Aggregation Technique for Wireless Sensor Networks

V.SAKTHI PRIYANKA Asst.Professor,
Department of PGCS & IT
AJK College of Arts and Science

Abstract:

Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce. To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.

.1. Introduction

Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic meth- ods, because the attackers generally gain complete access to information stored in the compromised nodes. For that rea- son data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisti- cated algorithms are needed for data aggregation in the future WSN. Such an algorithm should have two features.

1. In the presence of stochastic errors such algorithm should produce estimates which are close
2. The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algo-rithm should also provide an assessment of the reli- ability and trustworthiness of the data received from each sensor node.
3. Identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms.
4. A novel method for estimation of

sensors' errors which is effective in a wide range of sensor faults and not susceptible to the described attack.

5. Design of an efficient and robust aggregation method inspired by the MLE, which utilises an estimate of the noise parameters obtained
6. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions 2 and 3 above.

2. Approaches Used

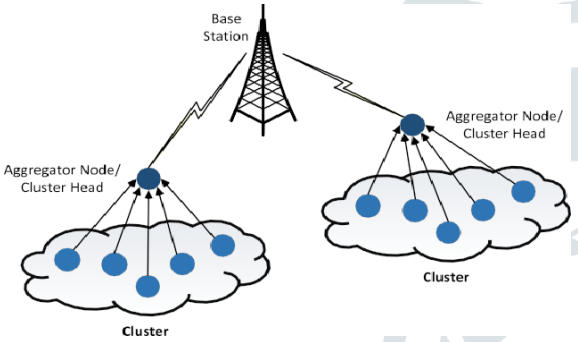


Fig. 1. Network model for WSN.

Sensors exhibiting a very small belief divergence at any given round of iteration. Therefore, under an attack of the kind described, the reputation value of the first iteration is equal to the simple average of readings, and the second vec-tor of weights is computed based on the distance of each sensor to the simple average provided by the first iteration. As most of the IF algorithms in the literature make the same assumption about the initial trustworthiness of sensors, we argue that an adversary with sufficient knowledge of such algorithms can launch an attack as we have described and deceive the aggregator node.

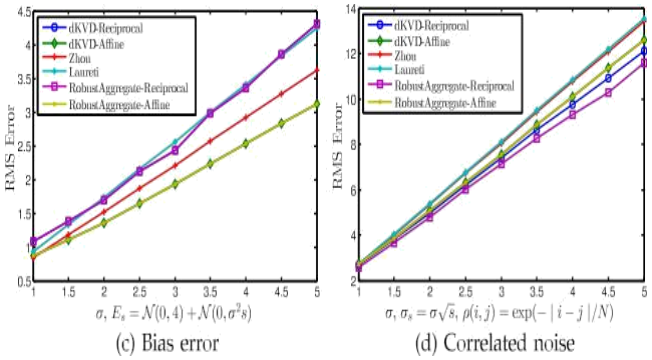
In the case in which the nodes use cryptography to ensure the confidentiality of readings they send to the aggregator, the adversary can still estimate these readings by sensing the measured quantity using the malicious nodes.

To address the shortcoming of existing IF methods, we focus on estimating an initial trust vector based on an esti- mate of error parameters of sensor nodes. After that, we use the new trust vector as the initial sensor trustworthiness in order to consolidate the algorithms against an attack sce- nario of the type described.

3. Related Survey

The objective of our experiments is to evaluate the robustness and efficiency of our approach for estimating the true values of signal based on the sensor readings in the presence of faults and collusion attacks. For each experiment, we evaluate the accuracy based on Root Mean Squared error (RMS error) metric and efficiency based on the number of iterations needed for convergence of IF algorithms.

The first IF method considered computes the trustwor- thiness of sensor nodes based on the distance of their readings to the current state of the estimated reputation The second IF method we consider is a correlation based ranking algorithm proposed by Zhou et al. in [9]. In this algorithm, trustworthiness of each sensor is obtained based on the correlation coefficient between the sensors readings and the current estimate of the true value of the signal. In other words, this method gives credit to sensor nodes whose readings correlate well with the estimated true value of the signal. Based on this idea, the authors proposed an iterative algorithm for estimating the true value of the signal by applying a weighted averaging technique. They argued that correlation coefficient is a good way to quantify the similarity between two vectors. Thus, they employed Pearson correlation coefficient between sensor readings and the cur- rent state of estimate signal in order to compute the sensor weight. We call this method *Zhou*.



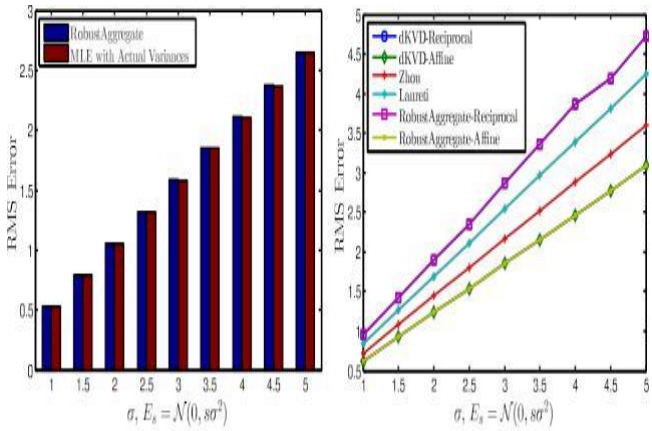
(c) Bias error (d) Correlated noise

4. Problem Formulation

In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. Wireless sensor nodes has been used for the sensing the information from harsh environment. In these nodes sensors of different types has been used for collecting information. Wireless sensor networks are of main two types, which are static wireless sensor nodes and mobility wireless sensor networks. In MWSNs t5he main threat in the network is security. Various types of attacks occurred in these networks. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate.

6. Results and Discussions

Sharing of tables is use for the detection of nodes from the replication.



(a) Unbiased error (b) Unbiased error

7. Conclusion

In this paper, we introduced a novel collusion attack sce- nario against a number of existing IF algorithms. More-over, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthi- ness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, We will investigate whether our approach can protect against compromised aggrega- tors. we also plan to implement our approach in a dep- loyed sensor network.

Refrences:

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sen- sor networks: A comprehensive overview," *Comput. Netw.*, vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, *All of Statistics : A Concise Course in Statistical Infer- ence*. New York, NY, USA: Springer,.

[3] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputa- tion systems," in *Proc. 5th Int. Workshop Security Trust Manage.*, Saint Malo, France, 2009, pp. 253–262.

[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Sur- veys*, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[5] R. Roman, C. Fernandez-Gago, J.

Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in *Security and Privacy in Mobile and Wireless Networking*, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,.

[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trust- worthiness assessment in sensor networks," in *Proc. 7th Int. Work- shop Data Manage. Sensor Netw.*, 2010, pp. 2–7.

[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E^2*MWSN*," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, 2011, pp. 1–4.

[8] C. de Kerchove and P. Van Dooren, "Iterative filtering in reputa- tion systems," *SIAM J. Matrix Anal. Appl.*, vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," *Europhys. Lett.*, vol. 94, p. 48002, 2011.

[10] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information fil- tering via iterative refinement," *Europhys. Lett.*, vol. 75, pp. 1006– 1012, Sep. 2006.

[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding infor- mation from noisy, redundant, and intentionally distorted sources," *Physica A: Statist. Mech. Appl.*, vol. 371, pp. 732–744, Nov. 2006.

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

[13] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," *Proc. IEEE Int. Conf. Symp. Inf. The- ory*, vol. 3, 2009, pp. 2051–2055.

[14] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," in *Proc. 20th Int. Conf. Found. Intell. Syst.*, Aug. 2012, pp. 405–414.

[15] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment," in *Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2011, pp. 159–167.

[16] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor net- works in the presence of sensor faults," *IEEE Trans. Parallel Dis- trib. Syst.*, vol. 24, no. 8, pp. 1525–1534, Aug. 2013.

[17] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.