Energy Efficient Method in Wireless Sensor Network for Securing Compromised Data Aggregation against the Collusion Attack

Jagtap Anagha M.
Department Of Computer Engineering
JSCOE, Pune, India

Ingle Madhav D.
Department Of Computer Engineering,
JSCOE, Pune, India

ABSTRACT

Due to sensors storage capacity limit, communication bandwidth and computation ability WSN has some limitations. Due to this limited resources the amount of data transmission in network should be reduced. Data aggregation is new method for the above purpose. From the present algorithms for data aggregation the efficient is Iterative Filtering (IF) algorithm, which provides trust evaluation to the various sources from where the data aggregation is done. Trust assessment is given as weights, to cure the vulnerability of the fundamental averaging aggregation strategy to the attacks.Iterative filtering algorithms are stronger than the straightforward averaging procedure but they are not competent to deal with the novel advanced attack which exploits the false information through number of compromised nodes. Iterative filtering is improved to oversee novel complex attack by initial trust estimate, which increases the robustness and preciseness of the IF algorithm.Present system considers attack only on cluster members and not on aggregator.The information is transferred to aggregator by cluster members, and at last to the base station, in this process if attack happens on aggregator, present system gets fails.This problem is discovered by considering attacks on both cluster members as well as on aggregator.The aggregator selection method is proposed which elects new aggregator depending upon maximum remaining energy and distance to the base station, when an attack is detected on aggregator. This makes the system more robust against the compromised aggregator node also it saves time and energy compared to the existing system.

General Terms

Wireless sensor networks, Security.

Keywords

Wireless Sensor Networks, Data Aggregation, Iterative Filtering, Collusion Attack, Trust, Reputation.

1. INTRODUCTION

A wireless sensor network includes a large number of low powered, low-cost sensing devices with restricted calculations, memory and communication resources. WSN is known as an exceptional class of ad hoc wireless network. Remote sensor network has some number of sensor nodes, those are scattered in an objective of identifying their physical or environmental conditions, Collects data and processes it. Mobile nodes are embedded with basic processor, application specific sensors, wireless transceiver and low battery. Data aggregation is utilized to decrease the transportation overhead because of finite amount of power in sensor nodes.

In the data aggregation method, the data of sensor nodes is consolidated at cluster head nodes and then transmitted thataggregated data to the base station.Data aggregation approach includes gathering of data and making information accessible to the base station in energy profitable manner. Fundamentally, based on topology, data aggregation protocols can be classified into tree based and cluster based protocols. In tree based data aggregation, data flows from leaf nodes (child nodes) to the upper level nodes (parent nodes) wherein aggregation is performed at the parent nodes. In case of cluster based aggregation, groups of nodes are formed which are called as clusters. Cluster head also called as aggregator performs data aggregation by gathering information from cluster members and then sends it to base station.

Sensor nodes have restricted to computation power, battery, and small storage capacity. Since of every of these limitations, there is a need of reducing the amount of data transportation so as to save such assets. This can be possible by utilizing the effective procedure called data aggregation. Information from various sensors is aggregated at one node called as aggregator, which then conveys theaggregated data with base station. Averaging is the simplest algorithm which is utilized for data aggregation. What's more, it is effective by considering the restrictions of sensor nodes. But such aggregation is vulnerable to faults i.e. with averaging algorithm adversary could easily attack on WSN without taking much effort. This can't be cure even by utilizing cryptographic strategies such as encryption decryption. This is because the compromised sensor node is totally under control of adversary and adversary could get to each data stored on node. Consequently more knowledgeable algorithm is required for performing data aggregation. For giving security with data aggregation, concept of trust appraisal to information from sensor node can be utilized.

Iterative Filtering (IF) algorithms can be utilized for the same purpose. It utilizes a single iterative method and gives solution for the issues, data aggregation and trust assessment. The dependability of every sensor is evaluated by taking into account the distance of sensor readings from the correct estimate values got in the preceding iteration of round as in the form of aggregation which is made of all sensors evaluations. Such data aggregation is typically a weighted average. Sensor readings are fundamentally varied from such estimate. So the sensors are considered as less dependability furthermore in the aggregation process, their readings are assigned with the lower weight in the present round of iteration.

For wireless sensor network, theWagner's proposed dynamic nodes model is considered, inwhich, clusters of nodesare formed and allcluster heads of formed clusters behaves asan aggregator. Information are intermittentlygathered and added up by the aggregator. It is expected that the collector itself not to be compromiseand focus on algorithm which make aggregationsecure even in the case when individualsensor nodes might be compromised and maybe sending false information to the aggregator.Every data aggregator must have sufficientcomputational power to run an IF algorithmwhich used for data collection.

2. RELATED WORK

In this paper [1], author introduces a new attack which is known as sophisticated collusionattack in contrast to existing IF algorithms.Advancement is contributed over the existingIterative filtering algorithm by giving initial approximation of trust, which makes existingalgorithm more factual, robust and faster converging.Limitation of the approach is it does not detect and protect compromised aggregators.Author tried to implement approach in adeployed sensor network.

Author proposed [2] a reputation algorithmwhich is based on correlation model and used in web based rating system to solve the rankingproblem that can be generated by the influenceof spammer attack. Author represents user'sreputation by using correlation coefficient and iterative method to find the similarity between users rating vector and objects weighted averagerating vector. Proposed algorithm is moreefficient and robust but still the exactness ofalgorithm can be improved.

Author introduced [3] an"Iterative Trustand Reputation Management Scheme" (ITRM)which is a strong system to estimate the reputationof the service provider and level of truston the ratters. Author proposes the central commandthat gathers reports and generates theprovider's reputation based on the obtainedratings from consumers. Outcome of the comparisonof proposed scheme and existing reputationcontrolling schemes shows that proposed scheme is more efficient and powerful to detect malicious ratings and to compute reputation ofprovider in less time in the existence of attack.

This paper presents [4], bipartite rating networks, which have two types of entities namely users and the objects. A user gives ratings to the objects. Ranking of the objects, based on user's ratings is the main challenge in bipartite rating networks. Existing algorithms are eithernot robust against spammers attack or notguarantee convergence. Author has introduced six new reputation-based ranking algorithms. For calculating user's reputation values, author has consideredthe outcome of aggregated difference between user's ratings and object's ranking. Author has reported proposed algorithms as more effective, powerful and efficient with the practical evaluation of it on three real datasets.

In this paper [5], author has proposed the game theoretic defence policy in order to secure sensor nodes and to assure high level of trust on nodes. The proposed policy is dependent on stackelberg competition which assumes that the attacker has limit on number of attacks. The proposed policy ensures that numbers of sensor nodes are protected in each attack iterations. This approach overcomes the issue of sensor data trustworthiness and protects sensor network from various malicious attacks in effective and efficient way.

Author proposed a framework [6], called RFSN, in which each sensor node maintains the reputation for each other node in a network, based on which the trustworthiness is calculated. The framework also considers the limitations of the sensor nodes. Within RSFN, a beta reputation system is established which uses Bayesian formulation to estimate the trustworthiness of sensor nodes. RFSN gives the approach to detect all misdeed resulted from malicious and faulty sensors in a network. It also integrates various solutions of security.

This paper proposed [7] a technique called Sensor Rank by investigating Markov Chain in the network. Faulty readings greatly affect accuracy of the query results in wireless sensor networks. A correlation network gives source of Sensor Rank for sensor nodes in the network. Trust Voting algorithm is proposed to overcome the faulty readings in case of Sensor Rank.

Author proposed [8] probabilistic algorithm for cluster formation named as LEACH. LEACH selects the cluster head by random number generation. Cluster gets formed based on the nearest distance, i.e. other nodes get added in cluster whose cluster head is nearest to it. LEACH uses one hop conversation. It emphatically manages the energy utilization in the WSN.

3. PROBLEM DEFINITION

Energy is the most important aspect in wireless sensor network. The existing system has a problem of energy depletion at particular node which generates cuts in the network that results in decreased network lifetime. The main problem with previous system is that they are randomly selecting aggregator in each cluster. The main role of aggregator is to communicate with each member of cluster and perform the aggregation of all the data. So it is obvious that more energy is consumed at that node. Hence to overcome this problem aggregator node is elected based on maximum energy from each cluster. Because of this low power performance of aggregator occurs in network. The aggregator is more likely to be attacked because it has all the data from the cluster which is not addressed in existing system. So the proposed system incorporates a technique that performs data authentication to detect attacker. Thus system built is electing another aggregator node. Hence authenticated data is securely received at base station.

4. WORK OF EXISTING SYSTEM

The existing system works on the collusion attack in contrast to already available IF algorithms. The system proposes recognizable proof of a refined collusion attack in contrast to IF based reputation frameworks which exposes serious susceptibilities of present IF algorithms. Existing system introduced a technique for evaluation of node errors which is efficient in an extensive variety of node deficiencies also, not vulnerable to the depicted attack.The existing system detects attack only on cluster members and the cluster head selection is done randomly. Existing system mainly concentrated on collusion attacks of cluster member in wireless sensor network. As data is outsourced through cluster member to aggregator to base station, if in case attack occurs on aggregator then existing system gets fail.

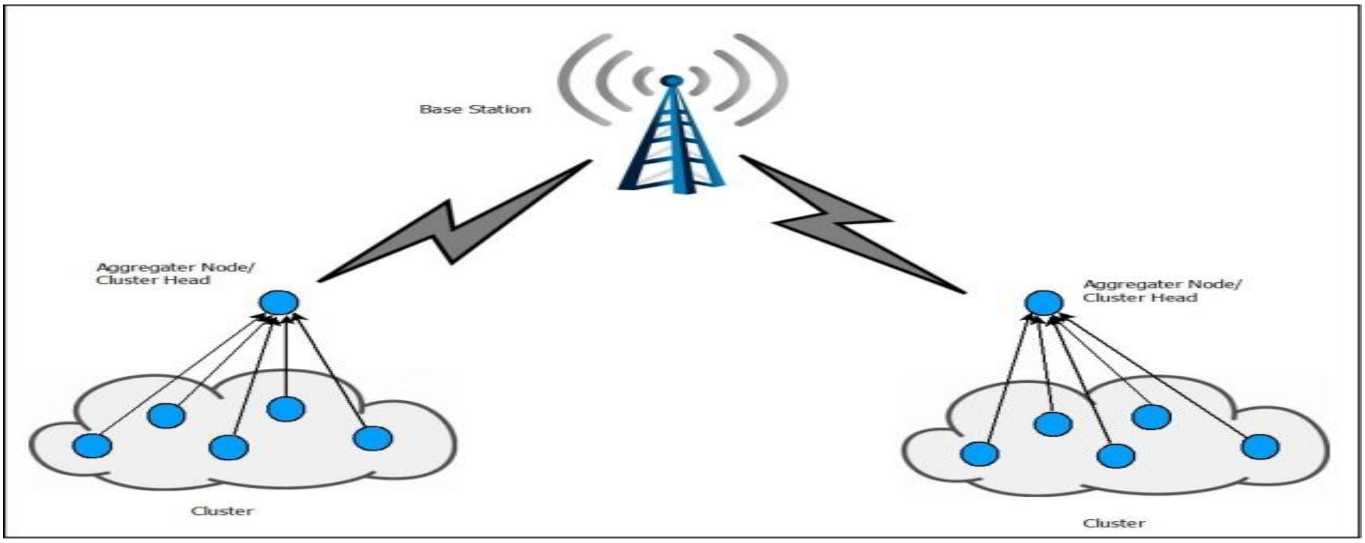

Fig. 1 Existing System Architecture [1]

5. WORK OF PROPOSED SYSTEM

The nodes of network are partitioned into disjoint groups, and every group has a head which is known as an aggregator or cluster head. Information are intermittently gathered and aggregated by the cluster head. In the proposed system the reality is accepted that the aggregator node can be compromised in the same way as that of cluster members. Compromised aggregator may send false aggregated values to the base station. Hence a technique is introduced in propose work that can detect attack on cluster memberwith the help of Iterative filtering algorithm as well as on aggregator using hashing technique. This also includes a protocol for electing a newaggregator on detecting attack over it. With the introduction of this, the expectoration of increase in security and energy efficiency of the WSN is fulfilled. Fig.2 shows the system architecture.

System is divided into number of stepswhich are described as follows:

- Generation of Network: Generation of sensor nodes network is performed here. And the nodes are connected through the edges.
- Cluster Formation: Numbers of clusters are formed by dividing the sensor nodes into different groups.
- Selection of Cluster Head/ Aggregator: Aggregator is selected from each cluster. Aggregator selection is done by using parameter like highest remaining energy of the nodes. This step is performed twice, after initial formation of clusters and for selection of new aggregator on detecting attack on old aggregator.
- Iterative Filtering: The new IF algorithm is used for detection compromised node in sensing network. This iteratively checks the readings and assigns weights to the node.
- Detection of Compromised Node: Compromised nodes are detected by comparing the weights to the threshold. The node with less weight is considered as the compromised node. It works for both the cluster members and aggregator too.

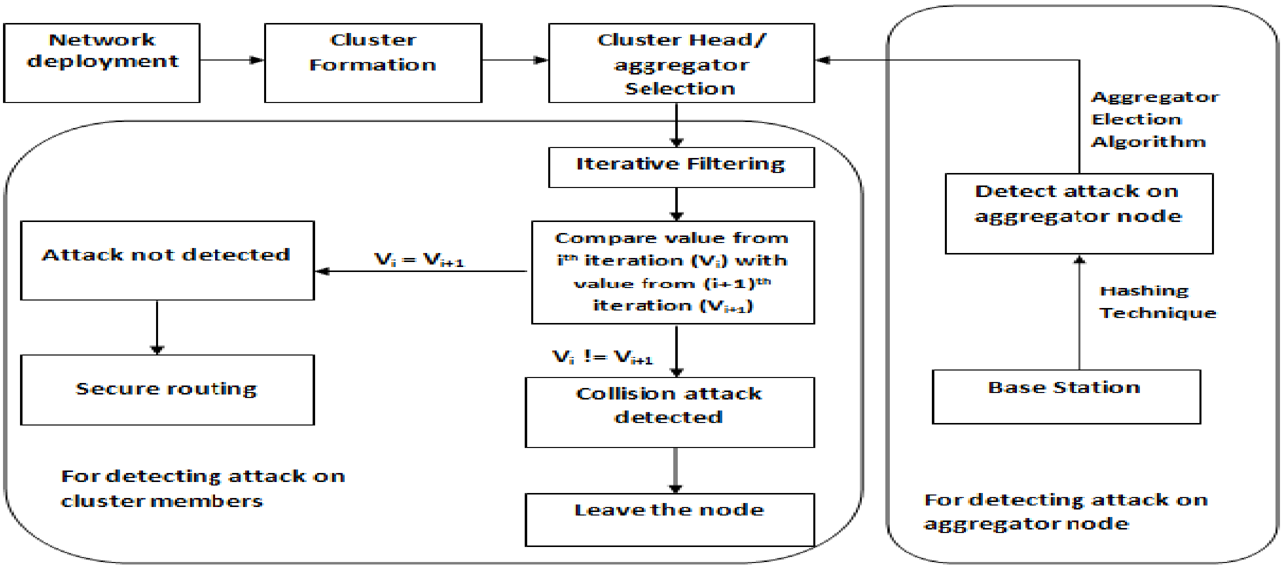
Network deployment
Cluster Formation
Cluster Head/ aggregator Selection
Iterative Filtering
Compare value from ith iteration (V_i) with value from (i+1)th iteration (V_{i+1})
$V_i = V_{i+1}$
Attack not detected
Secure routing
$V_i \ne V_{i+1}$
Collision attack detected
Leave the node
For detecting attack on cluster members
Aggregator Election Algorithm
Detect attack on aggregator node
Hashing Technique
Base Station
For detecting attack on aggregator node

Fig. 2 Proposed System Architecture

6. MATHEMATICAL MODEL

6.1 Set Theory

Let, S be a system, S= {N, C, CH, B, CN, A},

Where,

1) Deploy Sensor nodes...

N= {N1, N2,Nn},

N is set of all deployed sensor nodes.

2) Cluster formation.

C= {C1, C2, ..., Cn },

C is a set of all clusters.

3) Select the Cluster Heads that is aggregatorfor Each Clusters.

CH= { CH1, CH2, ..., CHn },

CH is a set of all cluster heads.

4) Create Base Station.

B= { B1, B2, ..., Bn }

B is a set of all base stations.

5) Find out compromised nodes

CN= { CN1, CN2, ..., CNn },

CN is a setof compromised nodes.

6) Robust data aggregation at aggregatornode.

A= { A1, A2, ..., An },

A is a set of all aggregated data files.

6.2 Mathematical Model For Proposed System

For Energy Calculation,

$$E_{Tx}(k.d) = E_{elec} * K + \in_{amp} * k * d^{n}$$

$$E_{Rx}(k) = E_{elec} * k$$

d: Distance for neighboring sensor node.

$\in_{amp}$: Energy required for the transmitter amplifier.

E_{elec} : Energy consumed for driving the transmitter or receiver circuitry.

6.3 Algorithm

Algorithm 1 Pseudo code of propose system is

1. Input**:** V= Set of all nodes
2. Initialize energy to each node of V.
3. Calculate energy of each node N.
4. Compare energy of all nodes.
5. Select maximum energy node.
6. Output: CH = node who's having maximum energy.

7. ANALYSIS AND RESULTS

Figure 3 shows the graph comparing the residual energy of the proposed and existing system. In which it is clearly seen that the residual energy level in proposed system is high compared to the existing system.

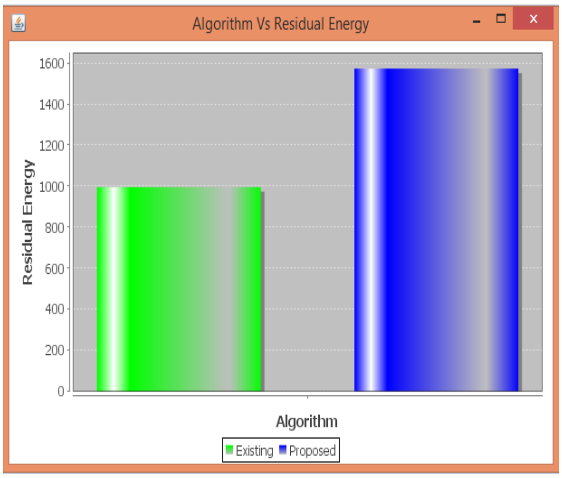

Fig. 3 Residual energy comparison graph

Table 1. Residual energy comparison

Parameter	Existing System	Proposed System
Residual Energy (in joules)	1000	1600

Figure 4 shows the latency comparison graph in which compared the time to send the package/data in the system. In the above graph the comparison of existing and proposed system is done and from figure shows that thelatency in proposed system is very less compared with the latency in the existing system.

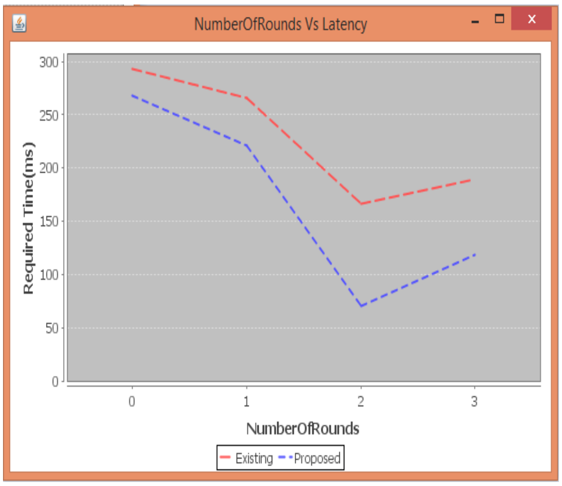

Fig. 4 latency comparison graph

Table 2. Latency comparison

Round	Existing System	Proposed System
0	290	260
1	260	225
2	160	65
3	110	190

8. CONCLUSION

Iterative filtering algorithm is one of the powerful techniques for secure data aggregation which provides trust valuation for sensor nodes based on the data gathered from differentsources. Recent IF algorithm uses initial approximation formaking algorithm more robust against attacks. Existing IF technique coversdetection of compromised cluster members but does not consider the fact that aggregator can also be compromised, which can be hazardous in reality. In proposed work, secure and robust data aggregation is performed in vicinity of collusion attacks which are accessible in wireless sensor network. Also it is able to detect the attack in cluster member as well as on aggregator and energy efficiency is improved by using introduced protocol for election of aggregator having more energy. As perexpectationthe proposed system is more robust against the compromised aggregator node also it saves time and energy compared to the existing system.

In this system, the simple and collusion types of attacks in wireless sensor networks are detected. Also the issue of detecting compromised aggregator node is addressed. The aggregator node or any other sensor node which is found as compromised will not be considered for further process in the network as attacker has control over it. So in future work the strategy can be developed to recover the compromised node and reuse it again in the network. Also in future, the system can be implemented to process the audio, video, image type of data.

In future we can incorporate methods that can prevent collusion attacks on images and videos.

9. ACKNOWLEDGEMENT

It is pleasure for me to thank lot of people who have support me in completing to this paper in different ways. Starting with, I would like to thank my Guide, Prof. M. D. Ingle for hissupport during the entire work. His support for helping me to get helpful content in the topic. I am thankful to HOD, Principal, teachers and collage to providing us the facilities in the department and their guidance

10. REFERENCES

[1] M. Rezvani, A.r Ignjatovic, E. Bertino, and S. Jha, “SecureData Aggregation Technique for Wireless Sensor Networksin the Presence of Collusion Attacks ”, IEEE transactionson dependable and secure computing, vol. 12, no. 1, january/february 2015.

[2] Y. Zhou, T. Lei, and T. Zhou, “A robust ranking algorithmto spamming,” Europhys. Lett., vol. 94, p. 48002, 2011.

[3] E. Ayday, H. Lee, and F. Fekri, “An iterative algorithm fortrust and reputation management,” Proc IEEE Int. Conf.Symp. Inf. Theory, vol. 3, 2009, pp. 20512055.

[4] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, “Robustreputation based ranking on bipartite rating networks,” inProc. SIAM Int. Conf. Data Mining, 2012, pp. 612-623.

[5] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu,“A gametheoretic approach for high-assurance of datatrustworthiness in sensor networks,” in Proc. IEEE 28thInt. Conf. Data Eng., Apr. 2012, pp. 1192-1203

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputationbased framework for high integrity sensor networks,”ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 15:1-15:37, Jun.2008.

[7] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, “UsingSensorRanks for in-network detection of faulty readingsin wireless sensor networks,” in Proc. 6th ACM Int. WorkshopData Eng. Wireless Mobile Access, 2007, pp. 1-8.

[8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan,“Energy-efficient communication protocol for wirelessmicrosensor networks,” in Proceedings of the 33rd AnnualHawaii International Conference on System Siences(HICSS’00), January 2000.

[9] O. Younis and S. Fahmy, “Distributed clustering in adhocsensor networks: a hybrid, energy-efficient approach,”in Proceedings of the 23rd Annual Joint Conference ofthe IEEE Computer and Communications Societies (INFOCOM’04), pp. 629-640, Hong Kong, March 2004.

[10] Suat Ozdemir, Yang Xiao, ”Secure data aggregation in wireless sensor networks: A comprehensive overview,” Computer Networks 53 (2009) 2022-2037.

[11] H.S. Lim, Y.S. Moon, and E. Bertino,”Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 27.

[12] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, ”Information filtering via iterative refinement,” Europhys. Lett., vol. 75, pp. 1006-1012, Sep. 2006.