ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Secure Data Aggregation Technique for Wireless Sensor Networks

Chaitali Nirmal[1], M.P. Dongare[2]

[1]M.E. Electronics, Department of Electronics Engineering, Amrutvahini College of Engineering, Sangamner, Maharashtra, India

[2] Professor, Department of Electronics Engineering, Amrutvahini College of Engineering, Sangamner, Maharashtra, India

ABSTRACT: In WSN, data from various sensor nodes is aggregated at aggregating node, which is usually done by simple techniques such as averaging as limited computational power and energy resources. However such aggregation is known to be highly vulnerable to node compromising attacks. These methods are highly susceptible to attacks as WSN are usually without tamper resistant hardware. Thus, determination of trustworthiness of data and reputation of sensor nodes is crucial for wireless sensor networks. Thus, Future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable, as the performance of very low power processors dramatically improves. Iterative filtering algorithms hold great promise for such a purpose. As assigned the corresponding weight factors to data provided by each source, such Iterative algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources. While significantly more robust against collusion attacks than the simple averaging methods, are still susceptible to a novel sophisticated collusion attack introduce. For these security issue, enhanced iterative filtering techniques are introduced which are more robust to collusion attacks and accurate.

KEYWORDS: Wireless sensor networks, Collusion attack, Robust data aggregation, Iterative Filtering Algorithms.

I. INTRODUCTION

Sensor nodes cooperatively send sensed data to base station which forms sensor networks data. These wireless sensor networks (WSNs) are usually redundant due to a need for robustness of monitoring and low cost of the nodes. At an aggregator node the data from multiple sensors is aggregated. As sensor nodes required computing power and energy source, it is essential to use an efficient amount of power in order to use networks for long duration [1].The main objective of data aggregation algorithms is to collect data and aggregate that data in an energy efficient manner so that lifetime of network is enhanced. Thus, at the present, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is very vulnerable to faults, and more importantly, detrimental attacks [1]. As the attackers generally can access the information stored in the compromised nodes completely, this cannot be solved by cryptographic methods only. As the traditionally encryption is used to provide complete confidentiality in sensor network, the aggregators in secure data aggregation it is need to decrypt the encrypted data to perform aggregation. But as it exposes the plaintext at the aggregators, this makes the data vulnerable to attacks from an adversary. Also an aggregator can inject false data into the aggregate and allow the base station accept false data. Thus, data aggregation improves energy efficiency of a network but it complicates the existing security challenges. For that reason data aggregation at the aggregator node has to be concentrate on estimation of steadiness of data from individual sensor nodes. Thus, for enhancement more practical algorithms are needed for data aggregation in the WSN which contain two main features.

In the presence of stochastic errors such algorithm should estimates the values which are close to the optimal ones in information theoretically. That is, if the noise present in each sensor is a Gaussian independently distributed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

noise with a zero mean, then the estimation produced by these algorithms should have a variance close to the Cramer-Rao lower bound (CRLB), thus, it should be also close to the variance of the Maximum Likelihood Estimator (MLE). However, this is unavailable in practice because that estimation should be obtained without transferring to the algorithm the variances of the sensors. In the presence of non-stochastic errors, this algorithm should also be robust, such as faults and malicious attacks, and, beyond aggregating data, such algorithm should also provide an appraisal of the reliability and trustworthiness of the data received from the sensor nodes.

Iterative Filtering (IF) algorithms are good option for wireless sensor networks because they clarify both complications like data aggregation and data trustworthiness assessment using a single iterative procedure [5]. Such steadiness estimate of each sensor is depend on the distance of the readings of such a sensor from the estimation of the correct values, obtained in the earlier round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is commonly a weighted average.

II. RELATED WORK

Simple data aggregation is highly susceptible to node compromising attacks and produces invalid data. Also the existing system lack in accuracy and faster while aggregating data which decrease the performance in the presence of non-stochastic errors, such as faults and malicious attacks. By simple data aggregation it is easily affect by exploiting false data injection through a number of compromised nodes.

Robust data aggregation is a serious concern in WSNs and there are a number of papers investigating malicious data injection by taking into account the various adversary models. The main research is around : Iterative filtering algorithms, certainty and reputation systems for WSNs, and secure data aggregation with compromised node detection in WSNs. There are a number of published studies introducing IF algorithms for solving data aggregation problem [4], [5], [6]. Li et al. The paper proposed by H.L.Shi [7] intoduces six different algorithms, which are all iterative and are similar and the only difference among the algorithms is their choice of norm and aggregation function. Ayday et al. proposed a slight different iterative algorithm in [8]. Their main differences from the other algorithms : 1) The ratings have a time-discount factor, so after time their importance will fade out; and 2) The algorithm maintains a black-list of users who are especially bad raters. Liao et al. proposed an iterative algorithm which beyond simply using the social network of users , also uses the rating matrix.

We Introduced the several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are still attackable to a novel sophisticated collusion attack we introduce. The performance of IF is approved by simulation on synthetically generated data sets. According to simulation results it clarify that the robust aggregation technique is effective in terms of robustness against the novel sophisticated attack as well as capable in terms of the computational cost. based on biased and unbiased readings in specified location, the sensor errors are estimated. IF provides greater accuracy and better collusion resistance than the other method.

III. PROPOSED SYSTEM

Figure 1 shows the architecture diagram of proposed system. User can enter into existing network topology if user is valid. We consider mobile database for experiment. These sensor database is first loaded at server. Server forward this data to aggreagator. After that it distributed into subdata according to no of clients. After encryption is done these clients forward this data to the aggregator again.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

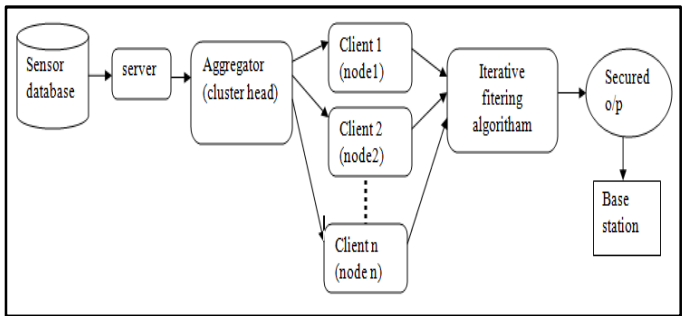

Fig.[1]:System Architecture.

At the aggregator , iterative filtering algorithm is applied and it estimate MLE with known variance which helps to check iscollusion attack is done or not. After that secured data is send to base station.

A. Robust data aggregation framework

Robust data aggregation is done at the cluster head, like Identification of a new sophisticated collusion attack which reveals a severe susceptibility of IF algorithms;

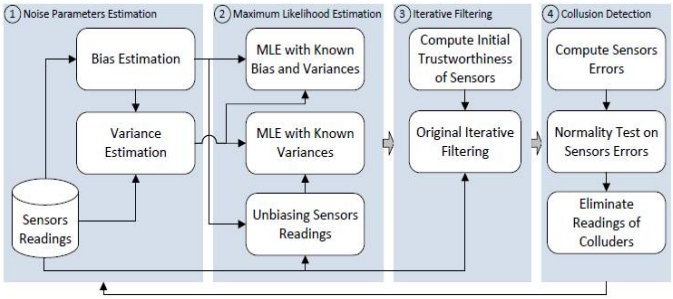

Fig.[2]:Robust data aggregation[1]

A method for estimation of sensors' errors which is effective in a range of sensor faults which solve collusion attack as; Using MLE, it design an efficient and robust aggregation method, which utilizes an estimate of the noise parameters; Improved IF able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs.

B. Bias Estimation

Assume that all sensor have some error denoted by $e^{t}_{s\ of}$ sensor s with sensor bias b_s and sensor variance σ_s.By setting the gradient of F(b) to zero we obtain a system of linear equations whose solution is our approximation of the bias values and they are written in following compact form

$$x_s^t = r_t + e_s^t \qquad (1)$$

$$\sum_{\substack{i=0 \\ j\neq 0}}^{n} \frac{2}{d(i,j)^2}\, bi - \sum_{\substack{i=0 \\ j\neq 0}}^{n} \frac{2}{d(i,j)^2} b_k - \gamma = \sum_{\substack{i=0 \\ j\neq 0}}^{n} \frac{2}{d(i,j)},$$

For all k= 1…., n

$$\sum_{i=1}^{n} b_i = 0 \qquad (2)$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

C. Variance Estimation,MLE with known variance:

We can now obtain an estimation which corresponds to MLE formula for the case of zero mean normally distributed errors, but with estimated rather than true variances. Thus, in the expression for the likelihood function for normally distributed unbiased case. Therefore, we assume that the expected value r_t of the measurements is the true value of the quantity measured, and is the only parameter in the likelihood function.

$$\mathcal{L}_n(r_t) = \prod_{i=0}^{n} \frac{1}{\sigma_i\sqrt{2\pi}} e^{-\frac{1}{2}\frac{\left(x_i^t - r_t\right)^2}{\sigma_i^2}} \quad (3)$$

By differentiating the above formula with respect to r_t and setting that equal to zero, we obtain,

$$r_t = \sum_{i=1}^{n} \frac{\frac{1}{v}}{\sum_{j=1}^{n} \frac{1}{v_j}} x_i^t \quad (4)$$

Above equation gives the estimation of true value of measurement in a form of weighted average of sensor readings.

IV. EXPERIMENTAL RESULTS

At the sever we load the mobile database from sensor database, this data is then aggregated at aggregator and generate patter recongnization from that database as shown in figure 3.At the aggregator this data is then distributed according to the no of clients i.e. cluster heads. In this module the weighted factor is assigned to each source in the network. The individual id specifies the node location by allocating weight factor to each node. Figure 3 Shows that each node is specified by their location by assigning weight factor. The allocation of weight factor is based on the computational energy need in any form of network. In this module the number of nodes connected into the network can also be identified.

Fig.[3]: Loaded mobile data from sensor database

This weighted data is then distributed to the clients. Using IP address of each client we can add no. of clients for data distribution. At the client, this data is the received from aggregator and it after encryption it again forwarded to the aggregator, here we consider these clients as a node and one client acts as a adversary node. After completing file transfer from each client to the aggregator, at the aggregator it estimates the bias and variance and using MLE with known variance it determine that which client has done changes in data i.e. adversary node is detected.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

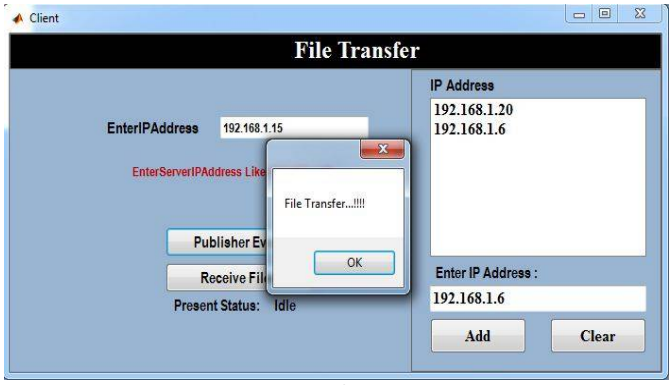

Fig.[4]: File transmission from aggregator to clients.

Figure 4 specifies the secure data aggregation using Iterative Filtering technique. It is a tool for maximum likelihood inference on partially observed dynamical systems. Stochastic reputations to the unknown parameters are used to explore the parameter space. Compare the different iterative value to provide the rank for each iteration. The highest rank iteration occurs more error and then this error is avoided using IF technique.

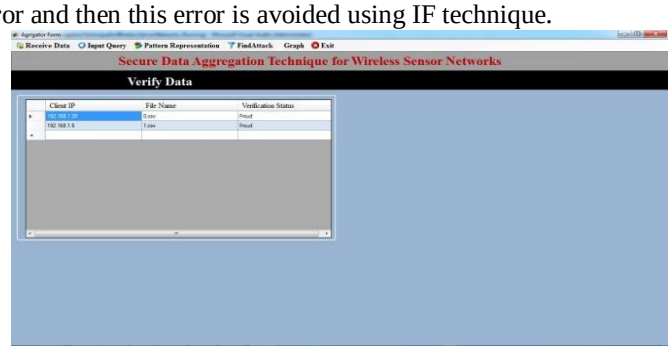

Fig.[5]: Collusion attack detection using IF.

We compare our system with other iterative filtering algorithm, which gives the following result according to bias and varinace estimation with known MLE variance.

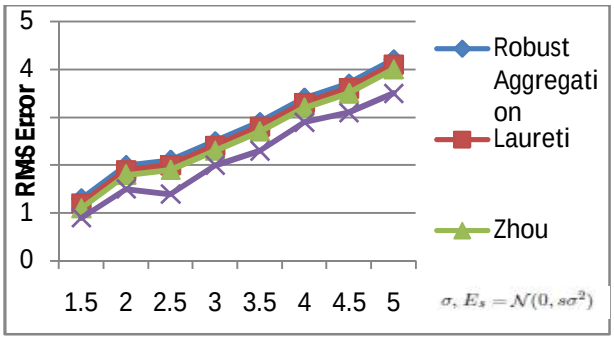

Fig.[6]: Graph of comparison of different IF algorithm with proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

V. CONCLUSION

In wireless sensor network needs the high computational cost and power need for transmitting the data. To reduce that data aggregation technique is used in WSN. This data aggregation is done by using various simple methods such as averaging but this technique is highly vulnerable. In proposed system, we introduced Iterative filtering algorithms with initial estimation by giving weighted factors which makes algorithm collusion robust, accurate and fast converging. In future work, we will investigate whether it can protect against compromised sensornodes in a deployed sensor network.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
[2] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in Proceedings of the 5 th International Workshop on Security and Trust Management, Saint Malo, France, 2009.
[3] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN '10, 2010, pp. 2–7.
[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surv., vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.
[5] 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.
[6] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 8, pp. 1525–1534, Aug 2013.
[7] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," CoRR, vol. abs/1012.3793, 2010.
[8] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," in Proceedings of the 2009 IEEE international conference on Symposium on Information Theory,Volume 3, ser. ISIT'09, 2009, pp. 2051–2055
[9] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A Statistical Mechanics and its Applications, vol. 371, pp. 732–744, Nov. 2006.
[10] 11. P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via Iterative Refinement," EPL (Europhysics Letters), vol. 75, pp. 1006–1012, Sep. 2006.