Design and Analysis of Secure Data Aggregation Technique using IF algorithm

Pravallika Maddi[1], M.Omprakash[2]
[1]*M.Tech, Computer Science &Engineering*
[2]*Associate Professor & HOD, Department of CSE*
JJ Institute of Information Technology

Abstract- **As now we have limited power resources and computational power, data aggregation from multiple sensor nodesis done using easy methods similar to averaging. WSN's are more commonly unattended, they are particularly vulnerable to nodecompromising attacks. Consequently making it critical to ascertain trustworthiness of data and repute of sensor nodes iscritical for WSN. The aggregation of data from multiple sensor nodes is done at the aggregating node, by way of simple process comparable to averaging. Nevertheless such aggregation is known to be totally susceptible to node compromising assaults. Traditionally, WSNs are totally inclined to such attacks because of absences of tamper resistant hardware. Iterative Filtering process concurrently combination data from a couple of sources, typically in a form of corresponding weight reasons. Iterative Filtering is introduced which are extra effective towards collusion attacks than the easy averaging approaches.**

Index Terms- Collusion Attacks,data aggregation, Iterative Filtering Algorithm, wireless sensor network.

I. INTRODUCTION

Wireless sensor networks are usually composed of hundreds or thousands of inexpensive, low-powered sensingdevices with limited memory, computational, and communication resources [1,2]. These networks offer potentiallylow-cost solutions to an array of problems in both militaryand civilian applications, including battlefield surveillance,target tracking, environmental and health care monitoring,wildfire detection, and traffic regulation. Due to the lowdeployment cost requirement of wireless sensor networks,sensor nodes have simple hardware and severe resourceconstraints [6]. Hence, it is a challenging task to provideefficient solutions to data gathering problem. Among theseconstraints, ''battery power" is the most limiting factor indesigning wireless sensor network protocols. Therefore,in order to reduce the power consumption of wireless sensor networks, several mechanisms are proposed such asradio scheduling, control packet elimination, topology control, and most importantly data aggregation [2,3]. Dataaggregation protocols aim to combine and summarize datapackets of several sensor nodes so that amount of datatransmission is reduced. An example data aggregationscheme is presented in Fig. 1 where a group of sensornodes collect information from a target region. When thebase station queries the network, instead of sending eachsensor node's data to base station, one of the sensor nodes,called data aggregator, collects the information from itsneighboring nodes, aggregates them (e.g., computes theaverage), and sends the aggregated data to the base stations over a multihop path. As illustrated by the example, dataaggregation reduces the number of data transmissionsthereby improving the bandwidth and energy utilizationin the network.

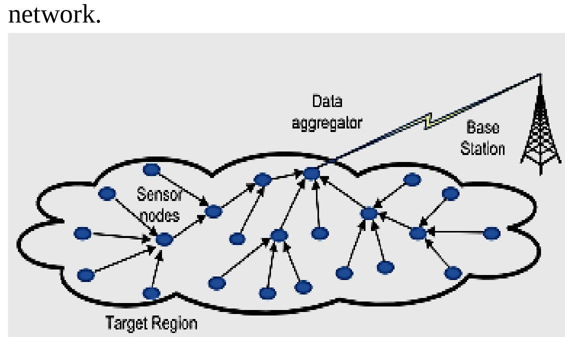

Fig. 1. Data aggregation in a wireless sensor network

In wireless sensor networks, the benefit of data aggregation increases if the intermediate sensor nodes performdata aggregation incrementally when data are being forwarded to the base station. However, while this continuous data aggregation operation improves the bandwidthand energy utilization, it may negatively affect other performance metrics such as delay, accuracy, fault-tolerance,and security [3]. As the majority of wireless sensor network applications require a certain level of security, it isnot possible to sacrifice security for data aggregation. Inaddition, there is a strong conflict between security anddata aggregation protocols. Security protocols require sensor nodes to encrypt and authenticate any sensed dataprior to its transmission and prefer data to be decryptedby the base station. On the other hand, data aggregation protocols prefer plain data to implement dataaggregation at every intermediate node so that energy efficiency is maximized. Moreover, data aggregation results inalterations in sensor data and therefore it is a challengingtask to provide source and data authentication along withdata aggregation. Due to these conflicting goals, dataaggregation and security protocols must be designed together so that data aggregation can be performed withoutsacrificing security.

The necessity of implementing data aggregation andsecurity together have led many researchers to work on secure data aggregation problem. In this paper, we aim toprovide an extensive overview of secure data aggregationconcept in wireless sensor networks by defining the mainissues and covering the most important work in the area.Compared to general data aggregation problem which isa well researched topic in wireless sensor networks, securedata aggregation problem still has the potential to providemany interesting research opportunities. Hence, we alsoaim to give a starting point for researchers who are interested in secure data aggregation problem by presentingthe open research areas and future research directions inthe field

II. METHODOLOGY

A. Network model

The conceptual model proposed by Wagner in [4] isconsidered for sensor network topology. Fig. 2 showsassumption for network model in WSN. The sensor nodesare divided into seperate clusters, and each cluster has acluster head which acts as an aggregator. Data areperiodically collected and aggregated by the aggregator.Authors in [5] assume that the aggregator itself is notcompromised and concentrate on algo-rithms which makeaggregation secure when the individual sensor nodesmight be compromised and might be sending false data tothe aggregator. It also assume that each data aggregatorhas enough computational power to run an suitablealgorithm for data aggregation.

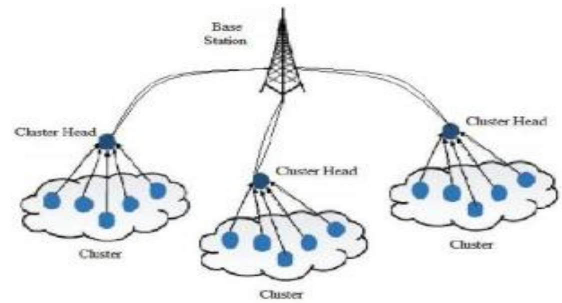

Fig .2.Network model of wirelss sensor network.

B. Adversary model

The past researchers [1][6] developes the attack models byconsidering the fact that they cannot rely on cryptographicmethods forpreventing the attacks, since the adversarymay extract cryptographic keys from the compromisednodes. The authors in, considers Byzantine attack model,where the ad-versary can compromise a set of sensornodes and insert any false data through the compromisednodes [7]. Following are some assumptions made in thismodel

a. Sensors are deployed in a hostile unattendedenvironment with some physically compromisednodes.

b. When a sensor node is compromised, all theinformation which is inside the node becomesaccessible by the adversary. System cannot depend oncryptographic methods for preventing the attacksbecause the adversary may extract cryptographic keysfrom the compromised nodes [8].

c. Through the compromised sensor nodes the adversarycan send false data to the aggregator with a purpose ofchanging the aggregate values.

d. All compromised nodes can be under control of asingle adversary or a colluding group of adversaries,enabling them to launch a sophisticated attack.

e. The adversary has enough knowledge about theaggregation algorithm and its parameters. The basestation and aggregator nodes cannot be compromisedby adversary node.

C. Collusion attack scenario

In this scenario ten sensors are assuming that report thevalues of temperature, which are aggregated using asuitable aggregation algorithm Most of the algorithmsemploy simple assumptions about the initial values ofweights for sensors [9]. In the suitable adversary model, anattacker is able to mislead the aggregation system throughcareful selection of reported data values. The collusionattack scenarios are as follows.

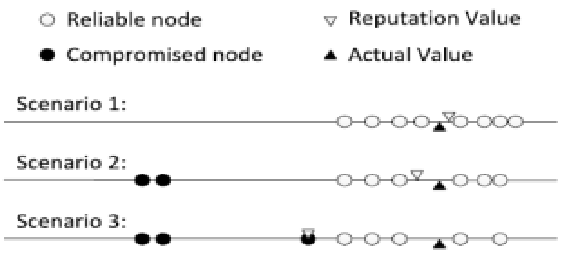

Fig.3.Collusion attack scenario.

Most of the IF algorithms occupy simple assumptionsabout the initial values of weights for sensors. In case ofour opponent model, an attacker is able to misinform theaggregation system from side to side cautious range ofreport data standards. Assume that ten sensors report thevalues of temperature, which are aggregated using the IFalgorithm planned in with the reciprocal discriminatedfunction.

In scenario 1, all sensors are reliable and the result of theIF algorithm is close to the actual value.

In scenario 2, an adversary compromises two sensornodes, and alters the readings of these values such that thesimple average of all sensor readings is skewed towards alower value. As these two sensor nodes report a lowervalue, IF algorithm penalizes them and assigns to themlower weights, because their values are far from the valuesof the sensors. The algorithm assigns very low weights tothese two sensor nodes and consequently theircontributions decrease.

In scenario 3, an adversary employs three compromisednodes in order to launch a collusion attack. It listens to thereports of sensors in the network and instructs the twocompromised sensor nodes to report values far from thetrue value of the measured quantity.

III. SYSTEM ARCHITECTURE

The important intention of data aggregation algorithm is to acquire and aggregate data in an energy effective manner so thatnetwork existence time is more advantageous. Wi-fi Sensor community presents an increasingly, attractive method of data gathering indistributed procedure architectures and dynamic access through wi-fi connectivity. Iterative Filtering system supplies asolution for a fundamental predicament concerning with data aggregation in WSN.IF, simultaneously aggregate data from multiplesources and furnish believe evaluation of these sources, generally in a type of corresponding weight factors assigned toinformation offered by means of every source. With the aid of demonstration it is proved that iterative filtering methods are more strong towardscollusion attacks than the straightforward averaging ways, to a novel refined collusion attack. To handle this protectiondilemma, an improvement for iterative filtering techniques is finished via offering an initial approximation for such techniquewhich makes them not handiest collusion effective, but in addition more accurate and turbo converging.

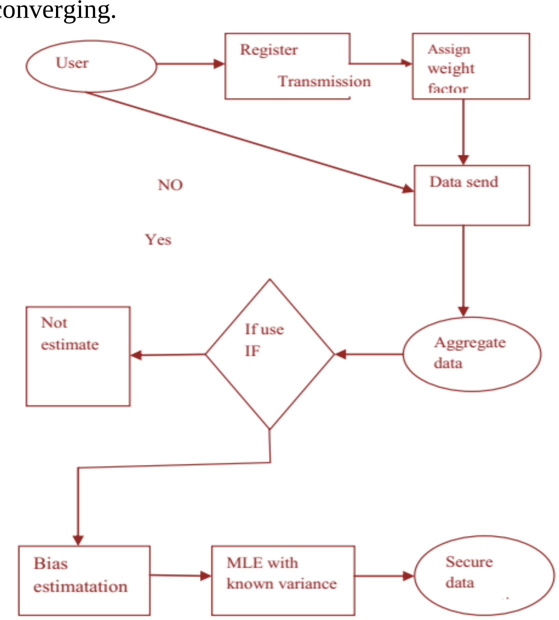

Fig 4 System Architecture

The architecture diagram for the proposed system is shown in Fig 4.. After registration in the network if the user isvalid they can enter into the existing network topology. The user must register their login credentials and to select theassigning weight factors depending on the number of data have to be used. By using IF, the sensor error is estimated ina wide range of sensor faults and not susceptible to the described attack. It utilizes an estimate of the noise parameters obtained from sensor nodes. The enhanced IF schemes able to protect against sophisticated collusion attacks byproviding an initial estimate of trustworthiness of sensor using input. The aggregated data is performing a filteringoperation. If any error occurs on the filtering process, first estimate the errors and calculate the new variance of datausing MLE and finally transmit the aggregated data in a secured way.

A. Node creation

In this module the weighted factor is assigned to each source in the network. The individual id specifies the nodelocation by allocating weight factor to each node. 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 thenumber of nodes connected into the network can also be identified.

B. Data aggregation in multiple sources

This module specifies the data aggregation from multiple sources. Data aggregation is any process in whichinformation is gathered and expressed in a summary form, for purposes such as statistical analysis. A commonaggregation purpose is to get more information about particular groups. The network is formed and the aggregate nodecollects many data from multiple nodes. It is also reduce the data traffic.

C. Find bias and unbiased readings using IF

To find bias and unbiased readings using Iterative Filtering method is specified. To propose a solution for suchvulnerability by providing an initial trust estimate, this is based on a robust estimation of errors of individual sensors.When nature of error is stochastic, such errors essentially represent an approximation of the error parameters of sensornodes in WSN such as bias and variance.

D. Secure data aggregation using IF

This module specifies the secure data aggregation using Iterative Filtering technique. It is a tool for maximumlikelihood inference on partially observed dynamical systems. Stochastic reputations to the unknown parameters areused to explore the parameter space. Compare the different iterative value to provide the rank for each iteration. Thehighest rank iteration occurs more error and then this error is avoided using IF technique.

IV. CONCLUSION

In wireless sensor network computational cost and energy need high level for transmitting the data. So that thedata aggregation technique is used in WSN. This technique is done by using various simple methods such as averagingbut this data aggregation is highly vulnerable. The Iterative Filtering algorithm in secure data aggregation is used toresolve a number of important problems, such as secure routing, fault tolerance, false data detection, compromisednode detection, secure data aggregation, cluster head election, outlier detection, etc.

REFERENCES

[1]. Mohsen Rezvani, AleksandarIgnjatovic, Elisa Bertino, and SanjayJha, “Secure Data Aggregation Technique for Wireless SensorNetworks in the Presence of Collusion Attacks” , IEEETransactions on Dependa-ble and Secure Computing (TDSC) ,2014

[2]. Y. Sun, H. Luo, and S. K. Das, “A trust-based framework for faulttolerant data aggregation in wireless multimedia sensor networks” ,IEEE Transaction on Dependable & Secure Computing ,Nov. 2012.

[3]. H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, “A gametheoretic approach for high-assurance of data trustworthiness insensor networks ” , IEEE International Conference on DataEngineering (ICDE), April 2012.

[4]. D. Wagner, “Resilient aggregation in sensor networks,” in Proc.2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 78–87.

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

[6]P.Laureti,L.Moret,Y-C.Zhang and Y-K.Yu(2006), “Information filtering via Iterative Refinement,”EPL (Europhysics Letters),vol75,pp.1006-1012.

[7]R-H.Li,J.X.Yu,X.Huang and H.Cheng(2012),”Robust reputation based ranking on bipartite ranking networks”, in SDM’12,pp.612-623.

[8]M. C. Vuran and I. F. Akyildiz, “Spatial correlation-based collaborative medium access control in wireless sensor networks,” IEEE/ACM Trans.Netw., vol. 14, no. 2, pp. 316–329, Apr. 2006.
[9]S.Ganeriwal, L.K. Balzano ,andM.B.Srivastava, “Reputationbasedframework for high integrity sensor networks,” ACM Trans. Sen. Netw., vol. 4,no. 3, pp. 15:1–15:37, Jun. 2008.
[10]M. Li, D. Ganesan, and P. Shenoy, “PRESTO: feedback-driven data management in sensor networks,” in Proceedings of the 3rd conference onNetworked Systems Design & Implementation - Volume 3, ser. NSDI’06, 2006, pp. 23–23.

BIODATA

PRAVALLIKA MADDI pursing M.Tech in Computer Science Engineering from **JJ INSTITUTE OF INFORMATION TECHNOLOGY**

M.OMPRAKASH working as Associate Professor & HOD, Department of CSE in **JJ INSTITUTE OF INFORMATION TECHNOLOGY**