

## SCALABLE AND SECURE DATA AGGREGATION TECHNIQUE FOR WSN IN THE OCCURRENCE OF CONSPIRACY ATTACKS

Ravi Teja Kumar Nallabathina<sup>1</sup> and Asiff Shaik<sup>2</sup>

Dept Of Computer Science

<sup>1</sup> PG Scholar, <sup>2</sup>Assistant professor, GIST, Nellore, India.

<sup>1</sup>[tejravi186@gmail.com](mailto:tejravi186@gmail.com), <sup>2</sup>[asiffali.shaik@gmail.com](mailto:asiffali.shaik@gmail.com)

### 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. To address security issue, an improvement for iterative filtering techniques is proposed by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.

## INTRODUCTION

Due to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks are usually redundant. 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 methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN.

In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. Thus, for example, if the noise present in each sensor is a Gaussian independently distributed noise with zero mean, then the estimate produced by such an algorithm should have a variance close to the

Cramer- Rao lower bound (CRLB) , i.e, it should be close to the variance of the Maximum Likelihood Estimator (MLE). However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice.

The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node.

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system. The main target of malicious attackers are

aggregation algorithms of trust and reputation systems .

## **II.RELATED PROBLEM**

Trust and reputation have been recently suggested as an effective security mechanism for Wireless Sensor Networks. Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data becomes a challenging task.

Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems data aggregation and data trustworthiness assessment using a single iterative procedure. Trustworthiness estimate of each sensor is based on the distance of the readings of a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors.

Such aggregation is usually a weighted average; sensors whose readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight. Iterative Filtering algorithms research did not take into account more sophisticated

collusion attack scenarios. If the attackers have a high level of knowledge about the aggregation algorithm and its parameters, they can conduct sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes.

## **III.PROBLEM ANALYSIS**

To propose a solution for vulnerability by providing an initial trust estimate, which is based on a robust estimation of errors of individual sensors. To Identify a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms. 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.

To design an efficient and robust aggregation method inspired by the MLE, which utilises an estimate of the noise parameters. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors.

## **IV.IMPLEMENTATION**

### **SENSOR NODE**

The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are

periodically collected and aggregated by the aggregator.

### REPUTATION MODEL

Each sensor node can identify its neighbor nodes and fix reputation for its neighbors. A sensor node can fix sensor node weight/reputation by giving 0 or 1, 0 refers to normal node, whereas 1 refers to attacker node. Reputation for any can be fixed by its neighbor node and it will be updated in sensor database.

### SENSOR DATA

Every sensor node in particular location will send a reading to its cluster head. It is assumed that sensors are reading a data of numerical value in range of 19.00 to 19.99 and the reading are sent to cluster head for aggregation.

### DATA AGGREGATION

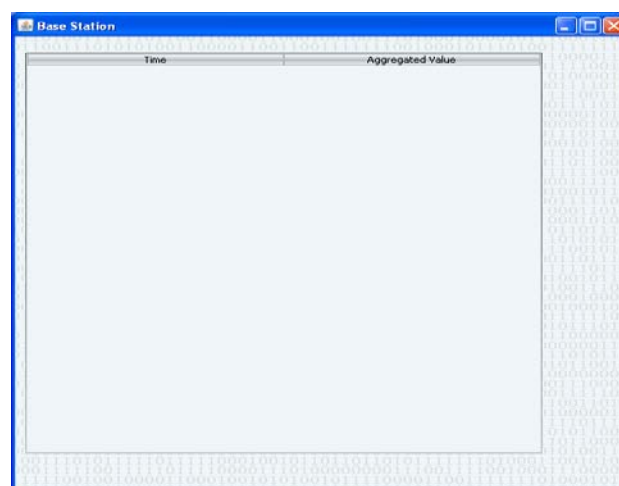
We consider a WSN with  $n$  sensors  $S_i, i = 1; \dots; n$ . We assume that the aggregator works on one block of readings at a time, each block comprising of 10 readings at  $m$  consecutive instants. It is assumed that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator. Each data aggregator has

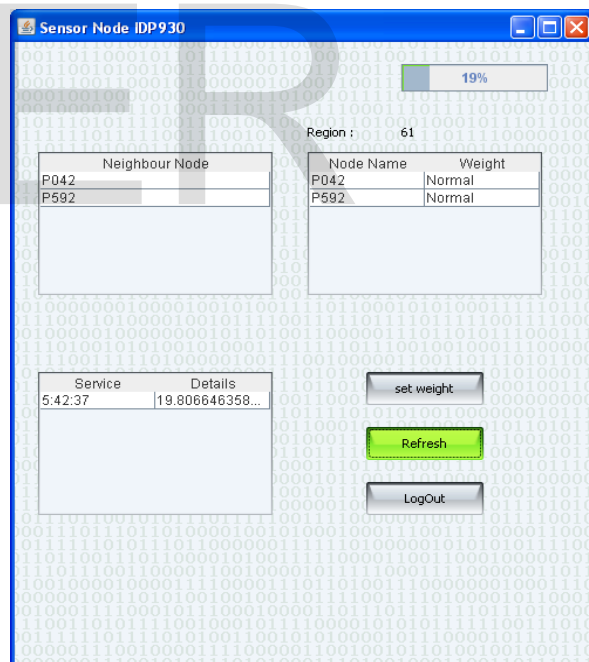
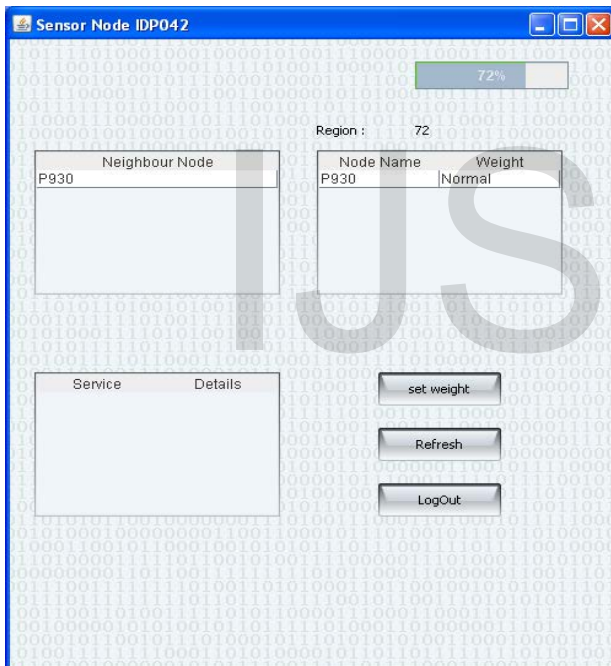
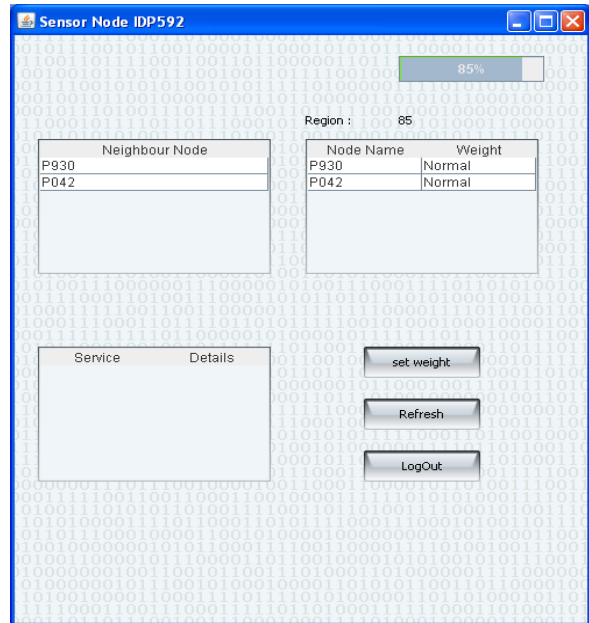
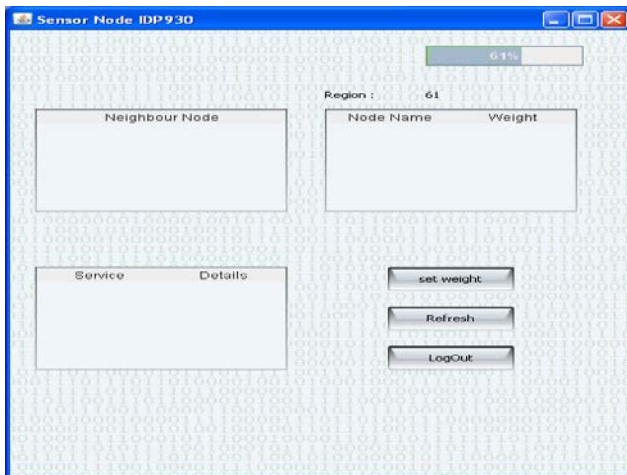
enough computational power to run an IF algorithm for data aggregation.

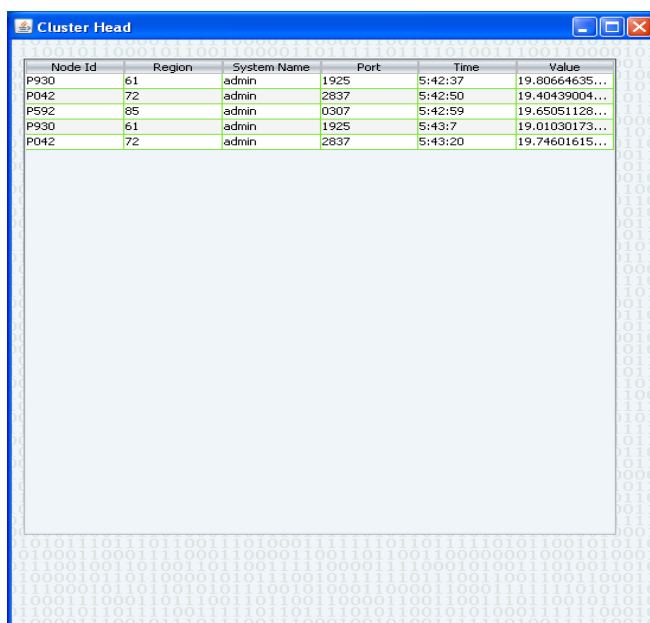
### FIND COLLUSION ATTACK

Through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of distorting the aggregate values. Compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack. The data from attacker node is identified by cluster head and it is dropped from aggregation. Only legitimate readings are aggregated and sent to cluster head.

## V.RESULT ANALYSIS







Node Id	Region	System Name	Port	Time	Value
P930	61	admin	1925	5:42:37	19.80664635...
P042	72	admin	2837	5:42:50	19.40439004...
P592	85	admin	0307	5:42:59	19.65051128...
P930	61	admin	1925	5:43:7	19.01030173...
P042	72	admin	2837	5:43:20	19.74601615...

## VI.CONCLUSION

A novel collusion attack scenario against a number of existing IF algorithms is proposed. Moreover, an improvement for the IF algorithms is proposed 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. In future work, investigate whether this approach can protect against compromised aggregators.

## 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] L. Wasserman, *All of Statistics : A Concise Course in Statistical Inference*. New York, NY, USA: Springer,.
- [3] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation 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. Surveys*, 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 trustworthiness assessment in sensor networks," in *Proc. 7th Int. Workshop 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: E2MWSN,” 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 reputation 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 filtering via iterative refinement,” Europhys. Lett., vol. 75, pp. 1006–1012, Sep. 2006.