International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Analysis of Secure Data Aggregation Technique for Wireless Sensor Network

Kandika Praveen Kumar
M.Tech, Computer Science & Engineering
Jayamukhi Institute Of Technological Sciences,Warangal.

Abstract: As we have now confined energy resources and computational power, data aggregation from multiple sensor nodes is completed using easy approaches equivalent to averaging. WSN's are quite often unattended, they're extremely vulnerable to node compromising assaults. As a result making it essential to determine trustworthiness of data and reputation of sensor nodes is valuable for WSN. Iterative Filtering algorithms have been learned to be very useful in this rationale. Such algorithms participate in data aggregation and provide trustworthiness comparison to the nodes within the form of weight explanations.These algorithms concurrently combination data from more than one sources and furnish a trust estimation of these sources, by and large in a type of corresponding weight explanations assigned to data provided with the aid of each and every source.

Key Words: Collusion Attacks,data ggregation,Iterative Filtering Algorithm,wireless sensor network.

I. INTRODUCTION

A wi-fi sensor network (WSN) includes a group of those nodes which have the power to experience, system data and keep up a correspondence with each and every other by way of a wireless connection. Wireless sensor networks (WSN's), the development in sensor technology has made it viable to have very small, low powered sensing instruments geared up with programmable compute, multiple parameter sensing and wi-fi message capacity. Also, the low rate makes it feasible to have a network of thousands or enormous quantities of these sensors, thereby improving the consistency and accuracy of data and the area coverage. Wi-fi sensor networks present data about isolated buildings, wide-unfold environmental alterations, and so forth. Wireless sensor network (WSN) is a network approach constituted of spatially disbursed gadgets making use of wireless sensor nodes to watch bodily or environmental crisis, similar to sound, temperature, and movement.

Trust and repute programs have a giant role in aiding operation of a huge range of distributed programs, from wireless sensor networks and e-commerce infrastructure to social networks, with the aid of offering an assessment of trustworthiness of members in such disbursed programs. A trustworthiness comparison at any given moment represents an aggregate of the habits of the contributors as much as that moment and needs to be effective within the presence of various varieties of faults and malicious habits. There are a quantity of incentives for attackers to govern the believe and status scores of contributors in a distributed process, and such manipulation can severely impair the performance of any such procedure. The most important goal of malicious attackers are aggregation algorithms of trust and repute systems. A sensor network is designed to participate in a suite of highlevel data processing duties equivalent to detection, track, or categorization. Measures of efficiency for these tasks are good defined, including discovery of false alarms or misses, classification errors, and monitor fine. Because the computational power of very low power processors dramatically increases, ordinarily pushed by demands of cell computing, and as the fee of such technology drops, WSNs will likely be equipped to come up with the money for hardware which will put into effect more refined data aggregation and believe assessment algorithms; an illustration is the latest emergence of multi-core and multiprocessor programs in sensor nodes.

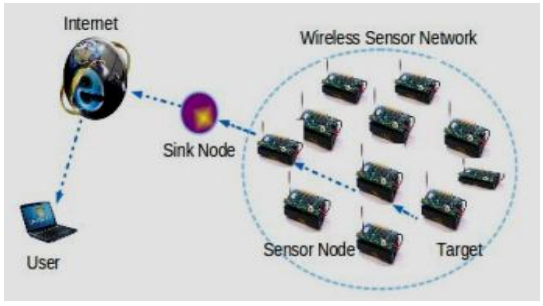


Fig.1: An operating system of a WSN

Iterative Filtering (IF) algorithms are an appealing alternative for WSNs considering that they solve each problems - data aggregation and data

trustworthiness evaluation - utilizing a single iterative method. Such trustworthiness estimate of each sensor is based on the distance of the readings of this type of sensor from the estimate of the correct values, acquired in the earlier circular of iteration by some type of aggregation of the readings of all sensors. Such aggregation is mainly a weighted normal; sensors whose readings tremendously range from such estimate are assigned less trustworthiness and consequently in the aggregation system within the ability round of new release their readings are given a control weight.

II. RELATED WORKS

In this paper [3] He, W., Liu, X., Nguyen, H. V., Nahrstedt, k., and Abdelzaher, T, they reward one privacy -retaining data aggregation scheme for additive aggregation capabilities, which can be huge to approximate MAX/MIN aggregation perform. The primary process Cluster-based private data Aggregation (CPDA) -leverages clustering protocol and algebraic residences of polynomials. It has the competencies of incur less conversation overhead. The second scheme Slice–mix-aggregate(intelligent) builds on cutting strategies and the associative property of addition.

In[4] Carlos R. Perez-Toro, Rajesh okay. Panta, Saurabh Bagchi on this paper RDAS, a robust data aggregation protocol that use a fame-founded strengthen to admire and cut off cruel nodes in a sensor network. RDAS is centered on a hierarchical cluster form of nodes, where a cluster head clarify data from the cluster nodes to find out the vicinity of an occasion. It makes use of the repetition of a couple of nodes experience an occasion to decide what data must have been reported by each node. RDAS is able to execute accurate data aggregation within the presence of independently hateful and collude nodes, as good as nodes that attempt to compromise the integrity of the fame method by using lying about other nodes‟ conduct.

In [1] S. Ganeriwal, L. Okay. Balzano, and M. B. Srivastava, Our work can also be carefully concerning the believe and reputation programs in WSNs. Authors proposed a common reputation framework for sensor networks in which every node develops a reputation estimation for different nodes by way of looking its neighbors which make a believe neighborhood for sensor nodes within the network.

In [6] Suat Ozdemir ,Yang Xiao presents data aggregation is the system of summarizing and combining sensor data with a purpose to lower the quantity of data transmission in the network. As wireless sensor networks are often deployed in faraway and adverse environments to transmit sensitive messages, sensor nodes are susceptible to node compromise attacks and security issues equivalent to data confidentiality and integrity are very foremost. As a consequence, wi-fi sensor procedure protocols, e.g., data aggregation protocol, need to be deliberate with safety in mind. This paper investigate the connection between protection and data aggregation method in wi-fi sensor networks. A taxonomy of secure data aggregation approach is given through surveying the current “state-of-the-art” work in this neighborhood. Moreover, based on the existing gain data of, the open study areas and future study directions in relaxed data aggregation thought are supplied.

In [8] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee proposed a trust situated framework which employs correlation to realize inaccurate readings. Additionally, they presented a ranking framework to accomplice a stage of trustworthiness with every sensor node founded on the number of neighboring sensor nodes are assisting the sensor.

III. NETWORK MODEL

A WSN consists of small-sized sensor instruments, which are organized with constrained battery power and are capable of wireless communications. When a WSN is deployed in a sensing area, these sensor nodes will be liable for sensing irregular hobbies or for accumulating the sensed data of the environment. Within the case of a sensor node detecting an abnormal occasion or being set to periodically file the sensed data, it will send the message hop-byhop to a specific node, called a sink node.

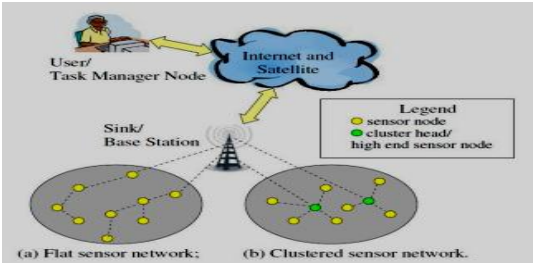


Fig.2: Network model of a WSN

The sink node will then inform the supervisor via the internet. The sensor nodes are divided into disjoint clusters, and every cluster has a cluster head which acts as an aggregator. Information are periodically together and aggregated by way of the aggregator.

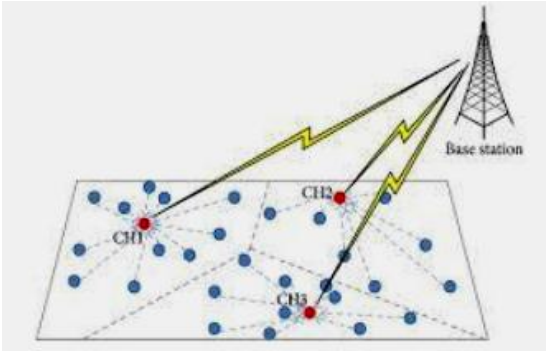


Fig. 3: Cluster head communication

IV. PROPOSED METHOD

Within the wireless sensor community contains sensor nodes these sensor nodes are scattered then deployed environment within the network and then to form the cluster ,each cluster has a cluster head after which data send to the aggregator node earlier than sending base station to verify the data, if any, error in the data, then to estimate the value utilising parameters such as bias and variance and in addition estimate MLE utilizing an iterative filtering algorithm The proposed approach architecture view can also be proven in Fig.4.

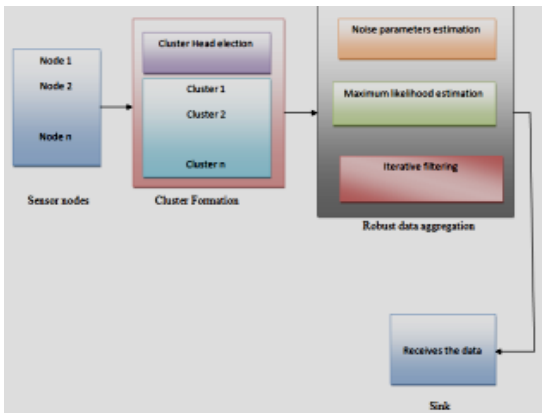
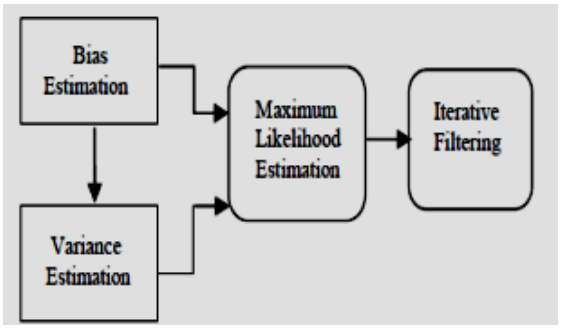


Fig .4 Proposed system architecture

A. Robust data aggregation framework

Robust data Aggregation model operates on batches of consecutive readings of sensors, continuing in a number of levels. In the first stage furnish an initial estimate of two noise parameters for sensor nodes, bias and variance details of the computations for estimating bias and variance of sensors. A novel technique for estimating the bias and variance of noise for sensors based on their readings. The variance and the bias of a sensor noise can be interpreted as the gap measures of the sensor readings to the genuine worth of the signal. In fact, the gap measures got as our estimates of the bias and variances of sensors additionally make sense for non-stochastic mistakes. Based on such an estimation of the bias and variance of each sensor, the bias estimate is subtracted from sensor readings and in the subsequent section of the proposed framework, we furnish an preliminary estimate of the reputation vector calculated making use of the MLE as proven in Fig 4.



A. Bias Estimation

All sensors may have some errors in their readings. Such error is denoted as e^t_s Of sensor is and it is modelled by the Gaussian distribution random variable with bias b_s And variance σ_s. Let rs Denotes the true value of the sensor at time t. Sensor readings x_s^t can be written as

$$x_s^t = r_s + e^t_s \qquad (1)$$

Since there is no true value, the error value of sensors is not to be found. But the difference values of such sensors are calculated with the equation given below. Let $\delta = \delta(i, j)$be an estimator for mutual difference of sensor bias.

$$\delta(i,j) = \frac{1}{m}\sum_{t=0}^{m}(e_i^t - e_j^t) = \frac{1}{m}\sum_{t=1}^{m} e_i^t = \frac{1}{m}\sum_{t=1}^{m} e_j^t \qquad (2)$$

$$a_i = \frac{1}{m}\sum_{t=1}^{m} e_i^t$$

variable and m be the number of readings for each sensor.Then the expected value is calculated by minimizing the obtained value with respect to the mean value and the equation is given below

$\delta(i, j)=ai-aj \approx bi-bj \qquad (3)$

B. Variance Estimation

With the known values of bias estimated from the equation 3 the variance of sensor errors are calculated.Each sensor bias value is substracted from the sensor readings.By using the error difference value from the equation 2 we can get the variance value as a squared difference of each sensor error and the bias value.This varies upto the last sensor reading and is defined as

$$\beta(i,j) = \frac{1}{m-1}\sum_{t=0}^{m}(e_i^t - b_i))^2 = \frac{1}{m-1}\sum_{t=1}^{m}(e_i^t - b_i))^2$$

(4)

C. Maximum Likelihood Estimation

The unbiasing sensor readings are extracted and take place with help of the bias estimated result which is calculated from the above section.After that the variance estimated result from equation 4 is considered.and the extracted unbiasing sensor is used to make the maximum likelihood estimation with variance value By differentiating the likelihood function the true values are obtained and are measured in the form of weighted average. It is defined as $r = \sum_{s=1}^{n} W_s X_s$ (5)

Thus it estimates the reputation vector without any iteration. Hence the computational complexity of the estimation is less than the existing IF algorithms.

V. CONCLUSION

Data aggregation mechanisms together with information averaging procedures are analysed. Network model proposed with the aid of Wagner is described for sensor network community. Adversary items with their assumptions are reviewed. New refined collusion attack situations along with its affect on wi-fi sensor networks is defined. As soon as computational power of very low power processors drastically improves, future aggregator nodes will likely be competent of performing extra tricky data aggregation algorithms, as a consequence making wi-fi sensor networks less vulnerable.

REFERENCES

[1] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputationbased framework for high integrity sensor networks,” ACM Trans. Sen. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.

[2] Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: a secure hop by hop data aggregation protocol for sensor networks,” in MobiHoc, 2006, pp. 356–367.

[3] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T. 2011. “Privacy preserving data aggregation for information collection "ACM Transaction Sensor Network. Article 6 (August 2011.DOI = 10.1145/1993042.199)3048.

[4] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenancebased 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.

[5] S. Roy, M. Conti, S. Setia, , and S. Jajodia, “Secure data aggregation in wireless sensor networks,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1040–1052, 2012.

[6]H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, “Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN,” in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1–4.

[7] B. Awerbuch, R. Curtmola, D. Holmer, C. Nitarotaru, and H. Rubens, “Mitigating byzantine attacks in ad hoc wireless networks,” Department of Computer Science, Johns Hopkins University, Tech, Tech. Rep., 2004.

[8] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, “Using SensorRanks for in-network detection of faulty readings in wireless sensor networks,” in Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, ser. MobiDE "07, 2007, pp. 1–8.

[9]. J. Bahi, C. Guyeux, and A. Makhoul, “Efficient and robust secure aggregation of encrypted data in sensor networks,” in Fourth International Conference on Sensor Technologies and Applications, July 2010.

[10]. L.-A. Tang, X. Yu, S. Kim, J. Han, C.-C. Hung, and W.-C. Peng, “Tru-Alarm: Trustworthiness analysis of sensor networks in cyberphysical systems ” ,IEEE International Conference on Data Mining , 2010.

Author Profile

Kandika Praveen Kumar pursing M.Tech in Computer Science & Engineering from **Jayamukhi Institute Of Technological Sciences,Warangal.**