ISSN: 2321-7782 (Online)
Volume 3, Issue 12, December 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Secure Data Aggregation Technique for Wireless Sensor Networks in Deployed Sensor Networks

Nikita P. Pareek[1]
Comp dept. LGNSCOE
Nasik, India

N. R.Wankhade[2]
Professor
Comp dept. LGNSCOE, Nasik, India

Abstract: ***As we have limited energy resources and computational power, data aggregation from multiple sensor nodes is done using simple methods such as averaging. WSN's are usually unattended they are highly vulnerable to node compromising attacks. Thus making it necessary to ascertain trustworthiness of data and reputation of sensor nodes is crucial for WSN. Iterative Filtering algorithms were found out to be very helpful in this purpose. Such algorithms perform data aggregation and provide trustworthiness assessment to the nodes in the form of weight factors. These algorithms are susceptible to the most sophisticated collusion attack scenario presented in this paper. To address this security issue we present the improved iterative filtering algorithm which are more accurate and fast converging.***

Keywords: Wireless sensor networks, robust data aggregation, collusion attacks, iterative filtering algorithm.

I. INTRODUCTION

Due to limitations of energy resource and computing power the data aggregation is done using simple averaging methods as a result these algorithms are more susceptible to malicious attacks [1] and these attacks cannot be solved using cryptographic methods because when the node is compromised attacker gains access to complete data stored in that particular node. Thus for this reason we need to ascertain trustworthiness of nodes. We need more sophisticated algorithm for aggregating data. Such algorithm should produce estimates which are close to the optimal ones in presence of stochastic errors.

The main target of malicious attackers is aggregation algorithms of the trust and reputation systems [2]. Trust and reputation systems are very effective mechanism providing security for Wireless Sensor Networks (WSN's) [3]. Sensors which are in the hostile environment are susceptible to attacks where attackers inject false data into system. So, assessing trustworthiness of data and announcing it to decision makers is challenging task.

Iterative algorithm is the best option for WSN's. It solves the problem of data aggregation and trustworthiness assessment by iterative procedure. The assessment of sensor is based on its distance of such readings from the estimated values by some form of aggregation. Sensors whose readings differ significantly have less trustworthiness and their reading get lower weight. In past research many iterative filtering algorithms are studied from that we may conclude that they provide better robustness than simple averaging technique but more sophisticated collusion attack scenario was not considered in past literature. Such vulnerability to sophisticated collusion attacks is observed because IF algorithms start the iteration process by giving an equal trust value to all sensor nodes. We propose a solution for such vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors. Stochastic errors essentially represent an approximation of the error parameters of sensor nodes in WSN such as bias and variance. Such initial estimation makes IF algorithms robust against sophisticated collusion attack and it is also more robust against general circumstances such as complete failure of some of the sensor nodes. This is in contrast with the traditional non iterative statistical sample estimation methods which are not robust against false data injection by a number of compromised nodes [4] and which can be severely skewed in the presence of a complete sensor failure.

II. Survey of Literature

In recent years, there has been an increasing amount of literature on IF algorithms for trust and reputation systems. There are two concepts we need to consider IF algorithms, trust and reputation systems for WSNs, and secure data aggregation with compromised node detection in WSNs. Li et al. in [5] proposed six different algorithms, all are iterative and similar. Their choice of norm and aggregation function is different. Liao et al. in [6] proposed an iterative algorithm which beyond simply using the rating matrix also uses the social network of users. None of these considered sophisticated collusion attack scenario.

We also came across much research on trust and reputation system in WSN's. Authors in [7] proposed a general reputation framework for sensor networks in which each node develops reputation estimation for other nodes by observing its neighbors which make a trust community for sensor nodes in the network. Tang et al. in [8] proposed a trust framework for sensor networks in cyber physical systems such as a battle-network in which the sensor nodes are employed to detect approaching enemies and send alarms to a command center. Although fault detection problems have been addressed by applying trust and reputation systems in the above research, none of them take into account sophisticated collusion attacks scenarios in adversarial environments.

Reputation and trust concepts can be used to overcome the compromised node detection and secure data aggregation problems in WSNs. Ho et al. in [9] proposed a framework to detect compromised nodes in WSN and then apply a software attestation for the detected nodes. They reported that the revocation of detected compromised nodes cannot be performed due to a high risk of false positive in the proposed scheme.

These studies focus on detecting false aggregation operations by an adversary. The problem of collusion and the problem of false data being provided by the data sources both are not addressed in the above literature. However, when an adversary injects false data by a collusion attack scenario, it affects the results of the honest aggregators and as a result the base station will receive skewed aggregate value. In this case, false data will be attested by the compromise nodes and thus all the reports are from honest sensor nodes is assumed by base station. Even if the mentioned research considers false data injection for a number of simple attack scenarios, collusion attack scenario by the compromised nodes has not been addressed anywhere.

III. Proposed System

a) Network Model

Fig. 1 shows network model in WSN. The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are regularly collected that are aggregated by the aggregator. Aggregator itself is not compromised is assumed and we concentrate secure aggregation when the individual sensor nodes might be compromised and might be sending false data to the aggregator. Each data aggregator has sufficient computational power to run an IF algorithm for data aggregation.

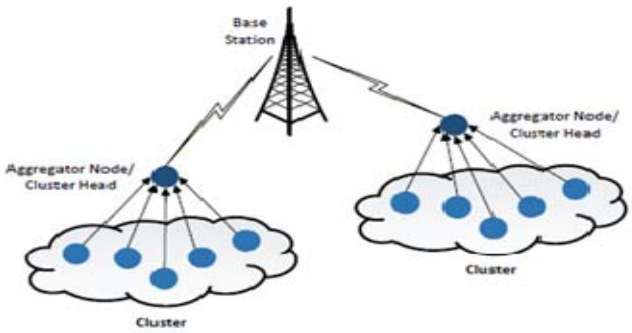

Fig. 1 Network Model of WSN.

b) Iterative filtering in reputation system

We briefly describe the algorithm in the context of data aggregation in WSN and explain the vulnerability of the algorithm for a possible collusion attack. We note that our improvement is applicable to other IF algorithms as well.

Algorithm: Iterative filtering algorithm.

Input: *X,n,m*.

Output: The reputation vector r

$l \leftarrow 0$;

$w(0) \leftarrow 1$;

Repeat

Compute $r\ (l+1)$

Compute d;

Compute $w\ (l+1)$

$l \leftarrow\ l + 1$;

Until reputation has converged;

- Where, we consider WSN with *n* sensors and we assume that aggregator work on one block of reading at a time each block consists of reading from *m* consecutive instants. Therefore the block of reading is represented by matrix *X*.
- *r* denotes the aggregated values it is called as a reputation vector computed with the sequence of weight *w*.
- The iterative procedure starts with giving equal credibility to all the sensors with initial value *w (0).*
- The value of the reputation vector $r\ (l+1)$in round of iteration $l + 1$ is obtained from the weights of the sensors obtained in the round of iteration *l.*
- The new weight vector $w\ (l+1)$ to be used in round of iteration $l + 1$ is then computed as a function g(d) of the normalized belief divergence d is the distance between the sensor reading and reputation vector $r\ (l)$.

This algorithm is the iterative filtering algorithm which is vulnerable to collusion attacks improvement to this algorithm is also applicable to other IF algorithms as well. We show that the algorithm converges in little iteration.

c) Collusion attack scenario

Most of the IF algorithms occupy simple assumptions about the initial values of weights for sensors. In case of our opponent model, an attacker is able to misinform the aggregation system from side to side cautious range of report data standards. Assume that ten sensors report the values of temperature which are aggregated using the IF algorithm planned in with the reciprocal discriminated function.

- In scenario 1, all sensors are dependable and the result of the IF algorithm is close to the actual value.
- In scenario 2, an adversary compromises two sensor nodes, and disturbs the readings of these values such average of all sensor readings is skewed towards a lesser value. As these two sensor nodes report a lower value, lower weights are assigned to them by IF algorithm, because their values are far from the values of other sensors. In other words, the algorithm is robust against false data injection in this scenario because the compromised nodes individually falsify the readings without any knowledge about the aggregation algorithm. The algorithm assigns very low weights to these two sensor nodes and consequently their contributions decrease.

» In scenario 3, in order to launch a collusion attack an adversary employs three compromised nodes. 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. It then computes the skewed value of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings.

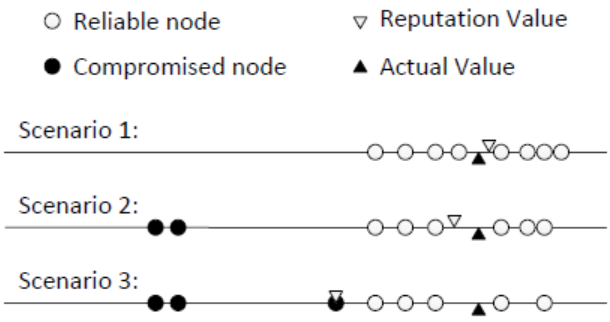

Fig. 2 Collusion attack scenario against IF algorithm.

d) Robust data aggregation

We need an initial estimation of the trustworthiness of sensor nodes which is to be used in the first iteration of the IF algorithm. Estimation methods for variance involve use of the sample mean. We are proposing a robust variance estimation method for skewed sample mean. Fig. 3 shows the stages of our robust aggregation framework and their connections. We provide an initial estimate of two noise parameters for sensor nodes, bias and variance in the first stage.

The bias estimate is subtracted from sensors readings and in the second phase of the framework, an initial estimate of the reputation vector calculated using the MLE. In the third stage the initial reputation vector provided in the second stage is used to estimate the trustworthiness of each sensor based on the distance of sensor readings to such initial reputation vector.

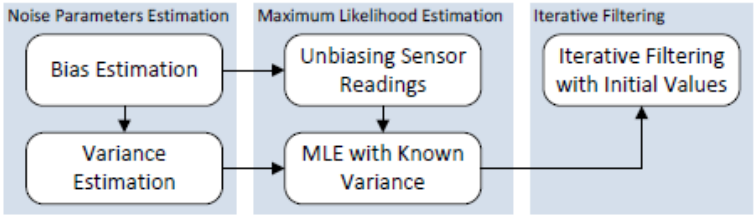

Fig. 3 Our Robust Data Aggregation Framework

It is clear that if the mean of the bias of all sensors is not zero, then there would be no way to account for it on the basis of sensor readings. On the other hand, bias of sensors, under normal circumstances, comes from imperfections in manufacture and calibration of sensors as well as from the fact that they might be deployed in places with different environmental circumstances where the sensed scalar might in fact have a slightly different value. Since by the very nature we are interested in obtaining a most reliable estimate of an average value of the variable sensed, it is reasonable to assume that the mean bias of all sensors is zero (without faults or malicious attack).

IV. CONCLUSION

We have introduced a sophisticated collusion attack scenario against a number of existing IF algorithms. Moreover, we have proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms robust against sophisticated collusion attacks. We plan to implement our approach 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. 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.
3. 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. Troubador publishing Ltd, 2009, pp. 105–128.
4. H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A game-theoretic approach for high-assurance of data trustworthiness in sensor networks," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on, April 2012, pp. 1192 –1203.
5. R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in SDM'12, 2012, pp. 612–623.
6. H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," arXiv e-prints, Aug. 2012.
7. 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.
8. L.-A. Tang, X. Yu, s. Kim, J. Han, C.-C. Hung, and W.-C. Peng, "Tru-Alarm: Trustworthiness analysis of sensor networks in cyber-physical systems," in proceedings of the 2010 IEEE International Conference on Data mining, Ser. ICDM '10, 2010, pp.1079–1084.
9. J.-W. Ho, M. Wright, and S. Das, "Zone Trust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing," Dependable and Secure Computing, IEEE Transactions on, vol. 9, no. 4, pp. 494–511, july-aug. 2012.

AUTHOR(S) PROFILE

Nikita P. Pareek, completed her graduation from SNJB's College of Engineering Nasik, Maharashtra. Presently she is perusing her post-graduation from LGN Sapkal College of Engineering Nasik, Maharashtra, India. Her research of interest include computer networks, network security, wireless sensor network.

Prof. N. R. Wankhade, completed his post-graduation from Bharti Vidyapith, Pune Maharashtra. Presently he is working at LGN Sapkal college of engineering, Nasik, Maharashtra, India as a professor and head of computer engineering department .He has presented papers at National and International conferences and also published paper in national and international journals on various aspects of the computer engineering and WSNs. His research of interest include computer networks, network security, wireless sensor network.

