Evaluation Of Functional Reputation Based Reliable Data Transmission And Aggregation For Wireless Sensor Networks

Dr. Dilip Sharma[1], Dinesh Dahima[2]

[1] *Assistant Professor, Department of Electronics and communication, Ujjain Engineering College, Ujjain, MP, India*

[2] *PG Scholar, Department of Electronics and communication, Ujjain Engineering College, Ujjain, MP, India*

---***---

Abstract - *In the field of measurement and instrumentation the wireless sensor network has an important role. One of the major vital aspects in the WSN is energy efficient communication. For this regards, the cluster based protocol for data communication has increasingly become a standard choice for the data communication. For this protocol, data aggregation for sensor data has been used in WSN to save the energy of cluster head By taken consideration of Security and trust three techniques is employed viz., AES based Encryption, decryption and DES based Encryption and Decryption. In this the paper, to identify the trustworthiness of the node and cluster head, the function reputation is used. Moreover, Advanced Encryption Standard (AES) is also compared with the conventional method for secure data transmission. The parameters which are used in this for performance analysis are the reputation value, normalized data transfer time. The simulation results show the AES provides greater security as compared to DES and TDES*

Keywords: **Reliable data aggregation, Aggregation Method, Wireless sensor networks, AES, DES, TDES**

1. INTRODUCTION

Wireless Sensor Networks (WSNs) hold the promise of enabling pervasive computing by providing nodes and networks capable of interacting with the physical environment and wireless communication with the wire line computing infrastructure [2-4]. A sensor network protocol must be highly energy efficient while being able to function securely in the presence of possible malicious nodes within the network. Data aggregation is potentially vulnerable to attackers who may inject bogus information or forge aggregated values without being detected. For instance, if a sensor close to the base station is compromised, it may claim a fake aggregation value to the base station and mislead the base station into trusting the fake information [5-8]. It may have a disastrous impact if end users respond according to the faulty information. Compromised nodes have access to cryptographic keys that are used to secure the data aggregation process. In addition, a compromised node that poses as an authorized node in the network cannot be detected using cryptography. Data outside of various sensors is aggregated by an aggregator node what in order that onward to the base station one of the aggregate values. At current, expected to constraint of the Computing power and energy resource of sensor nodes, Data is aggregated by extreme simple algorithms like balance. However, such aggregation is common to be actual available to faults, and also particularly, malicious attacks. The relevant form of optimization has been obtained using AES, DES and TDES sequence. A short summary has been given here [6-8].

1.1 Data Encryption Standard (DES)

DES is a Symmetrical Secret Key Algorithm that was promote by IBM. Algorithm uses by different banks and financial companies. Although that adaptation was formed by changing in algorithm for example Key reduced in size. **DES** is the earlier "data encryption standard"[7].

1.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard algorithm is an constant technique relatively than Festal cipher. **AES** is the replacement of DES as standard symmetric encryption algorithm for US federal organizations. AES need keys of 128, 192 or 256 bits, although, 128 bit keys transfer satisfactory strength today [7].

1.3 Triple DES (TDES)

In this approach to restate DES implementations. TDES is too slow especially in software implementations due to DES were invented as work in hardware. TDES simply enhance the key size of DES through implement the algorithm 3 times in cycle with 3 other keys. [7]

2. METHODOLOGY

We propose in Evaluate the data aggregation by a M-RDAT for WSN's. At first, the aggregator nodes are select located on the nodes relatedness. At the same time data aggregation, the encryption and authentication key is select to the nodes as long as transmitting data in the direction of data aggregator

- Perception of REPUTATION and TRUST is taken.
- Reputation is the fixedness of an object that exists.
- Trust is the anticipation of single object that exists around the response of other.

- Result of compromised nodes is check testing reputation system.

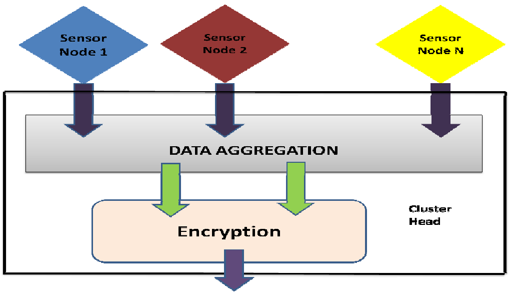


Fig -1: Data Aggregation System

2.1 Computing functional reputation and trust

By using beta density function of sensor node Nj's previous actions with respect to function X functional reputation value ($R^{X}_{i, j}$) is computed. The expected value of ($R^{X}_{i,j}$) is the Trust $T^{X}_{i,j}$. Let us take routing task as an instance. The sensor node N_i is counts the number of good and bad routing actions of N_j as α and β, respectively. Then, N_i computes the functional reputation $R^{routing}_{i,j}$ about node N_j as Beta (α +1, β +1). Following the definition of trust, $T^{routing}_{i,j}$ is calculated as the expected value of $R^{routing}_{i,j}$

$$T^{routing}_{i,j} = E(\text{beta}\ (\alpha + 1, \beta + 1) = \frac{\alpha+1}{\alpha+\beta+2} \qquad (1)$$

With the help of this equation the expected value of the beta distribution is shown as simply the fraction of events that have had outcome α. Therefore, the functional reputation value of routing is obtained as the ratio of good routing actions to total routing actions observed [10]. This is an intuitive decision which justifies the use of the beta distribution.

In the above formula, $R^{routing}_{i,j}$ represents the node N_i's observations about node N_j. In other way, it the first hand information is involved. Reputation systems that depend on only firsthand information has a very large convergence time [6-7].Thus, second hand information is required to confirm the first-hand information [5].

In the protocol RDAT, the functional reputation tables are being exchange in neighboring sensor nodes to provide second hand information which is further included in trust evaluation. Let us assume that sensor node N_i receives second hand information about node N_j from a set of N nodes and S_{info} ($r_{k,j}$) represents the second-hand information received from node N_k (k € N). N_i is already having previous observations about N_j as $\alpha_{i,j}$ and $\beta_{i,j}$. Further assume that, in a period of $\Delta t, N_i$ records $r_{i,j}$ good routing actions and similarly $s_{i,j}$ records bad routing actions of N_j. Then, N_i computes the trust $T^{routing}_{i,j}$ for N_j in following manner.

$$\left(\alpha^{routing}_{i,j}\right) v * \alpha_{i,j} + r_{i,j} + \sum_{k \epsilon N} S^{routing}_{info}\ \left(r_{k,j}\right) \qquad (2)$$

$$\left(\beta^{routing}_{i,j}\right) v * \beta_{i,j} + r_{i,j} + \sum_{k \epsilon N} S^{routing}_{info}\ \left(r_{k,j}\right) \qquad (3)$$

$$T^{routing}_{i,j} = E\left(\text{beta}\left(\alpha^{routing}_{i,j} + 1\ , \beta^{routing}_{i,j} + 1\right)\right) \qquad (4)$$

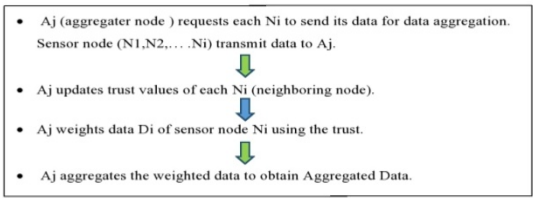
Where $v < 1$ is the aging factor that allows reputation to fade with time.

3. RELIABLE DATA AGGREGATION

In protocol RDAT, Reliable Data aggregation is performed periodically. In each data aggregation session, reliable data aggregation is obtained in two phases.

3.1First phase

Before transmitting data to data aggregators, each sensor node N_i computes $R^{aggregation}_{i,j}$ value for its data aggregator A_j and evaluates the trustworthiness of A_j. This is done in following sequence



- 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 (neighboring node).
- Aj weights data Di of sensor node Ni using the trust.
- Aj aggregates the weighted data to obtain Aggregated Data.

Fig -2: Method of Data Aggregation

3.2 Second phase

During this phase of data aggregation session, the obtained Reliable Data Aggregation (RDA) algorithm is run by data aggregators. Algorithm RDA depends on $R^{sensing}_{j,i}$ functional reputation values to mitigate the effect of compromised sensor nodes on aggregated data.

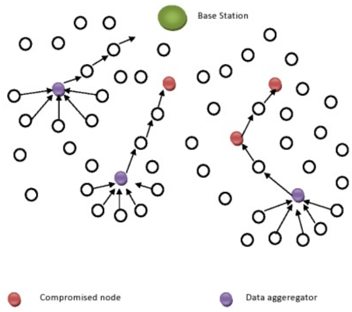


Fig -3: Architecture of data aggregation algorithm

4. RESULT AND ANALYSIS

4.1 Enhance Values of Cost Function

By the help of follow graph the network consisting of number of nodes is shown. The length of the network is taken as 1000 by 1000 meter. And the number of nodes has been taken as hundred and twenty. And these nodes are deployed in uniformly distributed random locations within given rectangular area. These Hundred and twenty nodes are further divided into six clusters and each cluster has a cluster head and also each cluster consists of nineteen sensors. This cluster head functions to gathers data from the nodes resides in the cluster. Data aggregator which aggregates data from the cluster head is present in this network. 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 Six.

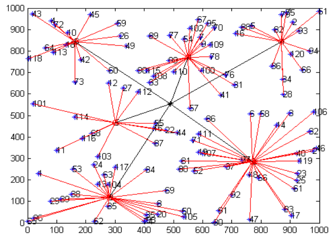


Fig -4: Enhance Values of Cost Function

4.2 Comparison for energy consumption

This bar graph shows the Various Techniques Comparison for energy consumption. There are four types of techniques are compared viz. named "no data aggregation", "RFSN", "RDAT", "M-RDAT". The comparison is purely made by taking the basis of energy consumption made by the aggregator node.

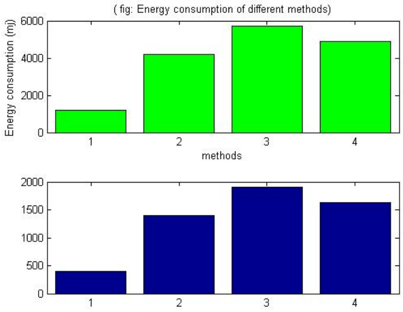


Fig -5: Comparison for energy consumption

4.3 Compromised node and Legitimate node

Graph showing the average reputation value of legitimate nodes and compromised nodes based on the increasing number of queries. The simulation has been performed by taking Two thousand queries initiated by the base station. The reputation value of the legitimate node is increased and the reputation value of the compromised node is decreased as the number of queries is increased. 30% of the network is assumed to be compromised in the simulation

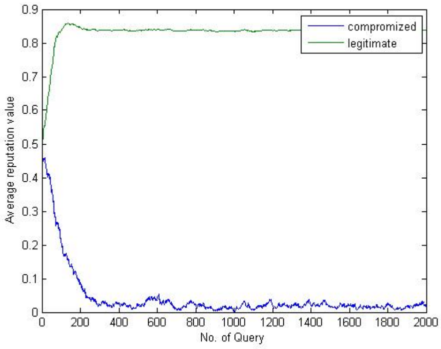


Fig -6: Legitimate node and Compromised node

4.4 Data Transfer Time

The data transfer time calculations in our conducted experiments are done, by considering the time from starting of the encryption from the first packet of a selected data file up to the decryption's end of the last encrypted packet which reaches the destination node on including End-to-End delay time. For the purpose of the computation of the transfer time the following equations were applied:

$$T_r = T_e = T_d = T_{EE} \qquad (5)$$

$$T_e \cong T_d \cong \sum_1^{Np} Ti \qquad (6)$$

$$N_p = F_s / P_s \qquad (7)$$

Where

- T_r denotes the encryption time (sec)
- T_e denotes the decryption time (sec)
- T_d denotes the End-to-End delay time (sec)
- T_{EE} denotes the number of packets in single data file
- N_p denotes the time taken to encrypt a single packet (sec)
- F_s denotes the data file size
- P_s denotes the single packet size

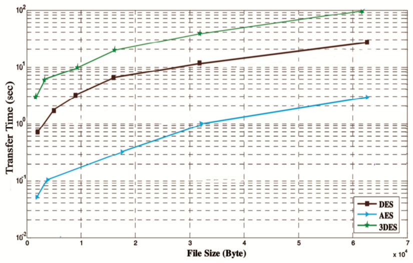
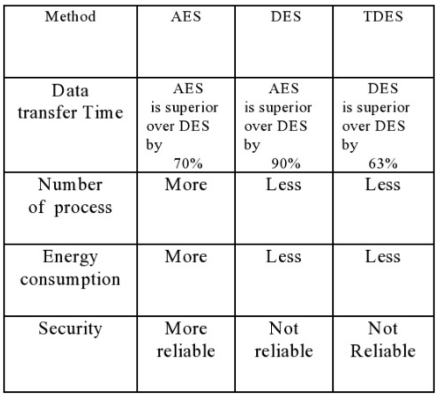


Fig-7: Encryption Transfer Time Results

Table -1: Comparison between AES and DES and TDES



Method	AES	DES	TDES
Data transfer Time	AES is superior over DES by 70%	AES is superior over DES by 90%	DES is superior over DES by 63%
Number of process	More	Less	Less
Energy consumption	More	Less	Less
Security	More reliable	Not reliable	Not Reliable

The transfer time results are shown in our study for the implemented encryption schemes.

The comparisons of AES based encryption, DES based encryption and TDES based encryption has been shown in above graph. The comparisons have been made on the basis of data transfer time in AES to the data transfer time DES and TDES. For the purpose of the security and originality of the data performed between the original data and encrypted data. With the help of experimental results we can show that transfer time for AES is approximately 90% less than the transfer time for DES encryption when running simulation in one mode. Moreover, 25% less transfer time is consumed by AES and approximately in comparison to DES encryption for small data files and (57%-80%) less than DES for larger data files.

5. CONCLUSIONS

Successfully performed the simulation setup for wireless sensor network data transmission. On no. of malicious nodes reliability of Data aggregation has been observed. The energy consumption is reduced in M-RDAT as compared to reliable data aggregation technique as early developed technique. For the security purpose AES is employed. DES and TDES based encryption is also employed to find out that the AES is better or not .In the first phase of the simulation the implementation of the network is done. In the second phase, the concept of function reputation is used increase the performance of the legitimate node and to reduce effect of the compromised node. Functional reputation has a greater advancement as compared to the existing system.

The used Protocol M-RDAT helps in improving the aggregated data reliability by evaluating sensor nodes and data aggregators by appropriate functional reputations. To analyze the security three techniques is applies, viz., AES based Encryption, decryption and DES based Encryption and Decryption. TDES based Encryption and Decryption the simulation results show the AES provides greater security as compared to DES and TDES.

REFERENCES

[1] R. Rajagopalan and P.K. Varshney, “Data aggregation techniques in sensor networks: A survey”, IEEE Communications.

[2] Tamara Pazynyuk, Jiang Zhong Li, George S. Oreku,” Reliable Data Aggregation Protocol for Wireless Sensor Networks”,IEEE2008.

[3] Hong Luo, Qi Li, Wei Guo , “RDA: Data Aggregation Protocol for WSNs”, Beijing Key Laboratory of IntelligentTelecommunications Software and Multimedia, IEEE2006.(p1-4).

[4] Dr Dilip Sharma, Dinesh Dahima: “An Efficiency & Latency based Compression of Hierarchical Network and Flat Network” International Journal on Recent and Innovation Trends in Computing and Communication 2017(p 2-3).

[5] SSasirekha, S.Swamynathan, “A Comparitive study and analysis of data aggregation technique in WSN”, ISSN 2015

[6] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao, “SDAP: A Secure Hop by Hop Data Aggregation Protocol for Sensor Networks”, Department of Computer Science & engineering, The Pennsylvania State University, ACM 2006

[7] H. C¸ am, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, and H.O. Sanli, “Energy-Efficient and secure pattern based data aggregation for wireless sensor networks”, Special Issue of Computer Communications on Sensor Networks, Feb.2006.

[8] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, “Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks”, n Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, A. Boukerche (ed.), Wiley and Sons, 2008.

[9] C. Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture forwireless sensor networks, in: Proc. of the Second ACM Conference on Embedded Networked Sensor Systems, 2004, pp. 162–175.

[10] Suat Ozdemir ,” Functional Reputation Based Data Aggregation for Wireless Sensor Networks”, IEEE International Conference on Wireless & Mobile Computing, Networking & Communication,2008

[11] H. Chan, A. Perrig, B. Przydatek, D. Song, SIA: secure information aggregation insensor networks, Journal of Computer Security (2007) 69–102.