ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

RELIABLE DATA AGGREGATION INCLUDING SECURITY BASED ON AES AND FUNCTIONAL REPUTATION

Piyush Malviya*, Mrs. Rekha Jain, Mr. Manish Panchal
*Elex. & Telecomm Deptt., Sgsits Indore,(MP), India

DOI: 10.5281/zenodo.60118

ABSTRACT

The wireless sensor network has an important role in the field of measurement and instrumentation. The many research activities on the WSN are going on for reliable and economic data communication. One of the important aspect in the WSN is energy efficient communication. In this regards, the cluster based protocol for data communication has become a standard choice for data communication. For this protocol, data aggregation for sensor data has been used in WSN to save the energy of cluster head. Security and trust are fundamental challenges in deployment of this technique in large wireless sensor networks. In this paper, the function reputation is used to identify the trustworthiness of the node and cluster head. Along with this, advanced encryption standard (AES) is compare with conventional method for secure data transmission. The reputation value, normalized correlation coefficient and time consumption are the parameters which are used in this paper for performance analysis.

KEYWORDS: AES, Data aggregation, WSN, Reputation, trust, etc.

INTRODUCTION

The wireless sensor node is recent research area now days. WSN nodes are scattered in the area where monitoring of the object parameter is to be done. Wireless network become a common for any data communication and IEEE 802.11 is a used for wireless LAN because of its simplicity. Sensor node deployment topology is frequently changed. The various sensor nodes are connected to sink and sink may be connect over local PC or remote PC over internet for monitoring the experimental area. WSN nodes are normally once deployed as per the requirement of the object to be monitored, and battery backup power supply could not be changed after deployment. Therefore power consumption is important issue for the WSN. Physical layer plays important role for the communication process of sensor nodes.

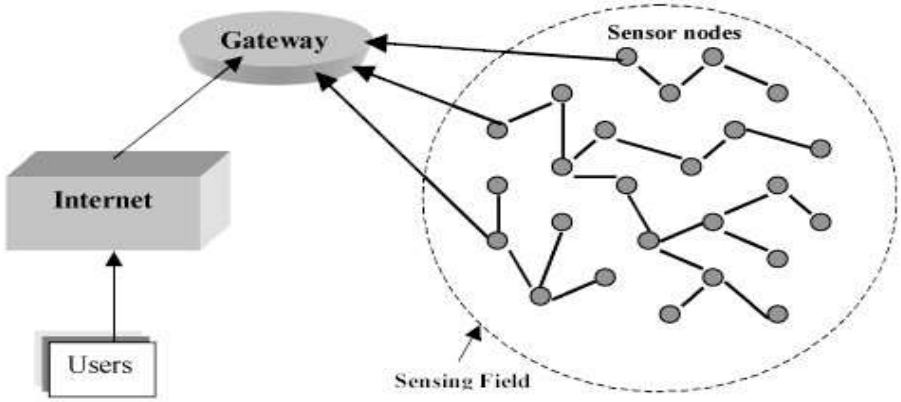


Fig: 1 Wireless sensor network architecture

A typical sensor communication architecture is shown in the figure -1 .Due to a need for robustness of monitoring, wireless sensor networks (WSN) are usually redundant. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. The important aspect of optimization has been achieved using AES and PN sequence. A brief description has been given here.

ADVANCED ENCRYPTION STANDARD (AES)

The more popular and widely adopted symmetric encryption method likely to be encountered today is the Advanced Encryption Standard algorithm. It is found that at least six times faster than triple Data Encryption Standard. A replacement for Data Encryption Standard (DES) was needed as its key size was too small. The increasing computing power, considered vulnerable against exhaustive key search attack. The triple Data Encryption Standard was designed to overcome this drawback but it was found slow.

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.
- Based on 'substitution–permutation network.
- Each of these rounds uses a different 128-bit round key,
- AES is widely adopted and supported in both hardware and software.

Operation of Advanced Encryption Standard (ASE)

Advanced Encryption Standard algorithm is an iterative rather than Feistel cipher. Comprises of a series of linked operations, some of which involve replacing inputs by specific outputs and others involve shuffling bits around.

- Interestingly, Advanced Encryption Standard performs all its computations on bytes rather than bits. Advanced Encryption Standard treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −
- The schematic of Advanced Encryption Standard structure is given in the following illustration.

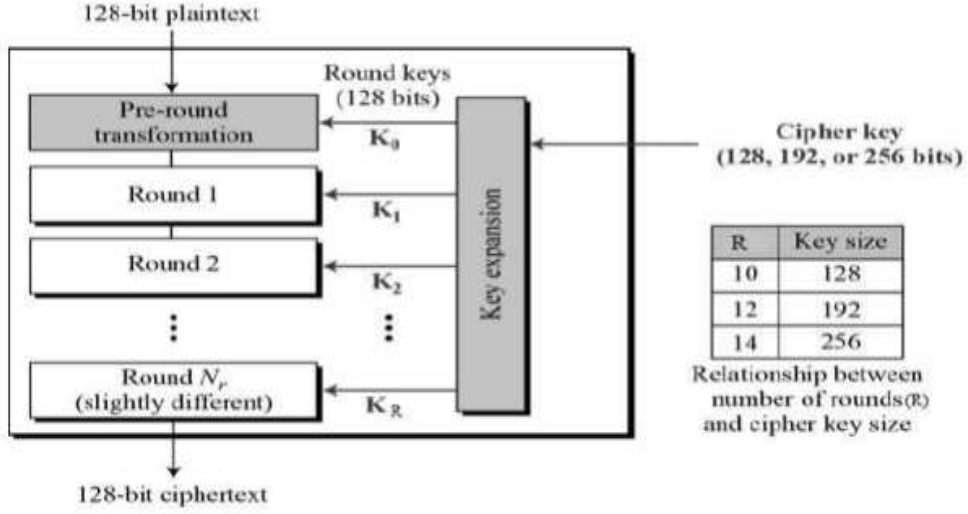


Fig: 2 The schematic of AES structure

Encryption Process

Here, we restrict to description of a typical round of Advanced Encryption Standard (AES) encryption. Each round comprise of four sub-processes.

ISSN: 2277-9655
Impact Factor: 4.116

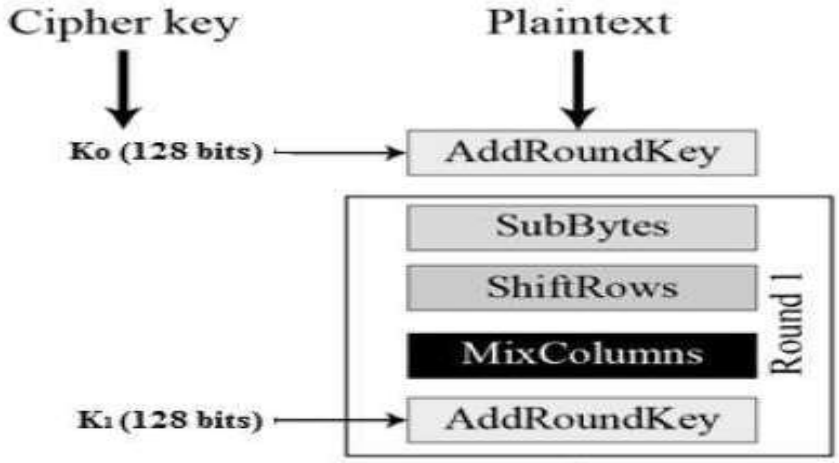


Fig:3 Encryption process architecture

PN SEQUENCE GENERATOR

- PN generator produces periodic sequence that appears to be random.
- Uses a linear-feedback shift register (LFSR).
- Output is periodic with max-period N=(2^n)-1;
- LFSR can always give a period N sequence.
- results in m-sequences

PROPOSED METHODOLOGY

In this paper, we propose a reliable data aggregation for wireless sensor networks. Initially, the aggregator nodes are chosen based on the nodes connectivity. During the data aggregation, the encryption key and the verification key is assigned to the nodes while transmitting data to the data aggregator.

- The concept of TRUST and REPUTATION is taken.
- Reputation is the trustworthiness of an entity.
- Trust is the expectation of one entity about the action of another.
- Effect of compromised nodes is mitigated using reputation system.

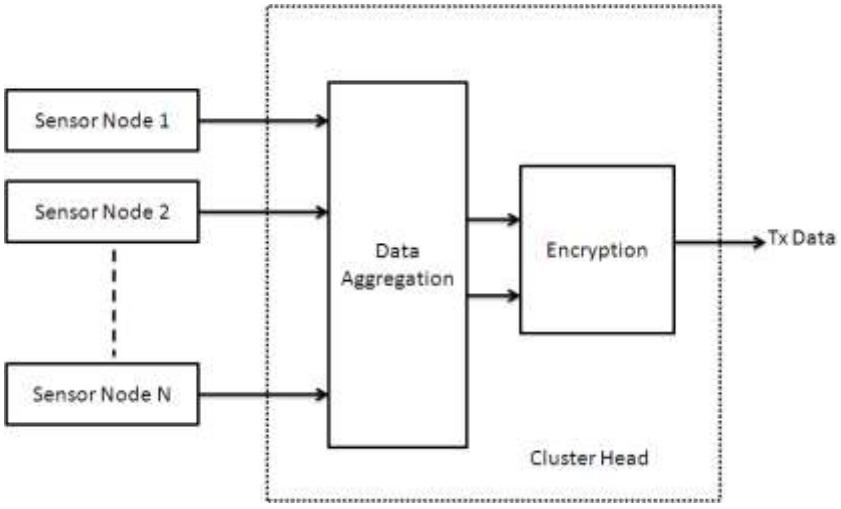


Fig: 4 System block diagram

ISSN: 2277-9655
Impact Factor: 4.116

Computing functional reputation and trust

- Functional reputation value ($R_{i,j}^{X}$) is computed using beta density function of sensor nodes.
- Trust ($T_{i,j}^{X}$) is the expected value of ($R_{i,j}^{X}$) .
- If a sensor node counts the number of good and bad routing action of α *and* β.
- then Node computes the computational($R_{i,j}^{routing}$) about aggregator node given as Beta.
- From definition of trust ($T_{i,j}^{routing}$) is calculated as the Expected value of ($R_{i,j}^{routing}$).

$$\left(T_{i,j}^{routing}\right) = \mathrm{E}\left(\mathrm{Beta}(\alpha+1, \beta+1)\right) = \alpha + 1/(\alpha+\beta+2)$$

Reliable Data aggregation (RDAT)

- Reliable Data aggregation is performed periodically.
- Aj (aggregater node) requests each Ni to send its data for data aggregation.
- Sensor node (N1,N2,… .Ni) transmit data to Aj.
- Aj updates trust values of each Ni(neighbouring node).
- Aj weights data Di of sensor node Ni using the trust. .
- Aj aggregates the weighted data to obtain Aggregated Data.

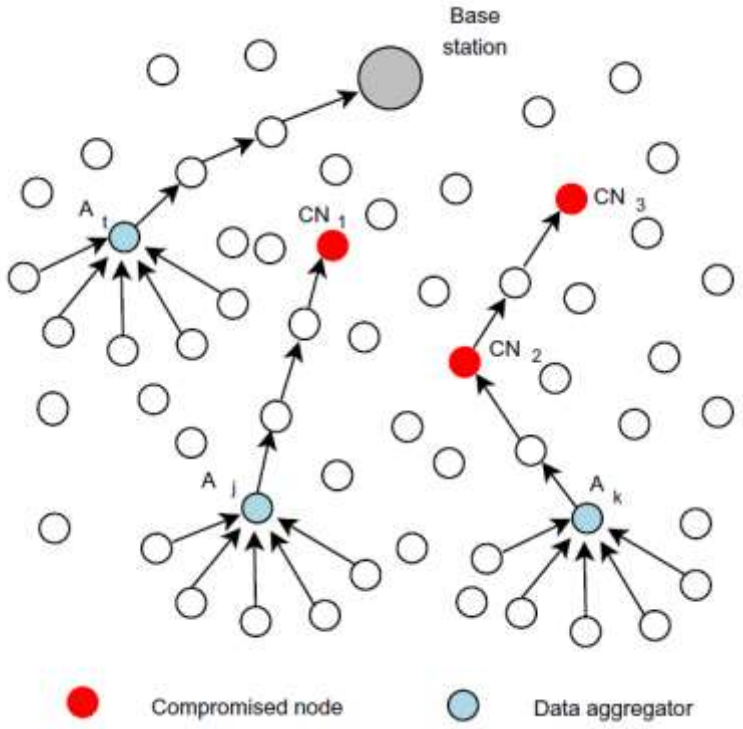


Fig: 5 General architecture of the data aggregation algorithm

RESULTS AND DISCUSSION

The simulation has been performed with the test bench developed in the MATLAB. The following parameters are used for the simulation

- No. of node – 120
- Area of simulation 1000 x 1000ss
- No. of data aggregator – 6
- No. of base station -1

ISSN: 2277-9655
Impact Factor: 4.116

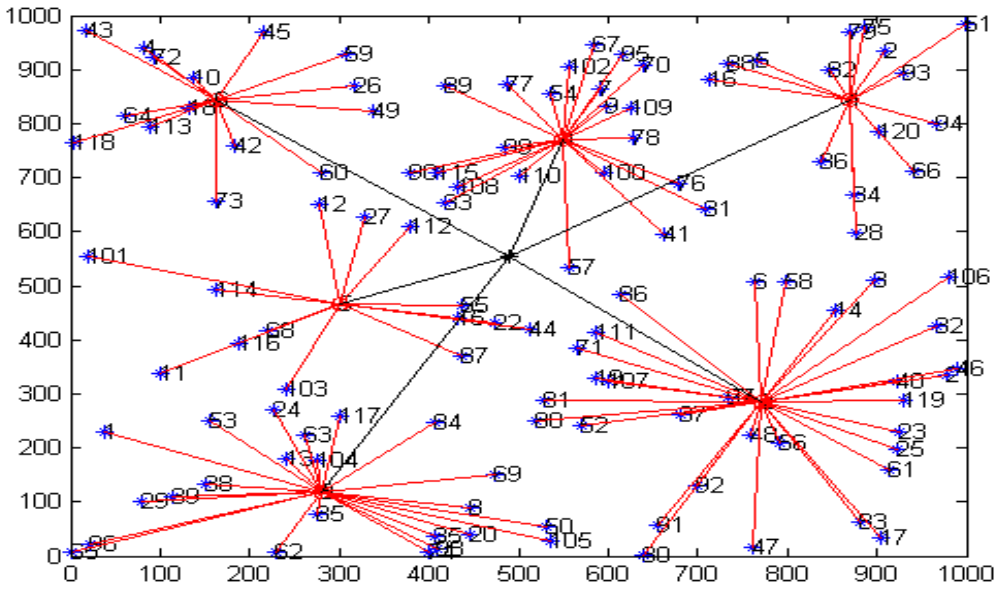


Fig: 6 Optimized values of Cost Function

The graph shows the network consists of number of nodes. The length of the network is taken as 1000*1000 meter. and the number of nodes has been taken as 120. And these nodes are placed in uniformly distributed random locations within rectangular area. These 120 nodes are divided into six clusters and each cluster has a cluster head and also each cluster consists of 19 sensors. This cluster head gathers data from the nodes resides in the cluster. This network consists a Data aggregator which aggregates data from the cluster head. The nodes are represented by "*".and cluster head is represented by "o". The information gathered is forwarded to the base station. The degree of the neighboring node is 7.

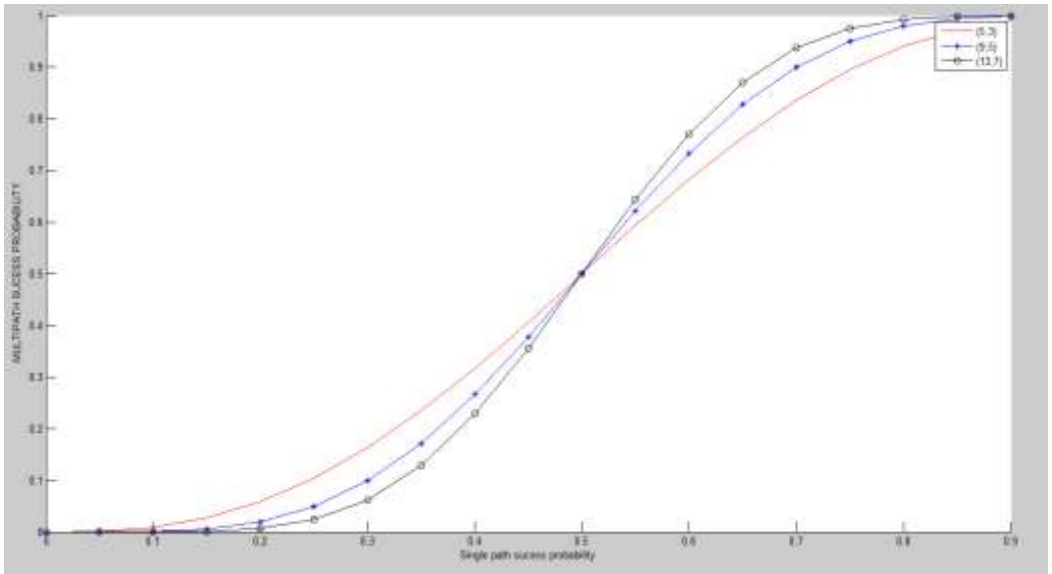


Fig:7Multipath verses single path probability

The graph above shows the multipath data transmission probability verses single path data transmission probability. If the successful data transmission probability φ_k is less than 0.5 than the success Probability of multipath routing is always lower than the corresponding single path success probability.

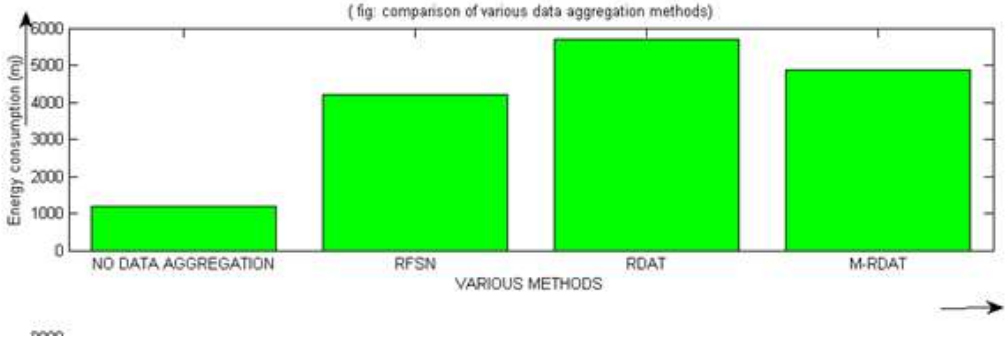


Fig: 8Average energy consumption of sensor node

This bar graph shows the comparison between various techniques. There are four types of techniques are compared named "no data aggregation", "RFSN", "RDAT", "M-RDAT". The comparison is made on the basis of energy consumption made by the aggregator node.
No. of queries – 2000
Reputation :-

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{\alpha-1}(1|-p)^{\beta-1} \quad 0 \leqslant p \leqslant 1,\ \alpha$$

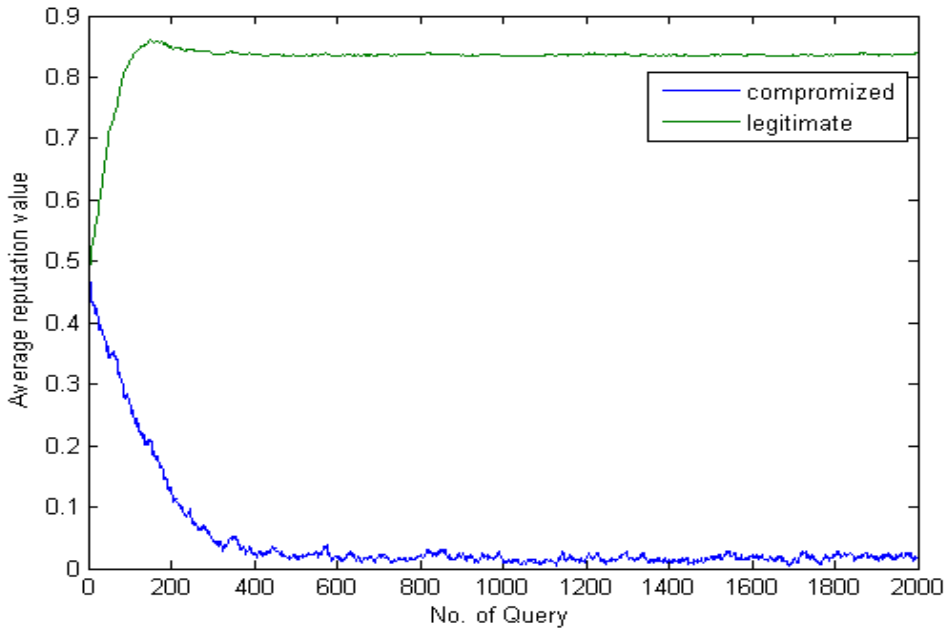
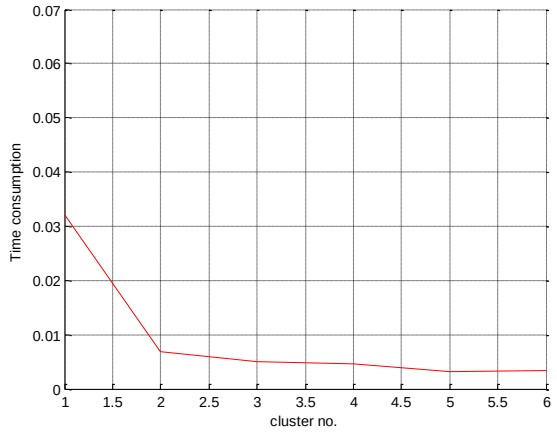


Fig:9 Compromised node and legitimate node

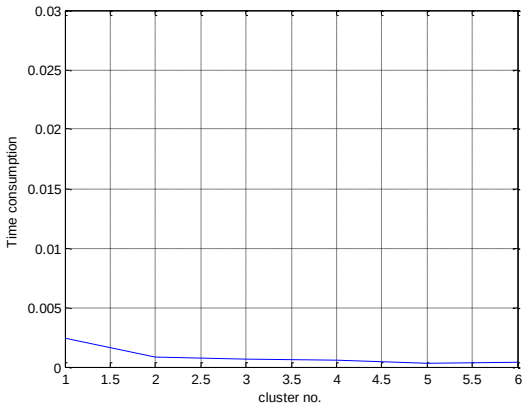
This graph shows the average reputation value of legitimate nodes and compromised nodes depends on the increasing number of queries. The simulation has been performed taking as 2000 queries initiated by the base station. As the number of queries is increased, the reputation value of the legitimate node is increased and the

ISSN: 2277-9655
Impact Factor: 4.116

reputation value of the compromised node is decreased. In the simulation 30% of the network is assumed to be compromised. The compromised node may send either false data values to data aggregator. The reputation value increases as compared to the RDAT.

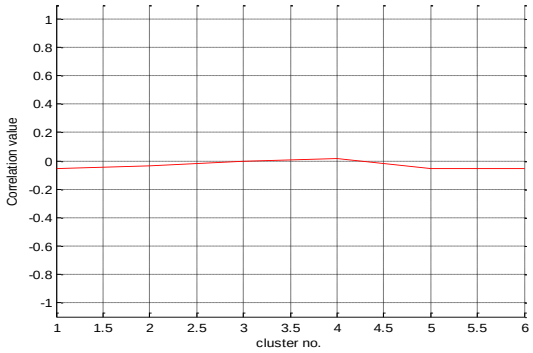


TIME CONSUMPTION OF AES

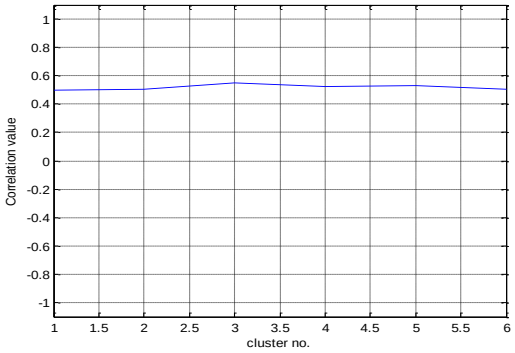


TIME CONSUMPTION PN SEQUENCE

Fig: 10Time consumption of AES Vs PN sequence encryption



AES BASED CORRELATION



PN SEQUENCE BASED CORRELATION

Fig: 11 Normalized cross correlation of AES Vs PN sequence based encryption

There are two graphs has been shown in the figure which shows the correlation of data between the original data and encrypted data. In PN sequence based encryption the energy consumption is low but for the security purpose it is not as much as reliable as AES.

CONCLUSION

The simulation setup of wireless sensor network data transmission has been performed successfully. The Data aggregation reliability has been demonstrated for no. of malicious nodes. Correlation of original data and aggregated data has also been performed .the result after simulation are highly correlated in AES as compared to PN sequence

based encryption. The AES gives better security but time consumption is high. Protocol M-RDAT improves the reliability of aggregated data by evaluating sensor nodes and data aggregators via appropriate functional reputations.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40 (8) (2002) 102–114.
[2] R. Rajagopalan, P.K. Varshney, Data aggregation techniques in sensor networks: a survey, IEEE Communications Surveys and Tutorials 8 (4) (2006),48–63.
[3] L. Xiong, L. Liu, A reputation-based trust model for peer-to-peer ecommerce communities, in: Proc. of IEEE Conference on Ecommerce,2003, p. 275.
[4] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in:Proc. of the 10th ACM Conference on Computer and Communications Security,2003, pp. 52–61.
[5] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A witness-based approach for data fusion assurance in wireless sensor networks, in: Proc. of IEEE Global Telecommunications Conference, 2003, pp. 1435–1439.
[6] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, M. Cardei, in: A. Boukerche (Ed.),Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks, Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, Wileyand Sons, 2008.
[7] P. Michiardi, R. Molva, CORE: a collaborative reputation mechanism to enforcenode cooperation in mobile ad hoc networks, in: Proc. of Communication and Multimedia Security, 2002, pp. 107–121.