture content of three types of forest fuels based on their drying speeds. These FMC are – Fine Fuel Moisture Code(FFMC), Duff Moisture Code(DMC), and Drought Code(DC). From the primary components, we derive two intermediate components (Fire Behaviour Indexes) that monitor the rate of spread of forest fire, the amount of fuel available for the fire to spread, and the intensity of the fire. These are – Initial Spread Index(ISI) and Buildup Index (BUI). The combination of these intermediate indexes gives us the fire weather index(FWI)[8][9]. The block diagram in figure 2 summarizes the FWI.

All of these six components have their unique scale of values and in each of them, a higher value indicates a more severe fire[2]. The FWI scale and the danger of fire for each range of values is indicated in Table 1.

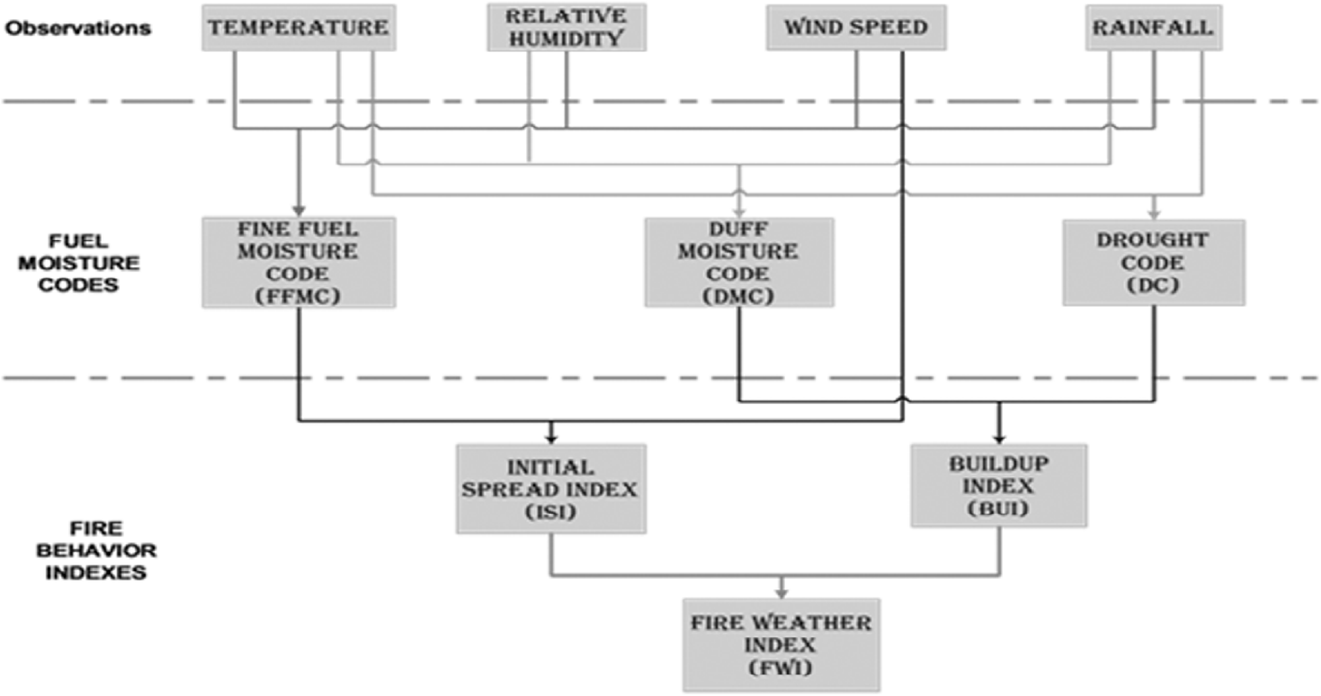


Figure 2: Block Diagram of FWI [8]

Table 1
Potential Fire Danger based on FWI Index [2]

FWI	*Range*	*Indicator*
Low	0-5	🟩
Moderate	5-10	🟩
High	10-20	🟨
Very High	20-30	🟧
Extreme	30+	🟥

3. SECURITY REQUIREMENT IN WSN BASED FOREST FIRE PREDICTION SYSTEM

Security is one of the most imperative aspects of any system. Thesecurity requirements of the proposed system can be understood by considering the following 2 communications patterns:

1. Base to Node Communication
2. Node to Base Communication

Base to Node communication primarily involves broadcast from the base station to all the nodes in the network. As the most commoncommunication paradigm, the network users are expectedto issue the queries to the network before obtaining theinformation of their interest. Furthermore, in wireless sensorand actuator networks (WSANs), the network users mayeven need to issue their commands to the network.The broadcast communication can be employed in the proposed system for over the air programming (OTAP) to reprogram the network remotely.

Node to Base communication principally broadcasts data from nodes in the network to the base station. The data transmitted involves the sensed parameters like rainfall, precipitation etc.Because of sensitivity, it becomes quite imperative to handle entity authentication,integrity, and freshness of the received data. The implementation of these security parameters is important so as to subvert any false alarms which may be generated.

The security requirements (*SR*) for both types of communication patternsaredefined as follows:

- *SR1:Node Authentication* -Node Authentication is used to establish that the communication from the sensor node to the base station is legitimate. An adversary may inject false alarms into the network. This can result in disruption of the system by raising false alarms or subverting a genuine alarm.
- *SR2:Broadcast Authentication* -Broadcast Authentication is used to validate a broadcast from a BS to all nodes in the network.
- *SR3: Data Integrity* -With data integrity, the transmission of sensor data from the sensor node to the Base Station cannot be modified or altered by any external or unauthorized source. The integrity is also paramount for broadcasted data.
- *SR4: Low Computational Cost* - WSN networks are characterized by severe resource constraints in terms of energy, computational power, bandwidth, and storage. The typical characteristics of a MicaZ mote are 8-Bit micro-controller,ATmega128L with 4 KB of RAM, 128 KB of ROM, thebandwidth of 250kbps, and is powered by two AA lithium cells with 2000mAH of energy [6].The security protocols must adhere to these constraints.

4. SECURITY FRAMEWORK

The proposed Security framework has been designed to achieve *SR1 to SR4*.The framework uses ECC to realize these security requirements for the 2 predominant communication patterns of the proposed system. The Notations used in the framework are tabulated in Table 2.

4.1. Node to Base Communication

Node N_i senses the respective parameters and encapsulates them in D_n.The sensed data is transmitted from the N_i to the Base station as given in (1):

$$N_i \rightarrow BS: K_n.H(id).PU_{base}||D_n||S_n||H(D_n) \tag{1}$$

On receiving (1), BS stores $K_n.H(id).PU_{base}$

Table 2
Notations Used

Symbol	*Description*
D_n	Sensor Data
B_n	Broadcast Data
N_i	Node i
BS	Base Station
Id	Node id of N_i
G	Generator Point of Elliptical Curve
K_n	Private Key of Node
K_b	Private Key of Base
$PU_{base}=K_b.G$	Public Key of Base
$PU_{node}=K_n.G$	Public Key of Node

$$Q = K_n.H(id).PU_{base} \tag{2}$$

BS multiplies (2) with K_b^{-1}

$$Q = K_n.H(id).PU_{base\,.}\ K_b^{-1}$$

$$Q = K_n.H(id).k_b.G\,.\ K_b^{-1}$$

$$Q = K_n.H(id).G_{\,.}$$

$$Q= PU_{node}.H(id) \tag{3}$$

BS calculates:

$$P = PU_{node.}H(id) \tag{4}$$

From its own storage BS verifies P==Q, if true N_i is authenticated by BS and the packet is accepted. For data integrity, BS recalculates the hash of D_n and verifies it with the received hash.

4.2. Base to Node Communication

The BS broadcasts $B_{n,}$ as given in (5)

$$BS^* \rightarrow K_b.(1+H(D_n)).G\ ||B_n \tag{5}$$

On receiving the broadcast the nodes store $K_b.(1+H(D_n)).G$

$$Q = K_b.(1+H(D_n)).G \tag{6}$$

Nodes compute $P = PU_{base}(1+H(D_n))$ from their own storage. Nodes verify $P==Q$,if true then the Base broadcast is authenticated. For data integrity nodes recalculates the hash of B_n and verifies it with the received hash.

5. IMPLEMENTATION

The programs for proposed system were implemented in TinyOS operating system using nesC Language and simulated on TOSSIM [10]. TinyECC [11] library has been used for performing ECC operations. The programs

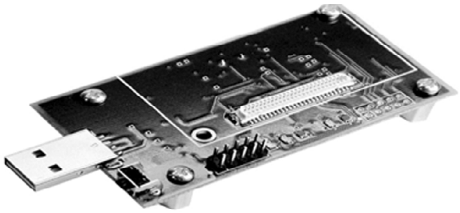
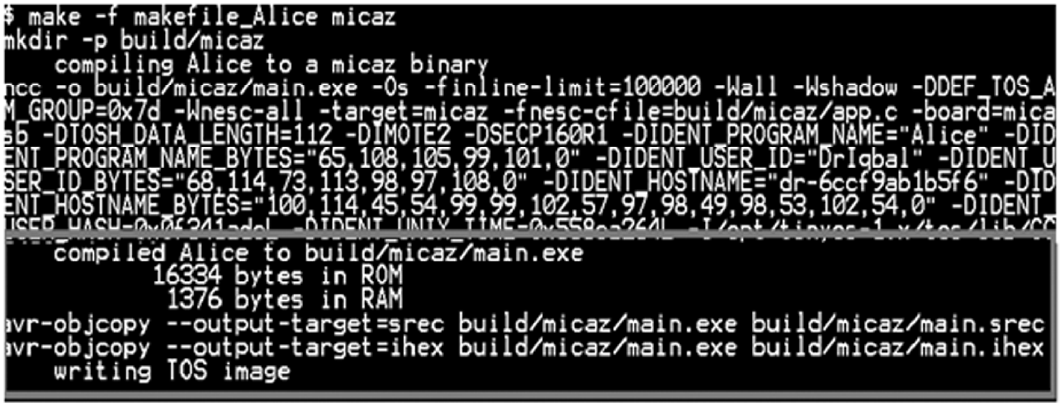


Figure 3: MIB520 System Programmer [16]



```
$ make -f makefile_Alice micaz
mkdir -p build/micaz
    compiling Alice to a micaz binary
ncc -o build/micaz/main.exe -Os -finline-limit=100000 -Wall -Wshadow -DDEF_TOS_A
M_GROUP=0x7d -Wnesc-all -target=micaz -fnesc-cfile=build/micaz/app.c -board=mica
s5 -DTOSH_DATA_LENGTH=112 -DIMOTE2 -DSECP160R1 -DIDENT_PROGRAM_NAME="Alice" -DID
ENT_PROGRAM_NAME_BYTES="65,108,105,99,101,0" -DIDENT_USER_ID="DrIqbal" -DIDENT_U
SER_ID_BYTES="68,114,73,113,98,97,108,0" -DIDENT_HOSTNAME="dr-6ccf9ab1b5f6" -DID
ENT_HOSTNAME_BYTES="100,114,45,54,99,99,102,57,97,98,49,98,53,102,54,0" -DIDENT_
USER_HASH=0x0f341adeL -DIDENT_UNIX_TIME=0x558ea264L -I/opt/tinyos-1.x/tos/lib/CC
    compiled Alice to build/micaz/main.exe
            16334 bytes in ROM
             1376 bytes in RAM
avr-objcopy --output-target=srec build/micaz/main.exe build/micaz/main.srec
avr-objcopy --output-target=ihex build/micaz/main.exe build/micaz/main.ihex
    writing TOS image
```

Figure 4: TinyOS Snapshot of writing TOS image on MicaZ

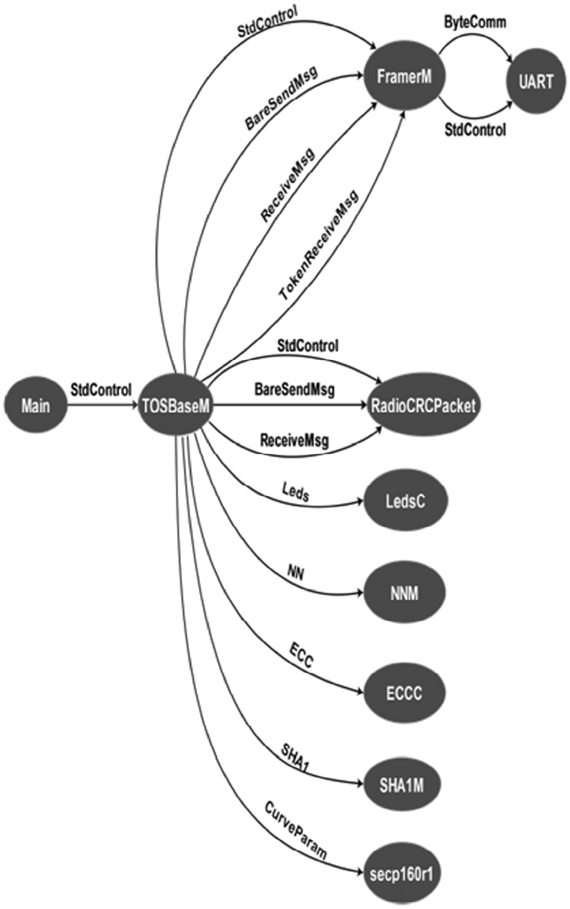


Figure 5: Component graph of Base Station program

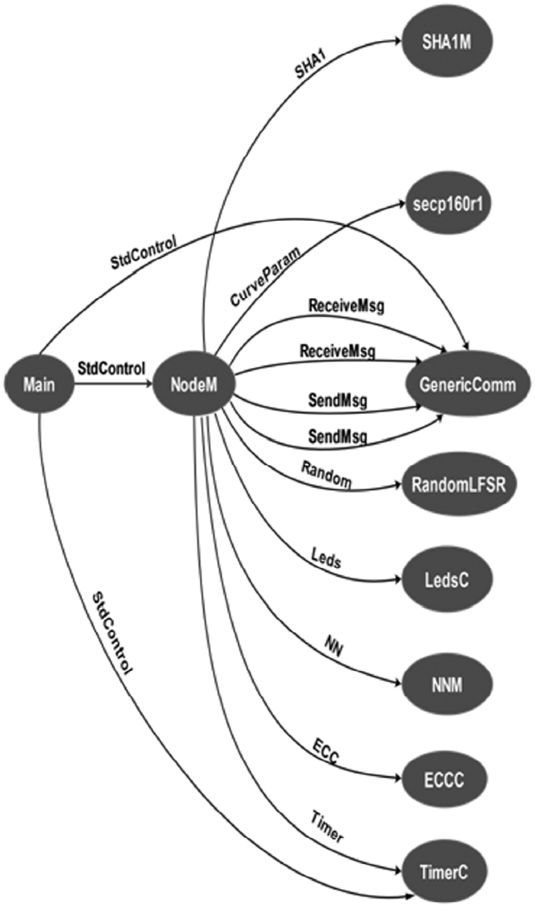


Figure 6: Component graph of Sensor Node Program

were burnt on MicaZ motes using a MIB520[6] programmer shown in figure 3. The TinyOS snapshot of MicaZ mote being programmed with MIB520 programmer is shown in figure 4. The component graph for the Base Station program and Sensor node program is shown in figure 5 and figure 6.

6. SECURITY ANALYSIS

The security scheme is based on ECC, thus the strength of this scheme is based on Elliptical Curve Discreet Log Problem(ECDLP).Some of the definitions pertaining to this discussion are listed as below:

Definition 1: An elliptic curve consists of a set of numbers (x, y), also known as points on that curve that satisfies the equation:

$$y^2 = x^2 + ax + b$$

The set of all of the solutions to the equation forms the elliptic curve.We generally see elliptic curves used over finite fields in cryptographic applications where the points (x, y) form an additive group[12][13].

Definition 2: In the elliptic curve group (E,+) defined over a finite field $F_p$for some prime no 'P', let 'G' be a generator point which gives every other point in the group. When this point 'G' is added 'n' number of times to itself, the point addition yields another point 'Q' belonging to the same Elliptical curve. Given the fact that 'G' and 'Q' are known, finding 'n' becomes infeasible. This problem of finding 'n' is called as Elliptical Curve Discreet Log Problem[12][13].

Definition 3:A secure hash function h() : x → y is one way; if given x , it is easy to compute h(x) = y; however, given y, it is difficult to compute $h^{-1}(y) = x$ [14].

6.1. SR1-Entity Authentication

Proof: Entity Authentication involves verification of the identity of the node by BS. The node sends $K_n.H(id).PU_{base}$ to the B.S. In this expression, $K_n$is the private key of the Node N_i, thus only Ni can generate $K_n.H(id).PU_{base}$. The expression $K_n.H(id).PU_{base}$ is ECDLP problem,thus K_n cannot be extracted from it. On receiving $K_n.H(id).PU_{base}$, BS evaluates it and after series of steps arrives at the expression $PU_{node}.H(id)$, where PU_{node} is the public key of the node N_i. $PU_{node}.$H(id) can be arrived at,if and only if K_n is used in the expression sent by N_i, thus verifying that $K_n.H(id).PU_{base}$ has been actually generated by $N_{i.}$ This leads to the entity authentication of N_i by BS.

6.2. SR2-Broadcast Authentication

Proof: Broadcast authentication involves authentication of the base broadcast by all the nodes in the network. BS broadcasts:$K_b.(1+H(D_n).G\ ||B_{n,}$. In this scalar multiplication expression K_b used is the private key of the BS. K_b is only known to BS, thus the expression $K_b.(1+H(D_n).G\ ||B_{n,}$ can only be generated by B.S. K_b cannot be extracted from $K_b.(1+H(D_n).G$ as it is an ECDLP problem. Authentication of the broadcast by the nodes is done by calculating $PU_{base}(1+H(B_{n,})$. If $PU_{base}(1+H(B_n))== K_b.(1+H(D_n)).G$, then the base is authenticated by the nodes in the network.

6.3. SR3-Data Integrity:

Proof: Each Node N_i has a preloaded one-way hash function h(). h() can be used for Data Integrity as shown in figure 7.

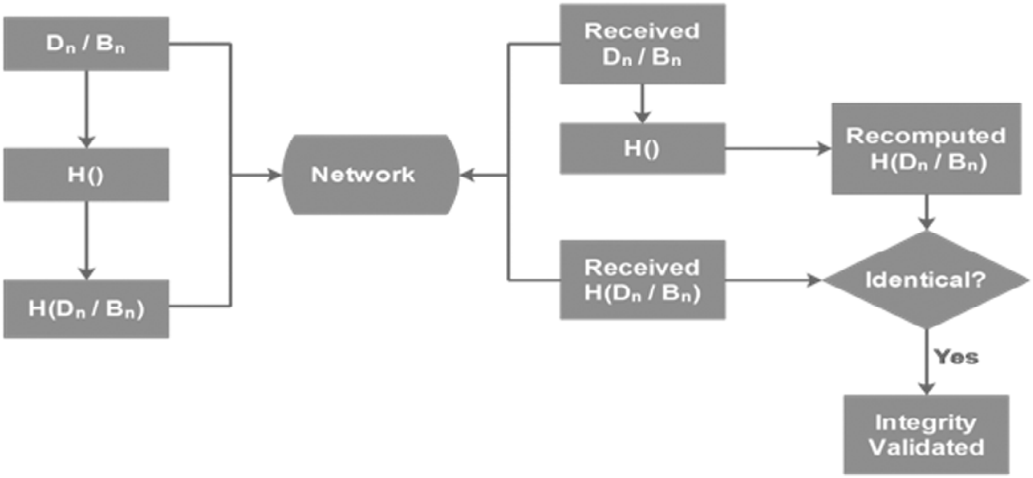


Figure 7: Hash for Data Integrity

6.4. SR4-Low Computational Cost

Proof: An ECC protocol needs 160-bit keys to provide security equivalent to 1024-bit RSA[15]. Lesser key size brings in other significant advantages in terms of smaller memory (both ROM as well as RAM), faster execution and efficient storage. The comparison[12][13] is shown in table 3.

Table 3
Key comparison between RSA and ECC in terms of security equivalence

Key length of RSA	*Key length of ECC*	*Ratio of RSA/ECC*
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

7. CONCLUSION

This paper firstly highlights the less explored yet essential security component of the existing WSN based Fire Detection Systems. Secondly, alight weight security framework has been presented to achieve basic primitives like node authentication, broadcast authentication, and data integrity. An Implementation of the framework has been performed on the TinyOS Platform using MicaZ motes.A comprehensive security analysis of the proposed system has also been presented. Organisation of the enormous data received from the motes, spread across a large forest area using Big Data concepts like Hadoop for fast retrieval and easy management is yet to be explored.

REFERENCES

[1] F. Akyildiz, Weilian Su, Yogesh Sankarasubramanian, and Erdal Cayirci. “A survey on sensor networks”, IEEE Communications Magazine, 2002, 40(8): PP. 102-114.

[2] Kechar Bouabdellaha, Houache Noureddine, Sekhri Larbi. “Using Wireless Sensor Networks for Reliable Forest Fires Detection”. The 3rd International Conference on Sustainable Energy Information Technology (SEIT 2013). Procedia Computer Science Volume 19, 2013, Pages 794-801

[3] Jaime Lloret, Miguel Garcia Diana Bri and Sandra Sendra. “A Wireless Sensor Network Deployment for Rural and Forest Fire Detection and Verification Sensors” 2009, 9(11), 8722-8747; doi: 10.3390/s91108722

[4] M. Hefeeda, M. Bagheri, “Forest Fire Modeling and Early Detection using Wireless Sensor Networks”, Adhoc& Sensor Wireless Networks, Vol.7, No.3/4, p169-224, 2009.

[5] Yunus Emre Aslan, Ibrahim Korpeoglu Özgür Ulusoy. “A framework for use of wireless sensor networks in forest fire detection and monitoring Computers, Environment and Urban Systems”36 (2012) 614–625

[6] Memsic Mote Manual

[7] Levis,P., and Gay.D., 2009 “TinyOS Programming. Cambridge University Press”.

[8] “Development and Structure of the Canadian Forest Fire Weather Index System”, C.E. Van Wagner 1987.

[9] J.A. Turner, B.D. Lawson “Weather in the Canadian Forest Fire Danger Rating System: auser guide to national standards and practices. Environment”. Canada, Canadian Forestry Service, Pacific Forest Research Centre, Victoria, B.C. -1978.

[10] Levis,P., Lee,N., Welsh,M. and Culler,D.E. et al “TOSSIM : Accurate and Stable Simulation of Entire TinyOS Applications”. SenSys

[11] A. Liu and P. Ning et al. “Tiny ECC: A Configurable Library for Elliptical Curve Cryptography in Wireless Sensor Networks”, IPSN 2008

[12] Darrel Hankerson, Alfred J. Menezes, Scott Vanstone. “Guide to Elliptic Curve Cryptography” Springer 2004

[13] BernardMenzes “Network Security and Cryptography”, Cengage Learning

[14] Hui-Feng Huang, “A New Design of Access Control in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, vol. 2011, Article ID 412146, 7 pages, 2011. doi:10.1155/2011/412146

[15] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. “Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. In CHES2004, volume 3156 of LNCS, 2004.

[16] Memsic MIB520 USB Interface Board Manual