Trust Evaluation for Securing Compromised data Aggregation against the Collusion Attack in WSN

[1]Mr.Lekhchand Sharnagat, [2]Prof.Rajesh Babu, [3]Prof.jayant Adhikari
1M.Tech Student, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.
2,3Assistant Professor, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.

Abstract— **With a storage space limit on the sensors, WSN has some drawbacks related to bandwidth and computational skills. This limited resources would reduce the amount of data transmitted across the network. For this reason, data aggregation is considered as a new process. Iterative filtration (IF) algorithms, which provide trust assessment to the various sources from which the data aggregation has been performed, are efficient in the present data aggregation algorithms. Trust assessment is done with weights from the simple average method to aggregation, which treats attack susceptibility. Iteration filter algorithms are stronger than the ordinary average, but they do not handle the current advanced attack that takes advantage of false information with many compromise nodes. Iterative filters are strengthened by an initial confidence estimate to track new and complex attacks, improving the solidity and accuracy of the IF algorithm. The new method is mainly concerned with attacks against the clusters and not against the aggregator. In this process, if an aggregator is attacked, the current system fails, and the information is eventually transmitted to the aggregator by the cluster members. This problem can be detected when both cluster members and aggregators are being targeted. It is proposed to choose an aggregator which chooses a new aggregator according to the remaining maximum energy and distance to the base station when an aggregator attack is detected. It also save time and energy compared to the current program against the corrupted aggregator node.**

Keywords— **Wireless sensor network, data aggregation, architecture, network lifetime, routing, tree, cluster, base station**

I. INTRODUCTION

There are a large number of low power and inexpensive sensing devices with low measurements, memories and storage space in the wireless sensor network. WSN is known to be an excellent ad-hoc service network agency. A number of sensor nodes in the remote sensor network are distributed in such a way that data on the physical or environmental surroundings are detected, collected and processed. Mobile nodes feature a fundamental processor, sensors and a portable low-power transceiver. The aggregation of data is used to reduce overhead transport due to the limited capacity of the sensor nodes. The data are collected at cluster head nodes during the data collection, and combined data is transmitted to a base station. The retrieval method of databases involves data collection and secure access to information at the base stations. Protocols of data aggregation can be classified as protocols based on topology tree and cluster. Data flows from the leaf nodes (child nodes) to the top nodes (parent nodes) in a tree-based data aggregation, where aggregations take place at the parent nodes. Through the aggregation of the clusters, groups are constructed of nodes that are referred to as clusters. The cluster head often named as an aggregator gathers data by gathering and then sending it to a base station information from cluster members. The sensor nodes only have power, battery and limited storage space in their computation. Given all these constraints, data transportation must be that in order to save these properties. Improve efficient method of aggregating the data. The information is transmitted from different sensors to a node called an aggregator, and the aggregated data is then forwarded to the base station. Measurement is the simplest algorithm used for data aggregation. This also succeeds in recognizing constraints on the sensor nodes. Nevertheless, such a combination could easily attack WSN without much effort by fault, i.e. with averaged adversaries to the algorithm. Also cryptographic techniques like encryption decryption can't remedy this. The compromise sensor node is completely managed by the opponent and the opposing person may access any data stored in a node. Therefore it is important to perform data aggregation with more competent algorithms. The definition of trust evaluation to information from the sensor node can be used for protection with data aggregation.

For the same reason, iterative filtering (IF) algorithms can be used. It uses a single iterative approach and solves problems, aggregates data and evaluates trust. The reliability of each sensor is calculated by considering the difference between sensor readings and the appropriate estimates in the previous round iteration as in the form of a summing of all sensor assessments. This is generally a weighted average data aggregation. There is a fundamental difference in sensor readings from this calculation. Therefore, in the aggregation phase, the sensors are regarded as being less dependable, with their measurements given the lowest weight in the present iteration number.

The Wagner proposed dynamic node model is used for the wireless sensor network. The model consists of the formation of node clusters and the aggregation of all cluster heads from established clusters. Information is gathered and aggregated intermittently. The collector itself will not be compromised and will concentrate on the algorithms that ensure a safe aggregation even if individual sensor nodes are compromised and false data are likely sent to the aggregator. That data

aggregator must be strong enough to run an IF algorithm used for data collection.

II. Literature Survey

A new attack in this paper [1], in comparison to current IF algorithms, is regarded as a sophisticated conspiracy attack. Achievement is achieved by providing an initial confidence estimate over the current Iterative filtering algorithm, which makes current algorithms more accurate, reliable and fast. The method is limited if no corrupted aggregators are identified and secured. In the deployed sensor network, the author tried to apply the method.

A trustworthy algorithm based on a web-based correlation model has been suggested to overcome the spammer attack impact question rankings. Author suggested [2] In order to create a correlation between index ratings and the weighted products with an average value function, the author describes consumers' confidence using a correlative and iterative approach. The proposed algorithm is more effective and precise, but the algorithm can also be more accurate.

The author has implemented [3] the ITRM which is an effective method for estimating the service provider's credibility and the extent of dependency on the service providers. It suggests that, information should be collected and the company's credibility based on the customer reviews received. By contrasting current reputation management systems with the schemes proposed, the scheme proposed is more accurate and efficient to detect malicious ratings, and the credibility of suppliers for attacks is evaluated in a less time frame.

Two-party rating networks have two types of entities in this paper [4]: users, and artifacts. A user sets scores for the products. In bipartisan rating systems the primary challenge is to rate the products based on user feedback. There are current algorithms that are either not reliable or do not guarantee convergence against spammers. The author has developed six new ranking algorithms based on credibility. The author has considered the product of aggregating discrepancies between the user ratings and the item ranking for the calculation of user credibility values. With realistic evaluation on three actual datasets, the author has shown proposed algorithms as more powerful, stronger and successful.

The author has suggested the theoretical security strategy in this paper [5] to protect sensor nodes and ensure a high level of trust on nodes. The proposal suggested relies on the pressure from stackelberg, which means the attacker is limited to the number of attacks. In each attack iteration, the policy proposed ensures that the sensor node number is secured. This approach answers the issue of sensor data trust and effectively and efficiently protects the sensor network from different malicious attacks.

A framework [6], called RFSN, was proposed by the Author to preserve the respect each node has for each other in the system based on the confidence-building process. The frame also tackles the sensor node limitations. A beta reputation framework has been developed within RSFN, which uses Bayesian formulation to estimate the confidentiality of sensor nodes. RFSN offers an approach to the identification of all misdeeds triggered by malicious and faulty network sensors. It also involves various security solutions.

The paper suggests a Sensor Rank methodology by analyzing the Network's Markov Chain. Faulty readings have a significant impact on question accuracy in WLANs. A network of correlations provides a Sensor Rank source for network sensor nodes. The confidence vote algorithm is proposed in order to resolve the faulty readings of the sensor number.

The author suggested [8] the probabilistic LEACH algorithm. By random numbers, LEACH selects the cluster center. Cluster is built on the nearest point, i.e. addition of other nodes in a cluster whose head of a cluster is closest to it. One hop conversation is used by LEACH. The energy use in the WSN is closely regulated.

III. Proposed Methodology

The network nodes are divided into disjointed groups, with a head known as a cluster head or aggregator in each group. The cluster heads assemble and intermittently store information. Data on that. Details. The suggested scheme specifies that the aggregator Node will be compromised much like the cluster Node. The corrupted aggregator sends the base station with fake aggregate values. Via the Iterative filtering algorithm as well as with aggregator, a technique is thus implemented to detect attacks against cluster members. This includes even a protocol to detect an attack by choosing a new aggregator. By implementing this, the WSN is fulfilling its expectoration of improved protection and energy efficiency. The machine architecture is illustrated in Fig.1.

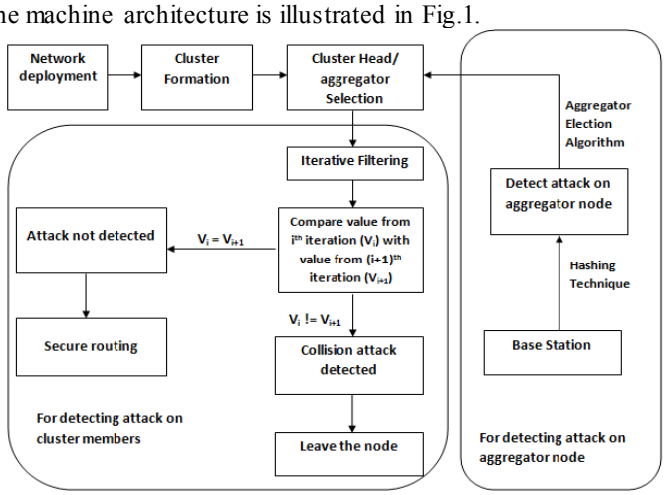

Figure 1. System Architecture

The method is divided into the next number of steps:

- Generation of Network: Sensor node generation is carried out in this section. And through the edges the nodes are linked.
- Cluster Formation: The number of clusters is divided into different classes by the sensor nodes.
- Selection of Cluster Head/ Aggregator: From every cluster, the aggregator is selected. The selection of the aggregator is made with parameters such as the highest remaining node capacity. After initial cluster forming and for the selection of new aggregator for attacking an old aggregator, this move will be done twice.
- Iterative Filtering: For identification of nodes in the sensing network, the latest IF algorithm is used. This tests the readings iteratively and assigns weights to the node.
- Detection of Compromised Node: By comparing the weight with the threshold, compromised nodes are detected. The less weight node is known as a node affected. It works with the cluster members as well as the aggregator.

Implementation Details

A. Mathematical Formulation

Let, K be a system, K= {P, Q, R, T, U, D},
Where,
1) Deploy the nodes of the sensor...
P= {P1, P2, Pn},
P includes all the sensor nodes that are deployed.2) Cluster formation.
Q= {Q1, Q2... Qn},
Q is all clusters in a group.
3) Choose the Heads of the cluster that is an Individual cluster aggregator.
R= {R1, R2... Rn},
R is a compilation of all heads of the cluster.4) Create Base Station.
T= {T1, T2...Tn}
T is a set of all bases.
5) Find variations on nodes
U= {U1, U2...Un},
U is a group of nodes affected.
6) The aggregator node's robust data aggregation.
D= {D1, D2...Dn},
D is a collection of all the data files aggregated.

B. Algorithm

1: Input: B= All nodes are included.
2: Initialize energy for every B node.
3: Calculate the energy of every P node.
4: Compare the energies of all the nodes.
5: Choose the maximum energy node.
6: Output: Q = the full energy node.

IV. Result Analysis

1. Energy Graph

The comparison graph of the current and expected device energy consumption ratio can be found in Figure 2. The energy consumed by the system is lower than the current systemas predicted.

Table 1: Comparison of current and planned schemes for energy use

Round	Existing System	Proposed System
0	340	290
1	280	230
2	390	370
3	290	260

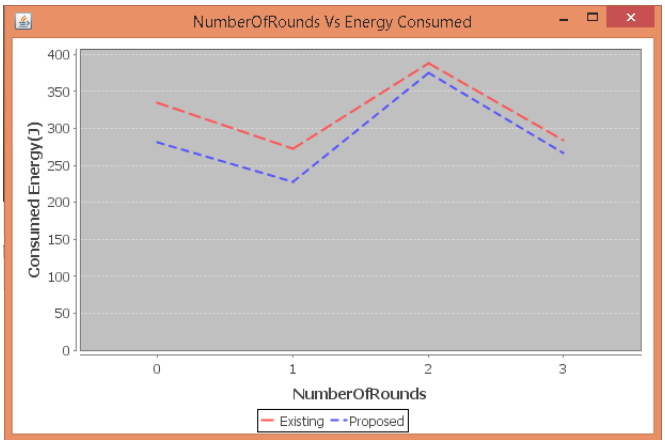

Figure 2: Comparison of energy between the current program and the plan

2. Latency Graph

The comparative graph for the required time ratio between the current and the proposed system is shown in Figure 3. The program proposed is simpler and stable in contrast to the current system, according to standards

.Table 2: Latency Comparison between Existing and Proposed System

Round	Existing System	Proposed System
0	160	60
1	170	110
2	170	160
3	250	160

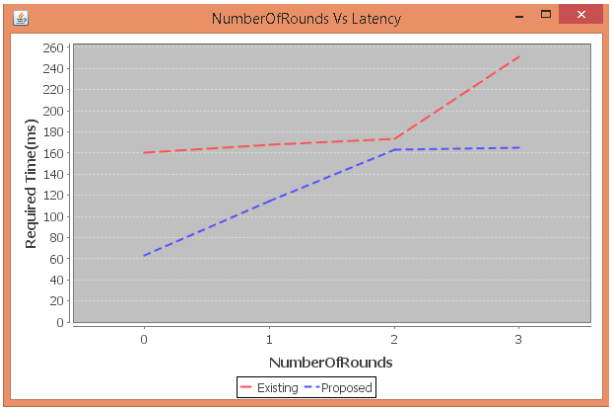

Figure 3: Latency comparison between existing and proposed system

3. Energy Residual Graph

The residual energy graph of the current system and its proposed system is shown in Figure 4. The system proposed saves more resources than the current system according to estimates.

Table 3: Comparison between current and planned network of residual energy

Parameter	Existing System	Proposed System
Energy in Joule	800	1500

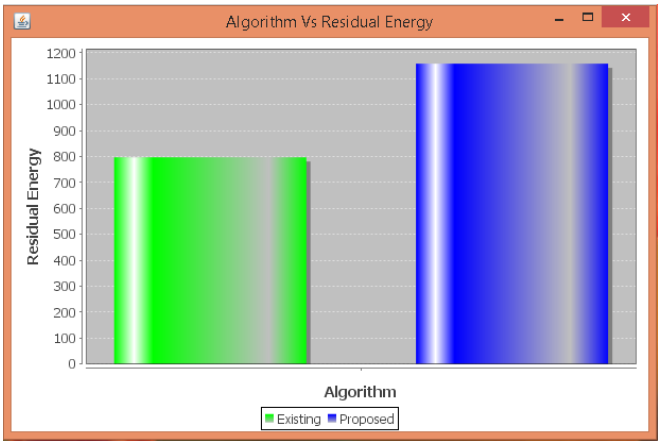

Figure 4: Comparison between current and planned schemes for residual energy

V. CONCLUSION

Another effective technique for safe data aggregation, which gives confidence assessment of sensor nodes based on data collected in different sources, is the inherent filtering algorithm. Initial approximation is used in the recent IF algorithm to make the algorithm robust against attack. The current IF-Technique does not recognize the fact that the aggregator may also be compromise, which in actual fact can be risky, but it identifies compromised members. Stable and reliable data aggregation in the vicinity of conspiracy attacks that are accessible in a wireless network is carried out in the proposed research. It can also detect a cluster Member attack, as well as aggregator attack and improves energy efficiency through the use of the implemented protocol to pick an aggregator with more resources. As the assumption is as expected, the proposed method is more reliable against the corrupted aggregator node.

The program detects the basic and colliding forms of attacks on the networks of wireless sensors. The identification of corrupted nodes of aggregators is also discussed. For more processes in the network, the aggregator node or any other sensor node found to be compromised and it cannot be considered because an intruder controls it. Thus, the technique can be built in future research to recuperate and reuse the damaged node in the network. The device can also be introduced in future in order to handle the audio, video, and image data form.

REFERENCES

[1] S Sundeep Desai, Manisha J Nene, "Node-Level Trust Evaluation in Wireless Sensor Networks", IEEE Transaction on Information Forensics And Security Vol: 14, Issue: 8, Aug 2019.

[2] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," volume 4, pages 1 - 9, International Journal of Computer Science and Information Security, 2009.

[3] Sakshi Srivastava and Kushal Johari, " A survey on reputation and trust management in wireless sensor network," volume 1, pages 139 - 149, International Journal of Scientific Research Engineering Technology, August 2012.

[4] Ke Liu, Nael Abughazaleh and Kyoung Donkang., "Location verification and trust management for resilient geographic routing," ELSEVIER, 2007.

[5] Efthimia Aivaloglou and Stefanos Gritzalis, "Hybrid trust and reputation management for sensor networks," Springer, October 2009.

[6] Riaz Ahmed Shaikh, Hassan Jameel, Brian J d Auriol, Heejo Lee, Sungyoung Lee, and Young- Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," pages 1698 - 1712, IEEE Transactions on Parallel and Distributed Systems, October 2009.

[7] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan, and Abdul Sattar, "A trust management architecture for hierarchical wireless sensor networks," pages 268 - 271, IEEE Conference, 2010.

[8] Idris M. Atakli, Hongbing Hu, Yu Chen, WeiShinn Ku, and Zhou Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation, " The Symposium on Simulation of Systems Security (SSSS08), Ottawa, Canada,, April 2008.

[9] Long Ju, Hongjuan Li, Yaqiong Liu, Weilian Xue, Keqiu Li, and Zhongxian Chi," An improved intrusion detection scheme based on weighted trust evaluation for wireless sensor networks", IEEE Conference on Local Computer Networks, 2010.

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

[11] 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.

[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robustreputation based ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612-623.

[13] 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

[14] 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.
[15] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using Sensor Ranks for in-network detection of faulty readings in wireless sensor networks," in Proc. 6th ACM Int. Workshop Data Eng. Wireless Mobile Access, 2007, pp. 1-8.