International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

BIST Based Secure Data Aggregation in Wireless Sensor Network

Rakesh Kumar Ranjan[1], S. P. Karmore[2]

[1]M.E. Student, Wireless Communication and Computing, GHRCE, Nagpur, India

[2]Assistant Professor, Department of Computer Science and Engineering, GHRCE, Nagpur, India

Abstract: ***Number of applications, like border surveillance, under water sensor networks widely use the Wireless Sensor Network. When in network data aggregation is performed there is significant reduction in the amount of communication overhead and energy consumption in a large WSN. Various types available for data aggregation techniques are: centralized approach, In-network aggregation, tree-based approach, Cluster-based approach, Different protocol which performs secured data aggregation considered are: Secure Data Aggregation Protocol (SDAP), Secure information aggregation (SIA), Threshold security for Information aggregation in Sensor networks (THIS), Privacy-preserving Data Aggregation (PDA), Secure Encrypted-data Aggregation (SEA), Data aggregation and authentication protocol (DAA). However in all these approaches the protocol does not allow intermediate nodes to perform data aggregation thus limits the benefit of data aggregation. In this paper the new approach i.e. BIST+RC6+Aggregation is considered which will perform secured data aggregation.***

Keywords: Data aggregation, Data security, Wireless sensor network (WSN), BIST.

1. Introduction

The Wireless Sensor Networks (WSNs) should have long network lifetime as it has limited power and communication capabilities. Minimum energy consumption is primary requirement as increasing network lifetime is main aim. To achieve this goal, we study a data aggregation technique. All Wireless sensor networks have small sensor nodes which are deployed for sensing, data processing and aggregation, and communicating components. The data aggregation plays a important role in WSN to reduce energy consumption that occurs due to excessive communication.

Applications of wireless sensor network are: building monitoring, habitat monitoring, military surveillance, health monitoring and target tracking. Energy, computation, memory and limited communication capabilities are the resource constraints of WSNs.

Data aggregation is useful to improves the lifetime of nodes by eliminating redundant data transmission. The data transmission follows a multi hop fashion technique in which each node sends its data to the neighbour node nearer to sink. The existing techniques must be replaced by an improved approach using aggregation, in data aggregation techniques aggregator node select all the information from different sensor nodes and reduce the amount of communication then sends the partial result to the base station. Therefore we can reduce the energy consumption and increase the lifetime of sensors.

Security is the main issue in wireless sensor network, why we need security and how we can provide security to the sensor nodes.

Security Requirements of WSN

The security requirements of WSN are necessary because of following reasons:

- Data confidentiality – To ensure that the content of the message should not be revealed to the unauthorized receiver. Some secure data aggregation techniques provide this property in hop-by-hop basis in which any aggregator node needs to decrypt the received encrypted data before applying the aggregate function on it and then encrypt the aggregate data before transmitting it directly to the base station (BS) or to the higher level aggregator. While the other techniques provide end-to-end data confidentiality in which any aggregator node directly apply the aggregation function to the received encrypted data.
- Data integrity and freshness – Data integrity guarantees that the message has not been altered during the propagation. But if data aggregation is employed then it is not possible to have end-to-end data integrity since data aggregation yields in alteration. Data freshness protects data aggregation from reply attack.
- Source authentication – Enables sensor node to ensure the identity of the peer node that it is communicating with. A compromised node can launch Sybil attack in which it may send data under several fake identities in order to corrupt the aggregated data.
- Availability – To guarantee the survivability of network services against Denial-of-Service attacks. The attack aiming at an aggregator can make some part of the network losses its availability because the aggregator is responsible to provide the measurement of that network part.

Next section discusses the literature review that addresses the security challenges facing data aggregation in WSN.

A. Literature Review

In [8,12], the authors elaborate the secure data aggregation in large scale WSN with static nodes. They proposed a scheme called SDAP (Secure Data Aggregation Protocol) for large-scale sensor networks. Divide and conquer rule, commit and attest rules are followed in the secure data aggregation. Aggregation trees are the main component of this scheme. Aggregation trees are divided into groups to reduce high importance level nodes in the tree. This is also called hop by hop aggregation technique. This reduces energy consumption and communication overhead. The problem arises when a node is compromised, which adds fake value in the aggregation data. So, a base station is required to monitor aggregation data. Group aggregate (sub tree aggregate) is formed hope by hope. Every group is then attested if suspicious aggregation value is found. The simulation performed by authors proves its efficiency like other existing protocols while the security is enhanced using SDAP.

Przydatek [13] proposed a secure information aggregation (SIA) which provides a statistical security property under the assumption of a single aggregator. The goal is to prevent stealthy attacks. If a reported aggregation result is close to a true aggregation value with high probability then the home server will accept the reported aggregation result, otherwise the home server will reject it.

Vu [9] proposed Threshold security for Information aggregation in Sensor networks (THIS). For data aggregation, each sensor node compares its reading with an aggregated value produced from the aggregator. If close enough, the sensor node replies to the aggregator with its signature; otherwise the sensor node ignores replying. The aggregator collects, and sends the aggregation values and all signatures to the base station. The base station receives the message containing the aggregation value and signatures. If the number of signatures is less than the threshold; the base station discards this message.

The author [10] proposed Privacy-preserving Data Aggregation (PDA) in Wireless Sensor Networks. The algorithm that performs eavesdropping data performs defence against the attacker. By slicing it into pieces each node hides its private data. It sends encrypted data slices to different intermediate aggregators. After the pieces are received, intermediate nodes calculate intermediate aggregate values and further aggregate them to the base station.

The authors in [11] classify the secure data aggregation techniques without decrypting the data and hence the data is not available to aggregators. This paper focuses on security and privacy of the information in mobile WSNs (MWSN). Secure Encrypted-data Aggregation (SEA) scheme in MWSN is proposed. Duplicate instances of original reading are stored in packet in order to save energy. If the received data on sensor's end are the same then the aggregators does not need to perform decryption of the data. The aggregators do not have decryption keys and so the aggregators have no information about data of WSNs. Random keys are used for encryption to avoid plaintext attacks, chosen-plaintext attacks, cipher text only attacks, and man-in-the-middle attacks.

Jakhar and Nandal [6] have introduced a secure data aggregation approach in WSN using Artificial Neural Network (ANN).Their approach has also incorporated false data detection with data aggregation and confidentiality. Thus, their approach is termed as DAA protocol. Their model is represented as nonlinear sensor model, where nodes are distributed dynamically. Faults in data packets are identified through NN-based scheme. DAA scheme has utilised new structure of a back propagation-type Neural Network (NN) in recurrent NNs.

Strength of this approach: NN provides the high accuracy and lifetime of sensor nodes can be increased with the back propagation type NN.

Weakness of this approach: The process of back propagation in NN induced overhead. Further, their approach has not considered routing.

B. Contribution

All the existing approaches mentioned above deals with secure data aggregation by considering static node in WSN and few has considered for dynamic node data aggregation in WSN. However in all these approaches the protocols do not allow intermediate nodes to perform data aggregation thus limits the benefit of data aggregation. In this paper the new approach i.e. BIST+RC6+Aggregation, (BIST stands for built-in self test) is considered which will perform secured data aggregation.

C. Organization of the Paper

The rest of the paper is organized as follows. In section II, discusses preliminaries to understand the proposed protocol. In section III, methodology for WSN. In section IV scenario of WSN is described. In section V the result are described with the help of snapshots. In section VI concludes the topic followed by the references.

2. Preliminaries

In this section we describe some preliminaries and properties as our existing researches that are useful to understand our proposed technique.

When sensor node dead or not secure because of any reason than that sensor node continuously sends repeated data to the BS.

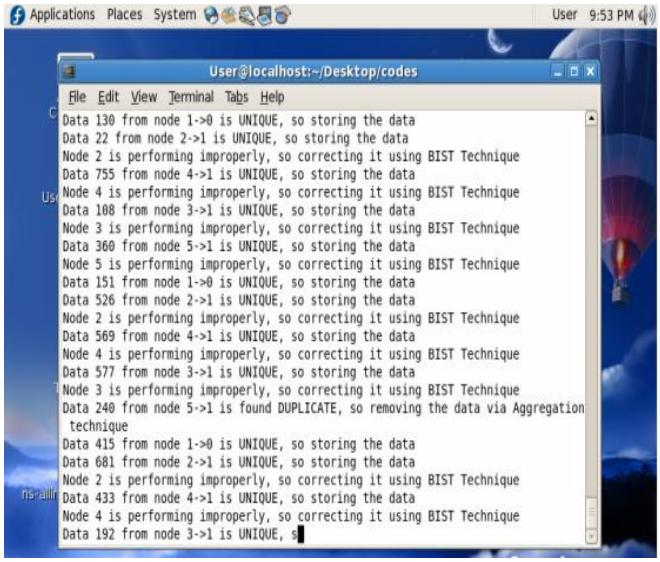

Figure 1: Working of algorithm

In figure (1) shows the working of our algorithm.

When we apply our algorithm (BIST+RC6+Aggregation) to the network first of all it checks data what is coming from nodes and follow given steps:

- If the data is unique then store that data.
- If the data is found duplicate then removes the data via Aggregation technique.
- If node is performing improperly then correcting it using BIST technique.
- It Protect to compromise from the attacker and gives the security using RC6 Algorithm.
- Using Aggregation techniques the life of node will increase.

3. Methodology

The following model to be constructed aims to aggregate data of sensor nodes to the BS through aggregator node. The model consists of three steps in one step we apply aggregation techniques, in second step we apply Built-in self test (BIST) and in third step we apply RC-6 for secure transmission. The corresponding algorithms in the respective mode will be described and related results are obtained. Thus, we describe the plan of project work as shown in Figure (2).

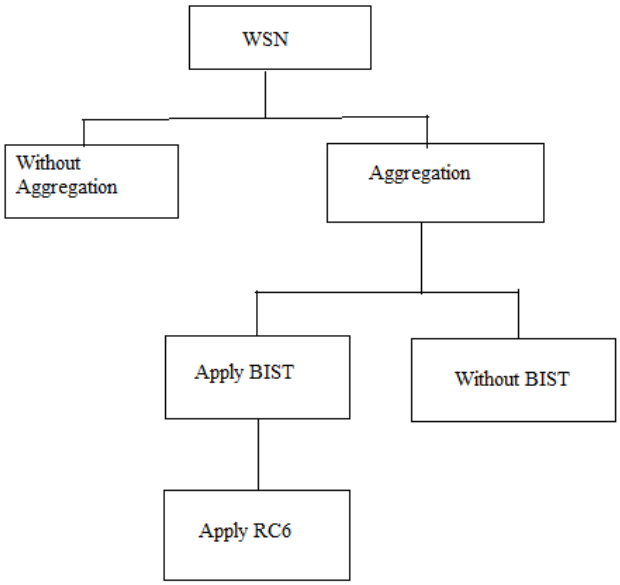

Figure 2: Stages of the work

4. Scenario of WSN

Figure (3) shows the scenario of Wireless Sensor Network (WSN), where a lot of sensor nodes are deployed randomly. In WSN sensor nodes are deployed for different purpose. Each Sensor node collect data and forward it directly to the Base Station (BS), but in aggregation technique there is one aggregator node between all nodes, in this techniques all nodes forward its data to the aggregator node then aggregator node forward partial result to the BS.

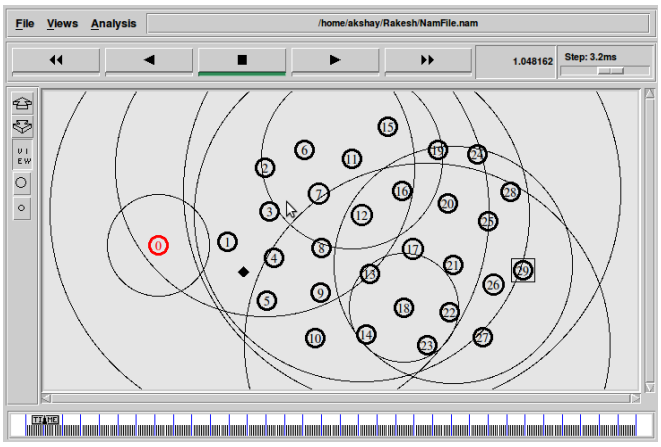

Figure 3: Scenario of WSN

In the figure (3) node0 acts as BS and node1 acts as a aggregator node. When we will not apply aggregation techniques in WSN then data fall will be more as shown in figure(4). Where Black Square shows the data fall and small arrow shows the data transmission toward the aggregator node.

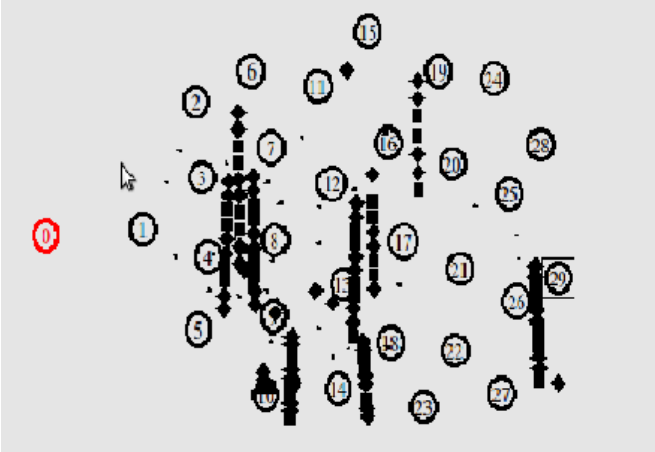

Figure 4: Without Aggregation

When we will apply aggregation techniques in WSN then data fall will be less as compare to without aggregation, this is shown in figure(5). Where aggregator node1 collect data from several nodes and forward partial result to the BS node0.

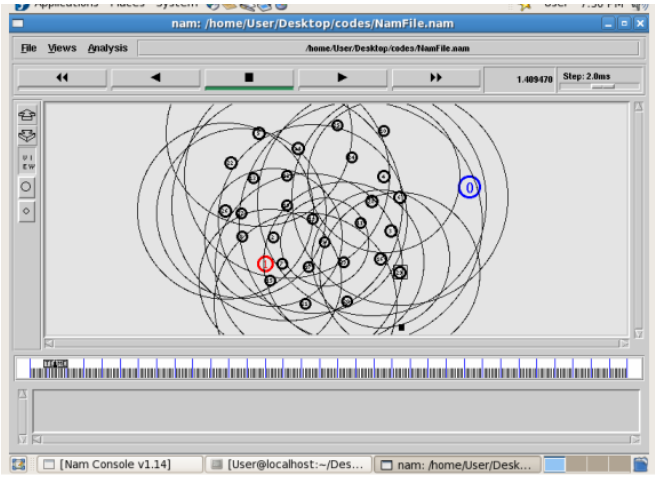

Figure 5: After Aggregation

5. Result

In-network data aggregation techniques aggregator node reduces the amount of communication and hence the energy consumed, especially in large WSNs. The main function is to perform partial data aggregation at intermediate nodes. In figure(6) it is shown that Initially when the network is performing normal communication in that case the energy of both the network is same but after nodes start failing the network energy goes on increasing in normal case while it remain almost constant in our algorithm (BIST+ RC6+Aggregation). Red line shows in normal case when aggregation had not applied, and green line shows reduce energy consumed.

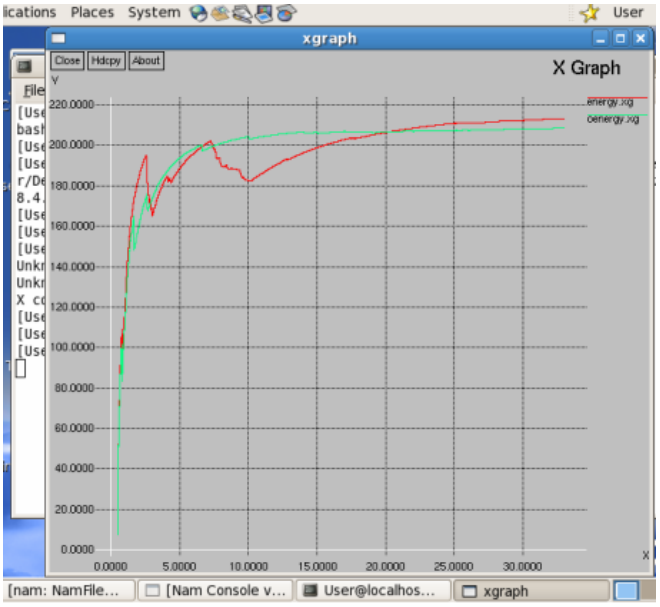

Figure 6: Energy Graph

Our algorithm (BIST+ RC6+Aggregation) is secure for communication but when we apply this algorithm in WSN the network will take more time for communication. Figure (6) shows the delay in communication red line is in normal case and green line is in our case.

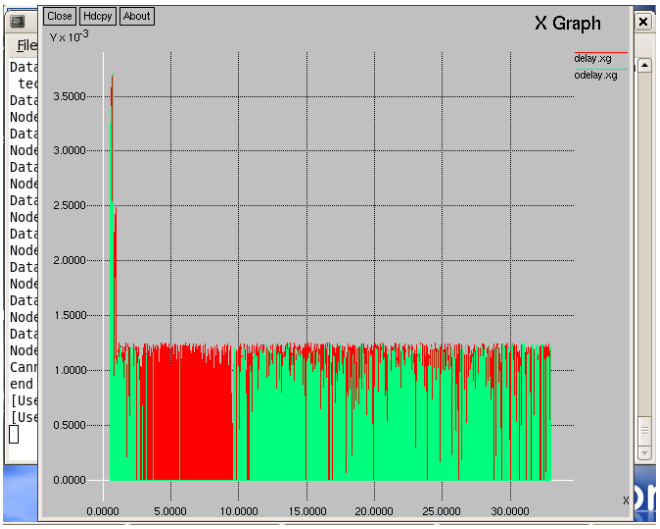

Figure 7: Delay Graph

When we apply our algorithm in WSN the Packet delivery ratio (PDR) will be maximize. Figure (8) shows the PDR graph where red line in normal case and green line in our case.

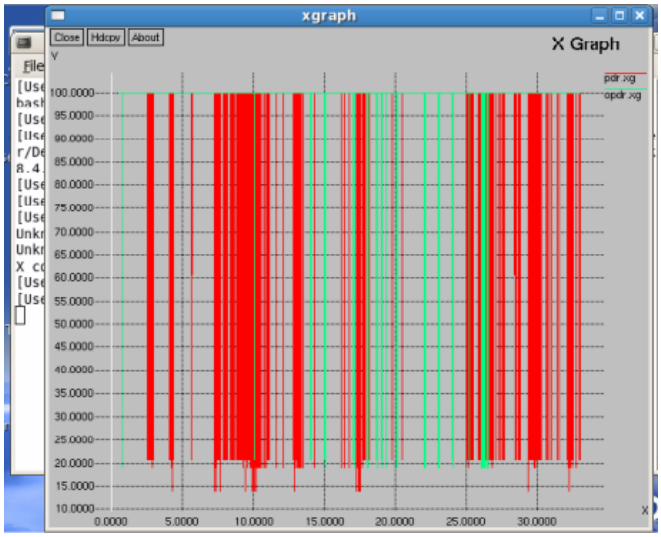

Figure 8: PDR Graph

6. Conclusion

This proposed BIST+RC6+Aggregation approach will detect the weak sensor node in the WSN network after that this approach will provide security only that node which is weak. Using this approach the sensors lifetime will be increased and nodes will be more secure.

References

[1] Sankardas Roy, Member, IEEE, Mauro Conti, Member, IEEE, Sanjeev Setia, and Sushil Jajodia, Fellow, IEEE, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions on information forensics and security, vol. 9, no. 4, april 2014.

[2] Sk Md Mizanur Rahman, Mohammad Anwar Hossain, Maqsood Mahmud, Muhammad Imran Chaudry, Ahmad Almogren, Mohammed Alnuem, Atif Alamri. "A lightweight Secure Data Aggregation Technique for Wireless Sensor Network",IEEE International Symposium on Multimedia-2014.

[3] Mohsen Rezvani, Student Member, IEEE, Aleksandar Ignjatovic, Elisa Bertino, Fellow, IEEE and Sanjay Jha, Senior Member, IEEE, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions on Dependable and Secure Computing (TDSC)2014.

[4] Triana Mugia Rahayu, Sang-Gon Lee*, Hoon-Jae Lee"Security Analysis of Secure Data Aggregation Protocols in Wireless Sensor Networks" 16th International Conference on advanced Communication Technology (ICACT)2014

[5] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef "Secure Data Aggregation in Wireless Sensor Networks" 12th Annual Mediterranean Ad Hoc Networking Workshop(MED-HOC-NET) IEEE 2013.

[6] Jakar, N.,Nandal, R.: "A secure data aggregation approach in WSN Using ANN", Int. J. Res. Eng. Appl. Sci., 2012, 2,(2), pp. 2249-3905.

[7] Anuparp Boonsongsrikul, Kyung-suk Lhee and ManPyo Hong, "Securing Data Aggregation against False Data Injection in Wireless Sensor Networks", Feb. 7-10, 2010.

[8] Y. Yang, X. Wang, and S. Zhu, "SDAP : A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," 2006

[9] S. Huang, "SEA: Secure Encrypted-Data Aggregation in Mobile WSNs," pp. 848–852, 2007.

[10] H. Vu, N. Mittal, and S. Venkatesan, "THIS: THreshold security for Information aggregation in Sensor networks." International Conference on Information Technology (ITNG'07), IEEE, 2007, pp. 89-95.

[11] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks." IEEE INFOCOM 2007 proceedings, 2007, pp. 2045-2053.

[12] S. Huang, "SEA: Secure Encrypted-Data Aggregation in Mobile WSNs," pp. 848–852, 2007.

[13] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by- Hop Data Aggregation Protocol for Sensor Networks." the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'06), 2006, pp. 356-367.

[14] B.Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks." In Proceedings of the 1stinternational conference on SenSys' 03, ACM, 2003, pp. 255-265.

Author Profile

Rakesh Kumar Ranjan received the B.E degree from RTMNU and corrently persuing ME in Wireless Communication and Computing from G.H.Raisoni College of Engineering. Recently student in G.H.Raisoni College of Engineering.