Simple Cryptographic Data Security Algorithm for Wireless Sensor Network

[1]Obiakor C. L, [2]Azubogu A.C.O, [3]Ayinla S.L,
[1,2]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria
[3]Department of Computer Engineering, University of Ilorin, Ilorin, Kwara State

[1]chiomaobiakor@gmail.com
[2]austinazu@yahoo.com
[3]ayinla.sl@unilorin.edu.ng

Abstract- Wireless sensor network (WSN) popularity is increasing for a wide variety of applications, yet the integrity and confidentiality of transmitted data remain one of the major barriers to its full exploitation. In this paper, a light-weight symmetric cryptographic algorithm was developed to encrypt and decrypt data transmitted between the terminal nodes and base station of the experimental WSN testbed developed for pipeline monitoring. This WSN incorporate accelerometers for measuring induced vibration non-invasively and has 5 terminal nodes that communicates to the sink node, which discards corrupt data, aggregates the uncorrupted data and forwards to the base station. A simulator running on a Visual Basic Interface was also developed to test the efficiency and functionality of the developed algorithm. Data was got by simulating leakage at different points of the pipeline with the opening and closing of the valves. The effect of simulated leakage in terms of amplitude of acceleration (vibration change) was found to be proportional to the leak location and sensor nodes location. The results generated from these simulations were implemented with the developed cryptographic simulator, to show how encryption and decryption of data at the different nodes are achieved.
Keywords: WSN, Cryptographic algorithm, accelerometers, testbed.

1.0 Introduction

A wireless sensor network consists of multiple detection stations called sensor nodes deployed over a geographical sensing area to monitor [2] and detect specific target parameters and collect data, and then send the data to sink or base station (BS) wirelessly [3]. Every sensor node is equipped with a transducer (sensing unit), microcontroller (processing unit), transceiver (communication unit) and power source [4]. A lightweight operating system enables a node to function and provides features such as sensor polling, data aggregation and manipulation, wireless communication, and remote access [5].Due to the recent technology advances, Micro-Electro-Mechanical Sensors (MEMS) technologies have made node miniaturization, manufacturing of small and low-cost sensors to become technically and economically feasible [6].WSN are used in several real life applications such as environmental monitoring [7], agriculture [8], production and delivery [9], military [10], structural monitoring [11] and medical applications [12].Depending on the area of deployment, the data gotten from these sensors can be sensitive and highly classified hence, are prone to attacks.

WSNs are known to be susceptible to a variety of attacks; there can be attacks on nodes or attacks on information such as node capture, physical tampering, and denial of service, prompting a range of fundamental research challenges [13]. An attacker can also eavesdrop on, inject or alter the data transmitted between sensor nodes, thereby compromising the confidentiality, authenticity, reliability, availability, and the integrity of the data being transferred. These make data security in wireless sensor network an area of great concern. Effective security technique is therefore required to ensure that data provided by the WSN meets its need without

compromise while ensuring also that this technique takes into consideration the sensor node constraints of low memory, flexibility, low cost of implementation and low energy consumption. Cryptography is one way to provide security. It can be by symmetric key techniques, asymmetric key techniques or by hybrid technique.

Considering these constraints, this paper describes the development of acceleration-based sensor nodes for pipeline monitoring and the implementation of a light weight symmetric cryptographic algorithm to ensure that the integrity and confidentiality of transmitted data are not compromised.

2.0 Review of Related Works

Security management is the process of protecting and securing information transferred within a WSN. Wireless sensor networks make use of a number of sensor nodes within or close to the area of event to not only collect and integrate but also process and relay the information [1]. Depending on the area of deployment, the data gotten from these sensors can be very sensitive, hence security of these information are of paramount importance. So research in an efficient security management in WSN is an on-going issue and a challenge especially as these networks have limited capabilities with respect to power and memory size. According to [14], Data Encryption Standard (DES) presented a model that uses 16 round Feistel structure, with a block size of 64bits; 8 bits for parity check and has the effective key length of 56 bits. DES is weak to linear cryptographic analysis and has short key length, its improvement; Triple DES is slower and computationally intensive in terms of memory and time.

Blowfish is keyed, symmetric cryptographic block cipher. It has a 64-bit block size and a key length between 32 bits and 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. Blowfish has long processing time hence is slow and are susceptible to plain text attack [15]. Two fish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. . It is said to be efficient both for software that runs in smaller processors but has very large file size. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits; it is very similar to RC5 in structure. It is very compact, and can be coded efficiently in assembly language on most processors but the lack of an on-the-fly round key computation capability causes decryption to require a large amount of RAM and reduces the key agility [16].

The authors [17] described Advanced Encryption Standard (AES) as an iterative rather than Feistel cipher. Its principle was based on a design principle known as a substitution-permutation network. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. AES is easy to implement, it is fast, has low energy requirement and its code size, data size, processing time, and power consumption make it desirable.

3.0 Methodology and System Design

An experimental testbed was setup behind the block *A* wing of Prof. Gordian Ezekwe Faculty of Engineering building, Nnamdi Azikiwe University, Awka, Nigeria. The asymmetrical testbed has the dimension of 21 m x 18 m with 15 pressure (PVC) pipes of 2-inches in diameter and valves labelled V_1 to V_6. Figure 1 shows the layout of the testbed drawn to scale.

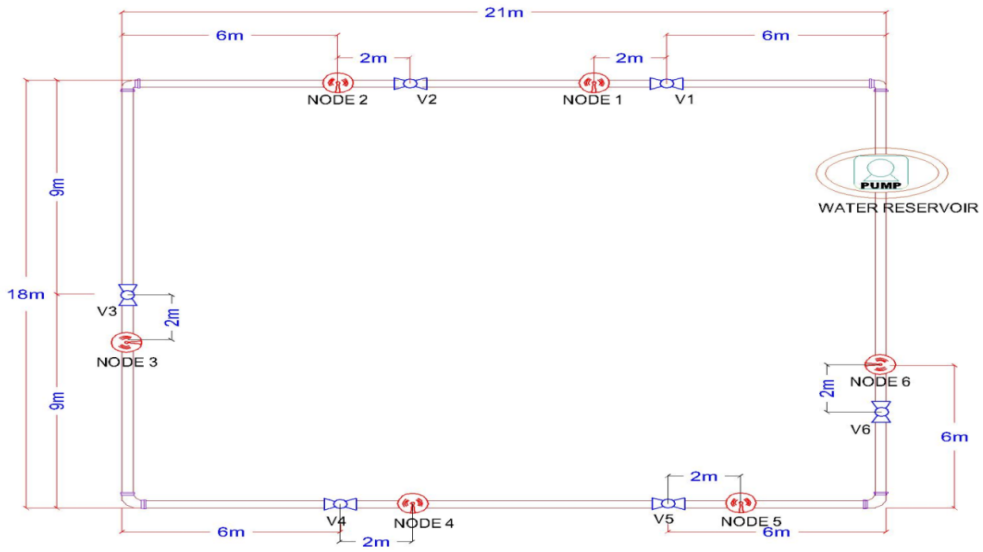

Figure 1: Experimental Prototype testbed

Acceleration-based sensor nodes were attached on each wing of the network close to the valves and the valves were used to simulate ruptures through opening and closing. A 1.5hp pumping machine was used to ensure water circulation around the pipeline during the experiment. The Source nodes were placed on the surface of the pipeline while the sink node also placed on the pipeline gathered and aggregate the data from the source nodes to be transported to the base station located few meters away from the sensing field to a PC as user interface.

Security Management algorithm was incorporated to enhance the data security and integrity and the cryptographic algorithm was employed on all microcontrollers to encrypt data before transmission from any of the terminal nodes to the base station, as well as the ability to decrypt on the base station.

- The base station queries the sink node for information.
- The sink node broadcasts this information to the source nodes every 8seconds.
- Each microcontroller on each node receives the broadcast and signals the sensors to sense.
- The sensor nodes are turned ON and senses.
- The microcontroller receives the sensed data and encrypts it.
- The radio device transfers the encrypted data from the front-end node to the sink node.
- The sink node decrypts the data, scrutinizes the data for viability, relevance and aggregation. Then it encrypts the relevant data and sends to the base station.
- The base station decrypts the information, which can therefore be used for further decision making depending on the nature of response.

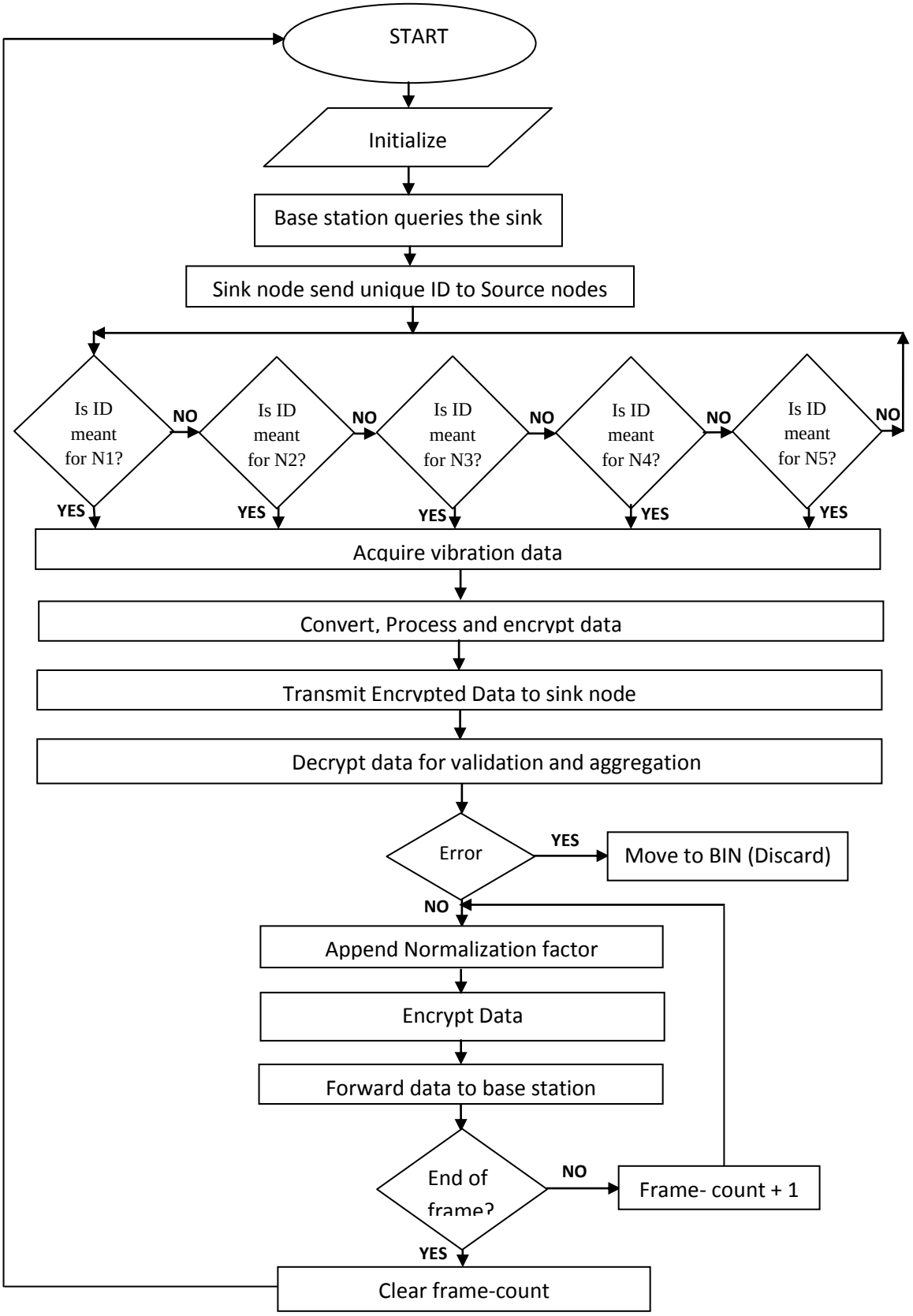

Figure 2: WSN Data Flow chart.

The cryptographic model was developed by considering the following parameters:

1. Code size: This size of the code was determined by the memory size of the

microcontroller on which it will be implemented. Hence the code size is made to be 5KB.

2. Secured protocol vulnerability: The implemented code was done using randomly selected encryption key and randomly selected decryption key developed with AES algorithm. This makes the code uniquely secured as it encrypts the data almost at the point of generation. It also combines this with a camouflage login method created for access control.
3. Data size: The encryption of the data increases the data size by 2KB and utilizes the memory size available in the microcontroller (65KB).

✓ The Encryption Algorithm:
The following are the steps involved in the encryption process:

1. Byte Multiplication step:
If data = M,
[Output from this stage = M*x (Where x is a randomly selected variable)]
2. The Shift Byte step:

In this step, the bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row; [Mx – 1].

3. The Add Random Key step:

In the Add Random Key step, each byte of the state is combined with a byte using the XOR operation (⊕); [(Mx – 1) ⊕ c], where c is a random byte.

4. Byte Addition:
The output from step 3 is then added to a fixed variable;
[((Mx – 1) ⊕ c) + y], where y is the fixed variable.

✓ Decryption Algorithm:
In order for decryption to work, all parameters of this function except cipher Text value - must match the corresponding parameters of the Encrypt function which was called to generate the cipher text. The decryption is simply a reverse of the encryption process.

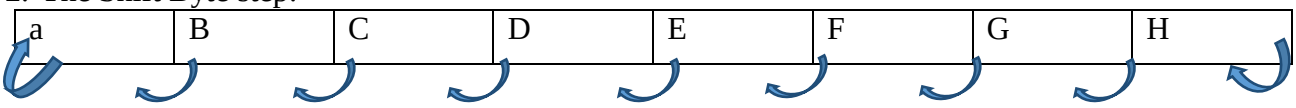

Figure 3: Shift Byte step.

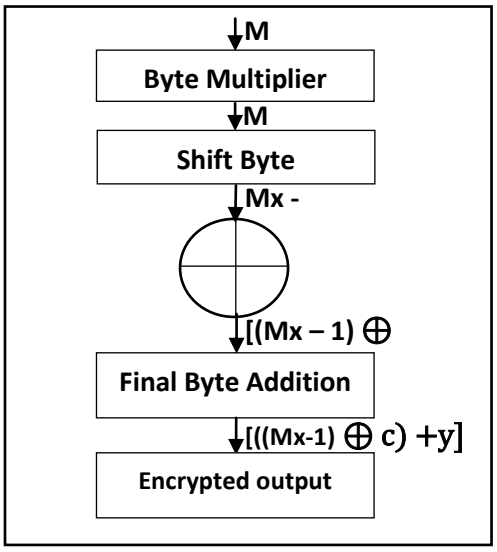

Figure 4: Encryption Algorithm Structure

4.0 Results and Discussion

The recorded data were processed in the form of distribution tables. The Cryptographic WSN security simulator was developed using Microsoft Visual studio 2015, with VB programming language to simulate the security system implementation of the cryptographic algorithm on the generated data recorded at the BS during the experiment. Fig. 2 shows the simulator interfaces for the WSN data security with sample encrypted and decrypted outputs gotten at the base station during the experiment.

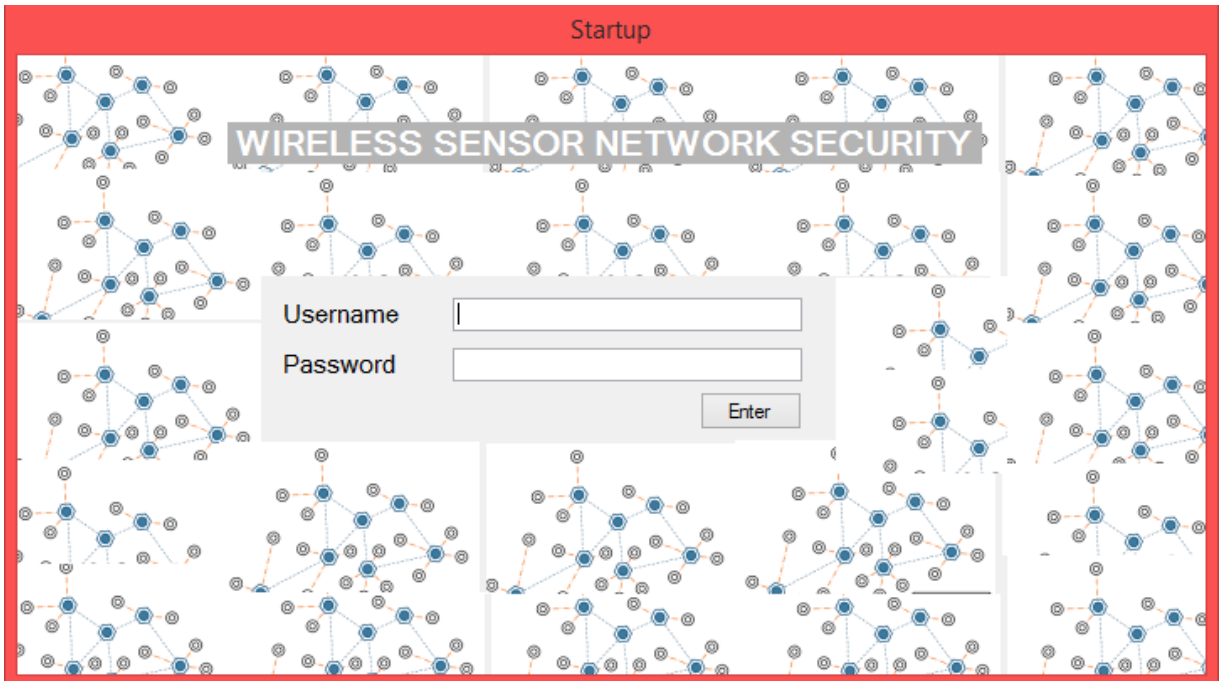

Fig 5: Cryptographic WSN Security Implementation Camouflage login interface.

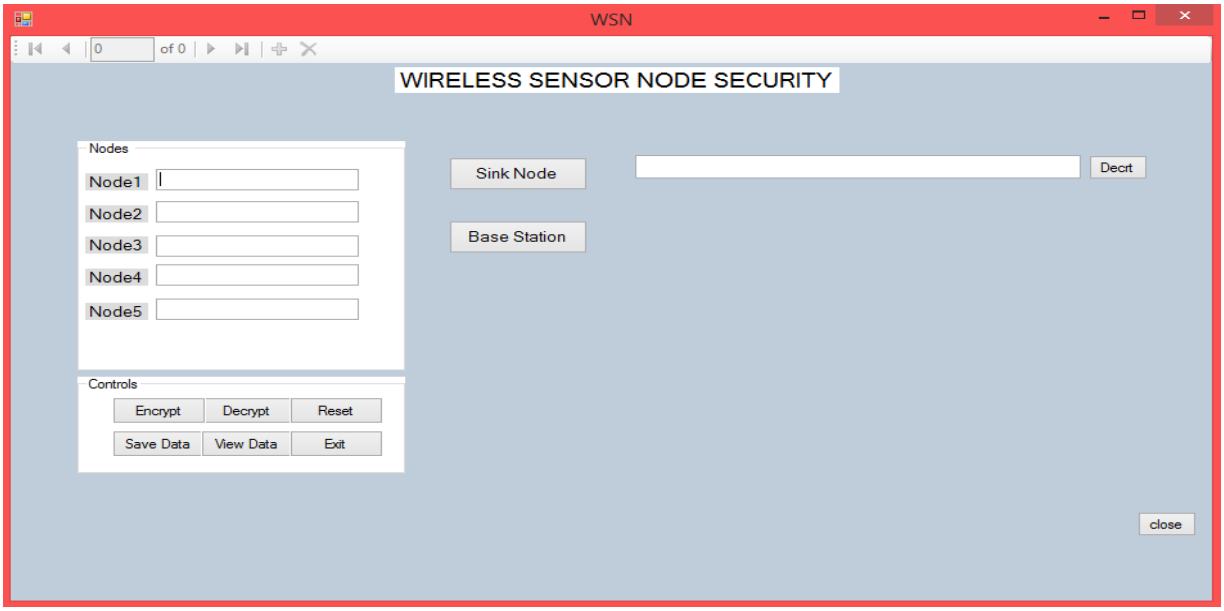

Fig 6: WSN Node Security Implementation Interface.

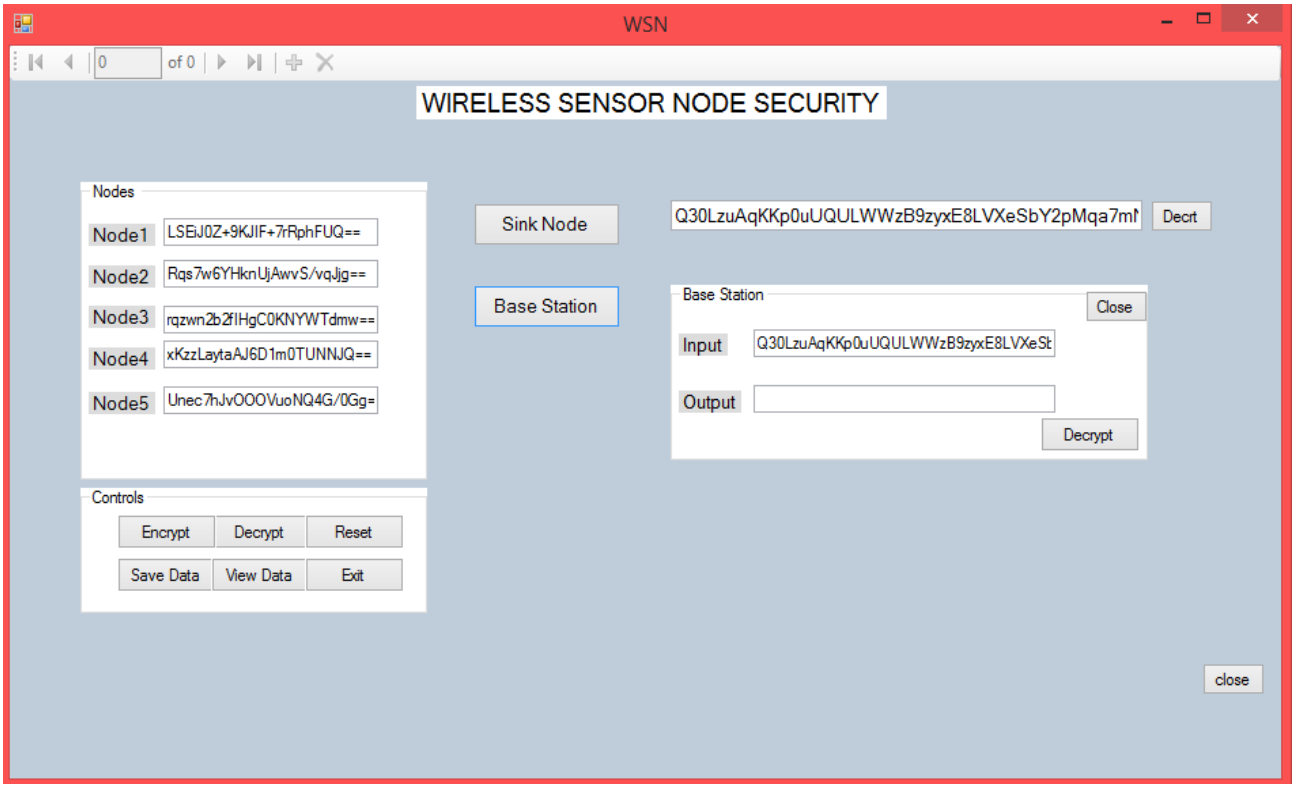

Fig 7: Encryption Simulation.

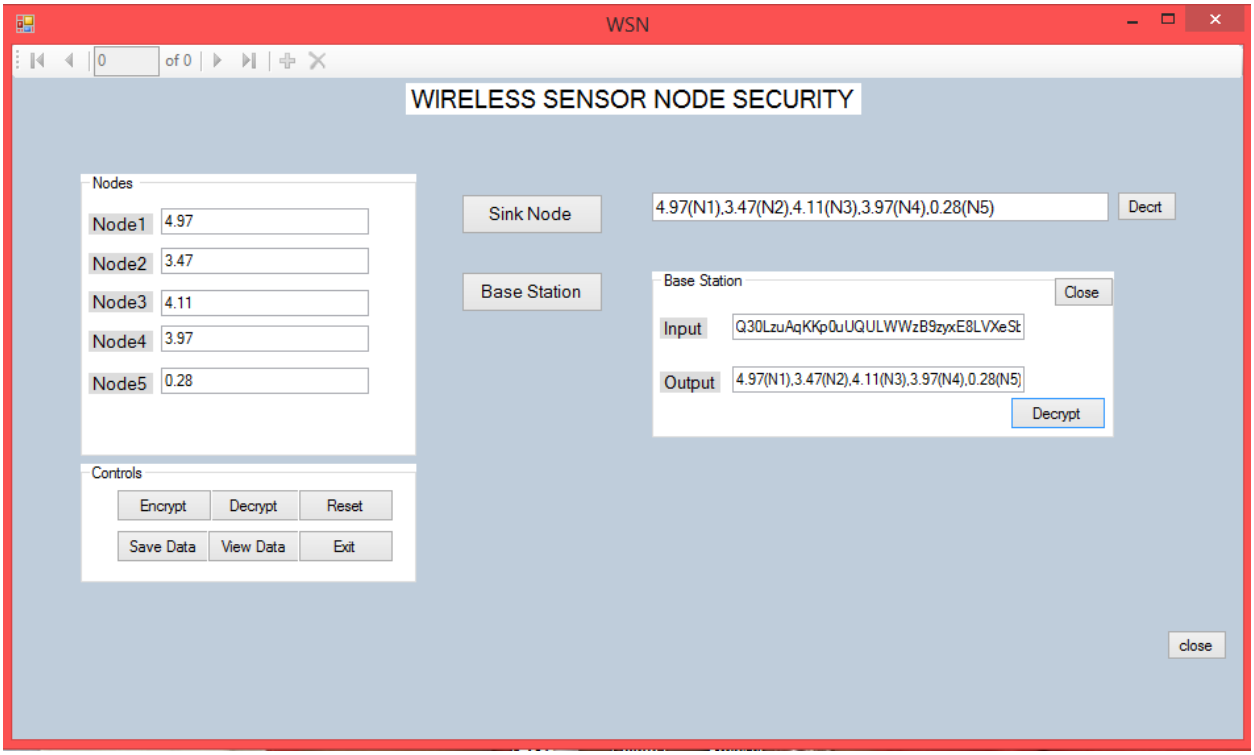

Fig 8: Decryption Simulation

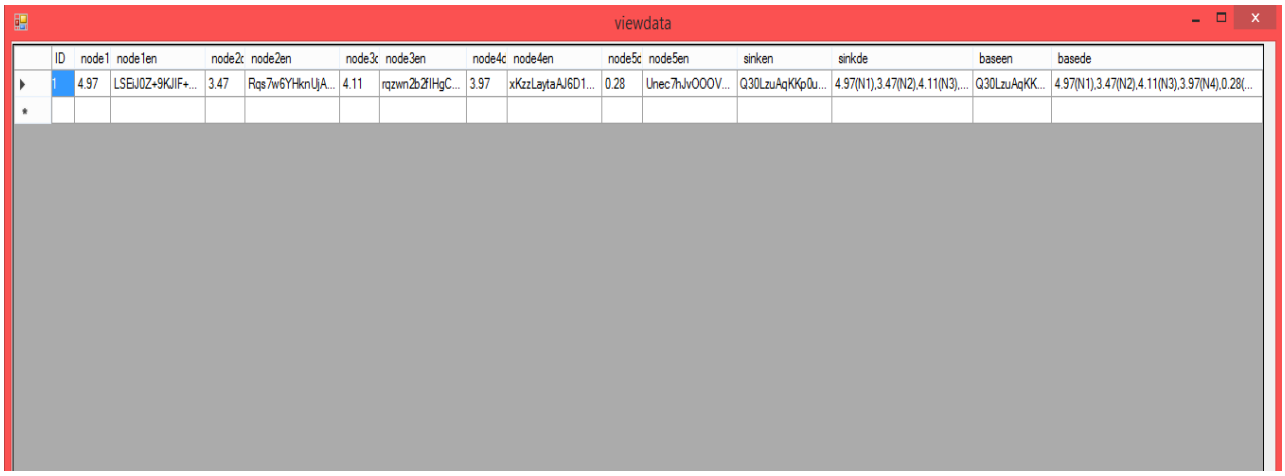

Fig 9: Database Containing Encrypted and Decrypted values.

To justify the performance of the developed algorithm, values gotten from the non-fluid flow condition experiment was simulated using the developed WSN security simulator, to show how the security was implemented in the source nodes, sink node, the base station and on the database.

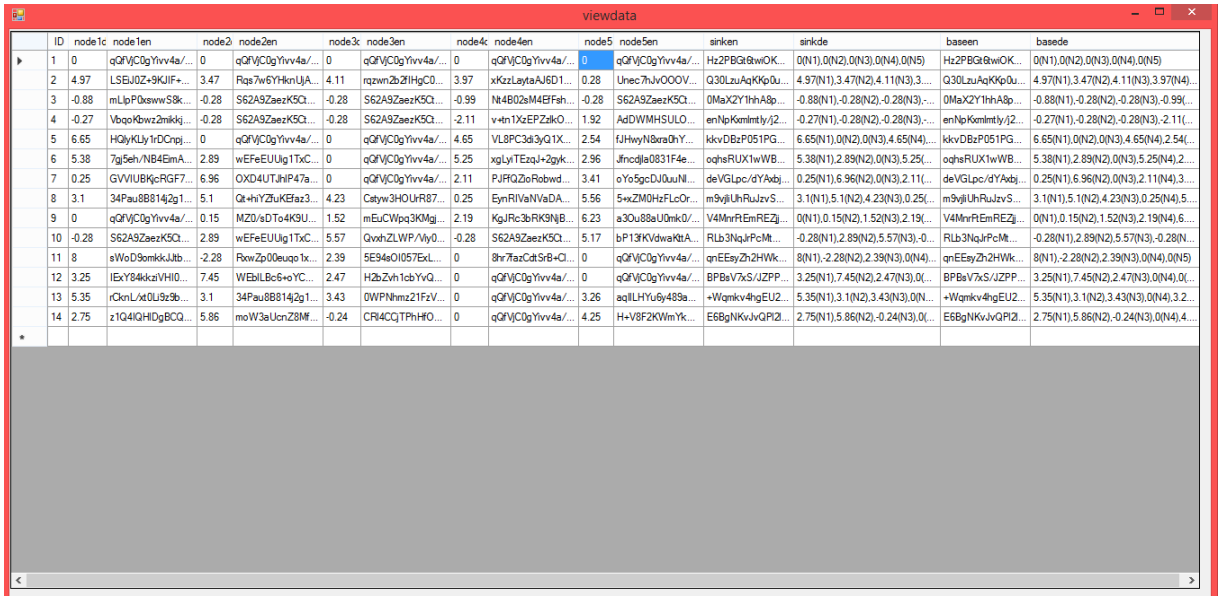

Fig 10: Database view showing the encrypted and decrypted values from table 1.

✓ *Additional security features of the software:*

1. Camouflage password access control to the base system.
2. Username and access control for database viewing.
3. The sink node discards all input in the wrong format or corrupt data, while it returns zero.

5.0 Conclusion

In this paper, development of wireless sensor network was achieved. The effect of the simulated rupture in terms of acceleration amplitude depends on the distance of the rupture point and size to the sensor location. Security management algorithm was developed and implemented on the microcontroller in such a way that data was encrypted before it was

transferred from one node to the other; the sink node has the ability to decrypt, aggregate, identify corrupt files, discard them and encrypt its aggregated output. The base station used a camouflage access control for login and a password control for accessing the database. This therefore ensures that data from the network was secured and useless to any attacker.

Future work should implement Hybrid algorithm on nodes while improving the memory size and energy requirement of the node. Also data interference on nodes security can be developed by giving the sink node additional feedback functionality, to identify interfering attacks.

References

[1] Amr Rasheed, Rabi Mahapatra. N., "The Three-Tier Security Scheme in Wireless Sensor Network with Mobile Sinks" IEEE Transactions on Parallel and Distributed system, IEEE Computer Society, VOL. 23, NO. 5, 2012, pp 958-965.

[2] Aderohunmu, F. A., "Energy Management in wireless sensor networks: Protocol Design and Evaluation". New Zealand: University of Utago, 2010.

[3] D. Suresh, K. Selvakumar, "Improving Network Lifetime and Reducing Energy Consumption in Wireless Sensor Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) 2014, page 1035-1038,.

[4] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges": Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[5] Nwalozie G.C., Azubogu A.C.O., Okafor A.C., Alagbu E., "Development of an Acceleration-based Wireless Sensor Node Platform", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2014, pp 7889-7895.

[6] Nwalozie G. C, Azubogu .A.C.O "Design and Implementation of Pipeline Monitoring System Using Acceleration-Based Wireless Sensor Network" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 9, page 2319 – 1805 September 2014.

[7] Werner-Allen. G., Johnson, J., Ruiz, M., Lees, J. and Welsh, M., "Monitoring Volcanic Eruptions With A Wireless Sensor Networking", Wireless Sensor Networks Proceedings, 2005, pp108-120

[8] Baggio, A., " Wireless Sensor Network in Precision Agriculture", In Proc. ACM Workshop on Real-world WIRELESS Sensor Networks (REALWSN 2005), Stockholm, Sweden, June 2005.

[9] Bertocco, M., Gamba, G., Sona, A., Vitturi, S., "Experimental Characterization of Wireless Sensor Networks for Industrial Applications," IEEE Trans. On Instrumentation and Measurement, Vol.57, No.8, pp.1537-1546, Aug. 2008

[10] Lee, K. B., Reichardt, M.E., "Open Standards for Homeland Security Sensor Networks," IEEE Magazine on Instrumentation and Measurement, vol.8 no.5, pp. 14-21,Dec. 2005.

[11] Dai-Hua, W., Wei-Hsin, L., "Wireless Transmission for Health Monitoring of Large Structures, "IEEE Trans. on Instrumentation and Measurement, vol.55, no.3, pp. 972-981, June 2006.

[12] Baldus, H., Klabundede, K., and Muesch, G., Reliable Set-Up of Medical Body-Sensor Networks, in Proc. EWSN 2004 Berlin, Germany, Jan.2004.

[13] Adrian Perrig, John Stankovic, and David Wagner. "Security in Wireless Sensor Networks": Commun.ACM, 47(6):53{57, 2004.

[14] Joshi, S. (2015, August 18), "What are the advantages and disadvantages of DES?",Retrieved May 28, 2017, from www.quora.com: https://www.quora.com/What-are-the-advantages-and-disadvantages-of-DES.

[15] Karthikeyan, B., & Leurent, G. (2016). On the Practical (In-) Security of 64-bit Block Ciphers Collision Attacks on HTTP over TLS and Open VPN. ACM CCS 2016, ACM CCS 2016, pp 2.

[16] Rivest, R. L. (1994). The RC5 Encryption Algorithm. Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e, (pp. 86–96).

[17] Daemen, J., & Rijmen, V. (2003, March 9), "AES Proposal: Rijndael", Retrieved February 21, 2013, from National Institute of Standards and Technology.