A Secured method of Data Aggregation for Wireless Sensor Networks in the Presence of Collusion Attacks

Mohith Aiyappa S[1], Ravi Kumar M N[2]

[1] PG Scholar, Dept. of E&C, Malnad college of engineering, Karnataka, India
[2] Associate Professor, Dept. of E&C, Malnad college of engineering, Karnataka, India

---***---

Abstract - *In today's world Wireless Sensor Networks (WSNs) plays a major role in various applications ranging from weather monitoring to military and surveillance applications. In each of these applications the sensor nodes senses the data and transmits the sensed data to the sink node. In earlier days data is transmitted to the sink directly without preprocessing using either single hop or by multi hop techniques in the network, hence this method consumes more energy. Data aggregation is an effective technique in WSN because it reduces the number of packets to be sent to sink and increases the lifetime of sensor network by aggregating the similar packets. Secure data transmission is a crucial need for achieving the QOS in WSN. Secure data aggregation technique is one of the very efficient technique to overcome the problem of weaker node attacks. To achieve this, IF Algorithm is used which is most effective solution. IF Algorithm is an efficient and reliable option for WSN because they solve both problems of data aggregation and data trustworthiness estimation using a single iterative procedure. In this paper planned to concentrate on many IF Algorithm which make robust against collusion attacks than simply averaging method. In WSN aggregation plays an important role in improving capacity. Data aggregation could be of two types, Exact and Approximate. Collusion attack means attacker tries to corrupt transmitting data, hence there will be a mismatch in aggregation.it is the agreement between nodes to act together secretly or illegally in order to deceive or cheat original data.*

To avoid collusion IF algorithm has been implemented. Iteration is the act of repeating a process, either to generate a unbounded sequence of outcomes or with the aim of approaching a desired goal, target or result. Each repetition of the process is also called as an Iteration. In mathematical Iteration function is used by applying a function repeatedly using the output from one iteration as the input to the next. Iterative filtering algorithms are a tool for maximum likelihood inference on partially observed dynamical systems. In this project different IF algorithm has been used to avoid collusion and get a proper result.

Key Words: **Wireless Sensor Networks, Sensor Nodes, IF Algorithm, Collusion Attacks, Secure Data Aggregation.**

1. INTRODUCTION

The primary use of Wireless Sensor Networks(WSN) is to collect and process data. WSN are emerging as the widely used technology in the present day world. A wireless sensor networks consists of a collection of these nodes that have the facility to sense, process data and communicate with each other via wireless connection. WSN is a network system comprised of spatially distributed devices using the wireless sensor nodes to monitor physical or environmental situations such as sound, temperature and motion. The main goal of data aggregation is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Fig 1 shows the network model for WSN. The sensor nodes are divided into different clusters and each cluster appointed as a cluster head. data are periodically monitoring from each node and then pass their data to the cluster head. finally cluster head processing that data and pass to the base station. WSN offer an increasingly attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. The process of grouping sensor nodes in a densely deployed large scale sensor network is known as clustering. sensor networks are the collection of sensor nodes which cooperatively send sensed data to base station. As sensor nodes are battery driven an efficient utilization of power is essential in ore use networks for long duration.

In WSN aggregation plays an important role in improving capacity. Data aggregation could be of two types. Exact and Approximate. collusion attack means attacker tries to corrupt transmitting data, hence there will be a mismatch in aggregation.it is the agreement between nodes to act together secretly or illegally in order to deceive or cheat original data.

To avoid collusion IF algorithm has been implemented. Iteration is the act of repeating a process, either to generate a unbounded sequence of outcomes or with the aim of approaching a desired goal, target or result. Each repetition of the process is also called as an Iteration. In mathematical Iteration function is used by applying a function repeatedly using the output from one iteration as the input to the next. Iterative filtering algorithms are a tool for maximum likelihood inference on partially observed dynamical systems. In this project different IF algorithm has been used to avoid collusion and get a proper result.

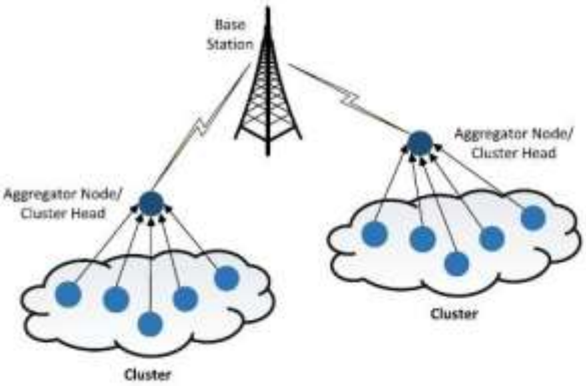

Fig. 1.Model for WSN

2. RELATED WORK

Many actions are discussed about different algorithm related to secure data aggregation. Aggregation problem has been solved by, investigate the relationship between security and data aggregation process in WSN. A taxonomy of secure data aggregation protocols is given by looking over the current “state-of-the-art” work in this area [1]

Synopsis diffusion approach make the protect against the attack launched by the compromised nodes. The algorithm is to enable the base station to securely process predicate count or sum even in the presence of such an attack.[2]

The computational proficient strategy to process a weighted normal (which we will call strong average)of sensor measurements, which appropriately takes sensor deficiencies and sensor noise into consideration[3]

The security vulnerabilities of data aggregation system and present a survey of robust and secure aggregation protocols that are resilient to false data injection attacks.[4]

The algorithm present an analysis framework that allows for general decomposition of existing reputation systems. the attacks are classified against reputation systems by identifying which system components and design choices are the target of attacks.[5]

The aggregation strategies become bandwidth intensive when combined with fault tolerant, multipath routing methods often used in these environments.[6]

To address the security issue one technique has been proposed that is to provide security to network from an attacker and also enhance the robustness and accuracy of an information. Iterative filtering algorithm is one of the algorithm to perform secure data aggregation and also provides security to the entire network.[7]

3. METHODOLOGY

In our proposed system we have considered IF algorithms has been proposed.

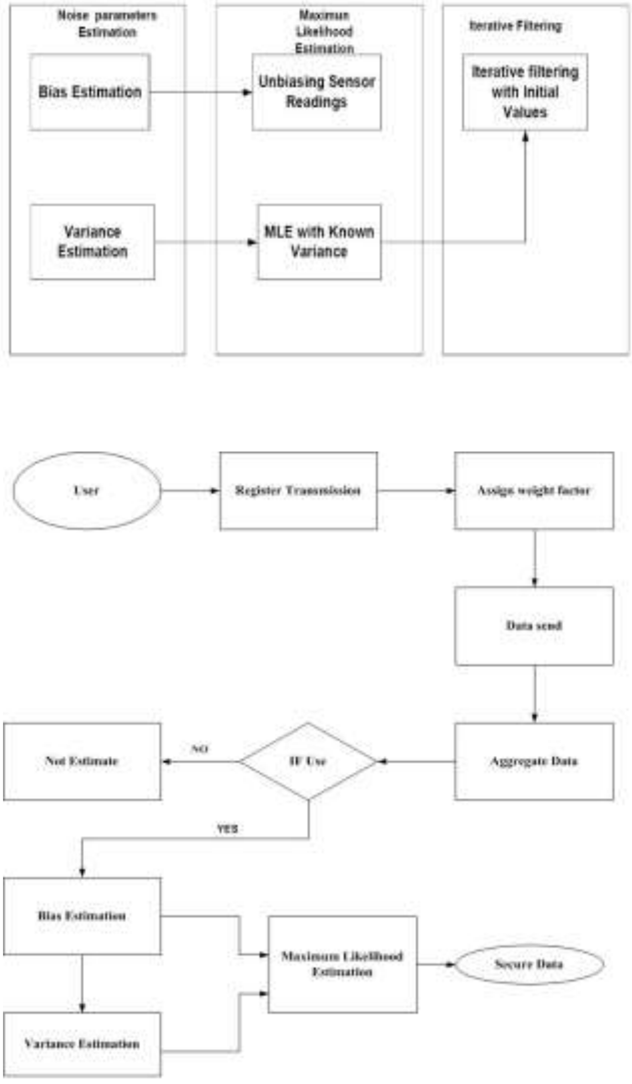

Fig. 2.Methodology

The above figure shows the block diagram and flow diagram of the iterative filter algorithm.

4.ITERATIVE FILTERING ALGORITHM

Iteration is the demonstration of repeating process either to produce an unbounded grouping of result or with the aim of approaching a desired goal, target or result. Each process of repetition is likewise called an iteration and the result of one iteration are utilized as the beginning stage for the next iteration.

Iteration in arithmetic may refer to the way toward emphasizing a capacity i.e. applying a function repeatedly, utilizing the output from one cycle as the input to the next. cycle apparently simple functions can create complex behaviours and difficult issues.

In computational arithmetic, an iterative technique is a numerical methodology that produces arrangement of enhancing approximate solutions for a class of problems

4.1 Benefits of IF Algorithm

- Some Iterative algorithms are designed for accuracy.
- Round off error are subjected to direct method.
- Iterating function reduces error to zero.
- It produces answer in a faster manner.
- It solves many matrix functions.
- speeds depends on number of non zero elements and total number of elements.
- It starts with approximate answers that is output can be acted as next input.
- Each iteration improves accuracy.
- During iteration matrix can not be changed so it can be operated efficiently.

4.2 Steps of IF Algorithm

- In the first step initialize the first round of iteration. taking the first round of output as the input to the next round
- In the second step initialize inputs as X,n,m where X is the block of readings and n is the number of sensors and m is the number of readings for each sensors.
- In the third step compute the output of reputation vector r that is output can be represented as r.
- In the next step initialize weight by giving equal credibility that is $w^{(0)}$ = 1 and multiplying that weight with X.
- After multiplying compute reputation vector $r^{(l+1)}$, assume l=0.
- In the sixth step compute the corresponding weight that is $w(l+1)$.
- In the final step repeat the above steps until the reputation vector has converged that means if the aggregate values are same for some iterations then stop the process.

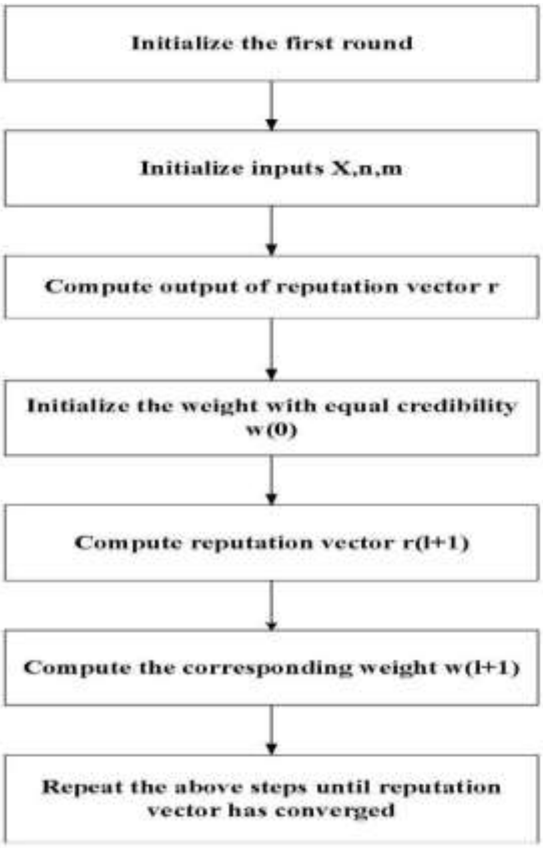
Initialize the first round
Initialize inputs X,n,m
Compute output of reputation vector r
Initialize the weight with equal credibility w(0)
Compute reputation vector r(l+1)
Compute the corresponding weight w(l+1)
Repeat the above steps until reputation vector has converged

Fig. 3.Flowchart of IF Algorithm

4.3 Modules for secure data aggregation using IF

1) Node creation with weight factors assigned to source.
2) Data aggregation in multiple sources.
3) Find bias and unbiased readings using IF.
4) Secure data aggregation using IF.

5. MATHEMATICAL ANALYSIS

In the reputation system of iterative filtering we will see the context of data aggregation in WSN and the weakness of the algorithm for a possible collusion attack.

Consider a wireless sensor network with n number of sensors denoted by S_i where $i = 1,2,3, \dots . n$. Data aggregator can be operated only one block of readings at a time.each block can be operated at a readings of m consecutive instants.

The matrix X can be represented as $X = x_1, x_2, x_3 \dots \dots x_n$ where $x_i = [x_i^1, x_i^2, x_i^3 \dots \dots x_i^m]^T$ The output vector is $r = [r_1, r_2, \dots r_m]^T$ for a time instants $t = 1,2, \dots . m$

The reputation vector can be computed iteratively and simultaneously with a sequence of weights $w = [w_1, w_2, \dots w_n]^T$. Initially the iterating procedure starts with giving equal number of weights to all sensors that is $w^0 = 1$. Then the reputation vector $r^{(l+1)}$ can be calculated as

$$r^{(l+1)} = \frac{X.w^{(l)}}{\sum_{i=1}^{n} w_i^l}$$

The begining of the reputation vector can be represented as $r^{(1)} = \frac{1}{n}X.1$ that is $r^{(1)}$.

$r^{(1)}$is just the simple average of readings of all sensors at each particular instants.The new weight vector $w^{(l+1)}$ can be computed as a function of $g(d)$ then

$$d = [d_1, d_2, \dots \dots \dots . d_n]^T$$

$$d_i = \frac{1}{m}\left\|X_i - r^{(l+1)}\right\|_2^2$$

$$w_i^{(l+1)} = g(d_i)$$

Function $g(x)$ is called as the discriminant function

- Reciprocal $g(d) = d^{-k}$
- Exponential $g(d) = e^{-k}$
- Affine $g(d) = 1 - k_1 d$

The above formulas are based on the computation of IF Algorithm.

6. COLLUSION ATTACK SCENARIO

Collusion attack means a secret understanding between two or more persons to gain something illegally.In wireless sensor network collusion attack means some hackers inject false data to the original node to mismatch the aggregate readings.In this scenario attacker is able to mislead the reported data values.

Let us consider three scenarios as shown in the below figure. Figure 3.2 shows the different scenarios against IF algorithm.

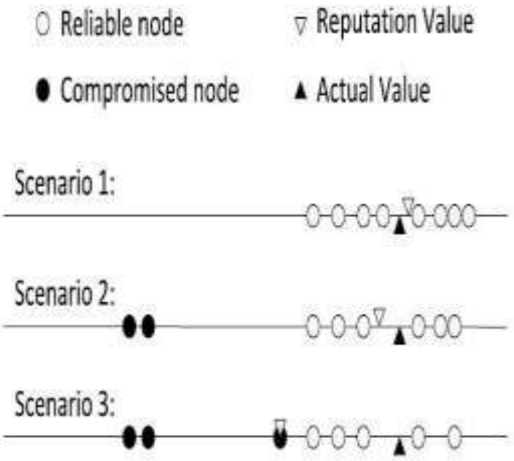

Fig. 4. Attacks scenario in IF

In the **first scenario** all sensors are reliable and the result of the IF calculations is near to the actual value.

In the **second scenario** an adversary compromises two sensor hubs, and modifies the readings of these values such that the normal average of all sensor readings is skewed towards a lower esteem. In that case IF algorithm punishes them and allots to them lower weights, because their values are a long way from the estimation of other sensors. Iterative Filter algorithm is strong against false data information because the compromised nodes individually falsify the readings without any learning about the aggregation calculation.

In the **Third scenario** an adversary employs three compromised nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity.

7. RESULT ANALYSIS

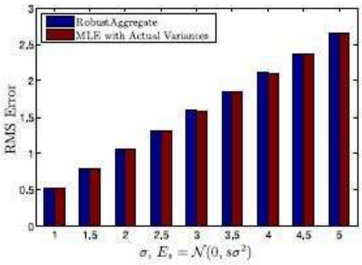

Fig. 5. Unbiased error using MLE

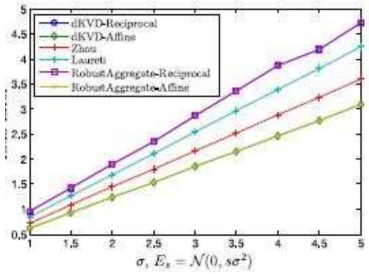

Fig. 6.Bias error

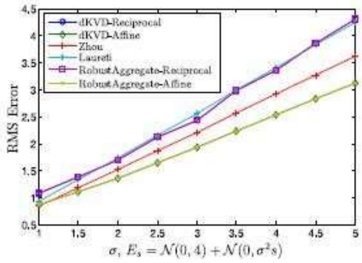

Fig. 7.Unbiased error

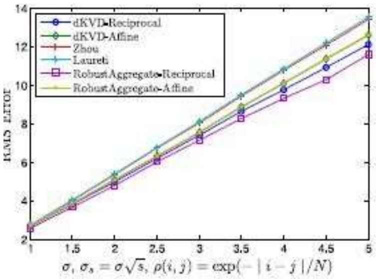

Fig. 8. Correlated noise

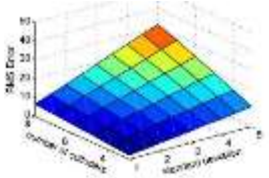

Fig.9. dVKD- Reciprocal

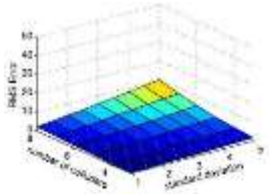

Fig. 10. dKVD- Affine noise

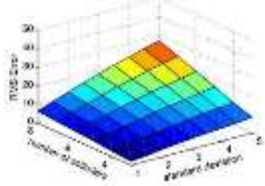

Fig.11. Zhou

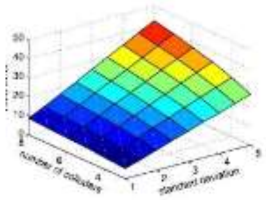

Fig.12. Laureti

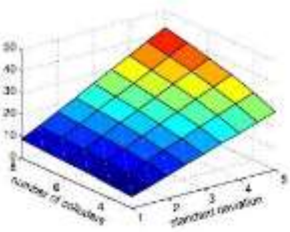

Fig.13. Robust aggregate Reciprocal

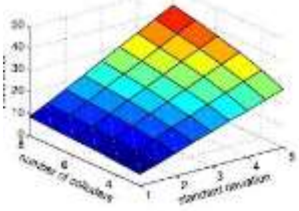

Fig.14. Robust aggregate Affine

The above figure shows the result of different IF algorithms. Different IF algorithms give different types of data aggregate readings.

8. COMPARSION RESULT

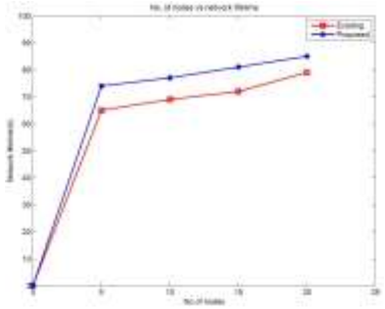

Fig.15. Network Lifetime

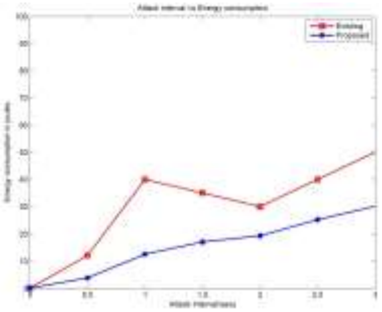

Fig.16. Energy Consumption

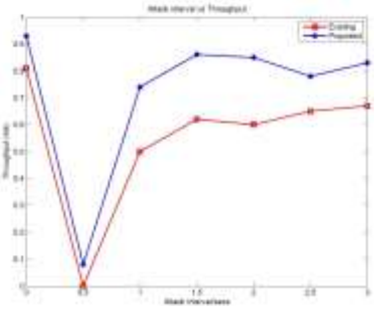

Fig.17. Throughput

9. CONCLUSION

In wireless sensor networks, an attacker can inject false data to damage the network data integrity by utilizing a compromised node Existing researches did not combine data aggregation, data Confidentiality, data integrity and false data detection together well. In this paper we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging.so finally we concluded that proposed IF algorithm is better than existing algorithm like network lifetime, energy consumption and throughput. In future, we will investigate whether our approach can protect against compromised aggregators.

REFERENCES

[1] Y. X. Suat Ozdemir Secure data aggregation in wireless sensor networks: A comprehensive overview, Elsevier computer Networks 2009

[2] Z. H. L. Sankardas Roy, Mauro Conti and S. Jajodia Secure data aggregation in wireless sensor networks: Filtering out the attackers impact,IEEE Transactionon Information forensic and security., vol. 09, no. 4, 2014.

[3] W. H. Chun Tung Chou Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults ,IEEE journal 2010

[4] Sanjeev SETIA , Sankardas ROY and Sushil JAJODIA Secure Data Aggregation in Wireless Sensor Networks" Department of Computer Science Proceedings of IEEE International Conference 2010

[5] Kevin Hoffman, David Zage, Cristina Nita-Rotaru A Survey of Attack and Defense Techniques for Reputation Systems" Department of Computer Science and CERIAS, Purdue University, 2007

[6] George Kollios, John Byers, Jeffrey Considine, Marios Hadjieleftheriou, and Feifei Li Robust Aggregation in Sensor Networks" Department of Computer Science, Boston University, 2005 IEEE

[7] X.Wu,Y.Xiong,W.Huang,H.Shen,M.Li. An efficient compressive data gathering routing scheme for large-scale wireless sensor networks, ElsevierComput.Electr.Eng,39(2013).1935-1946.

[8] K.Suriya, R.Dhanagopal An Efficient Apporach For Secure Data Aggregation Technique For Wsn In The Presence Of Security Attacks,Department of ECE, 2015 IJARTET

[9] C.de Kerchove and P. Van Dooren Iterative filtering in reputation systems, , SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812-1834, Mar. 2010.