ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 1, February 2015

National Conference on Computing and Communication (NC^3 2K15)

Organized by

Dept. of CSE, CARE Group of Institutions, Tiruchirapalli-620009, India on 27th February 2015

A Collusion Robust Iterative Filtering Technique For Data Aggregation In WSN

V.Prabaharan, D. Saravanan,

Student, Dept. of CSE, Pavendar Bharathidasan College of Engineering & Technology, Trichy , Tamilnadu, India[1]

HOD, Dept. of CSE, Pavendar Bharathidasan College of Engineering & Technology, Trichy, Tamilnadu, India[2]

ABSTRACT: In WSN the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing. When the cost of such technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms. The aggregation of data from multiple sensor nodes is done at the aggregating node, by simple method such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks.Generally, WSNs are highly susceptible to such attacks due to absences of tamper resistant hardware. Iterative Filtering technique simultaneously aggregate data from multiple sources, usually in a form of corresponding weight factors. Iterative Filtering is introduced which are more robust against collusion attacks than the simple averaging methods. IF, not only collusion robust but also more accurate and faster converging.

KEYWORDS: WSN, COLLUSION ATTACKS, DATA AGGREGATION.

I. INTRODUCTION

Sensor networks are collection of sensor nodes which cooperatively send sensed data to base station. As sensor nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration [1].The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. In WSN, sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size [2] and [3].Data aggregation is a process of aggregating the sensor data using aggregation approaches. The algorithm uses the sensor data from the sensor node and then aggregates the data by using some aggregation algorithms such as centralized approach, LEACH (Low Energy Adaptive Clustering Hierarchy), TAG (Tiny Aggregation) etc.This aggregated data is transferred to sink node by selecting the efficient path. In many sensor applications the data collected from individual nodes are aggregated at a base station or host computer.

To reduce energy consumption, many systems also perform in-network aggregation of sensor data at intermediate nodes enroutes to the base station. Most existing aggregation algorithms and systems do not include any provisions for security and consequently these systems are vulnerable to a wide variety of attacks. In particular, compromised nodes can be used to inject false data that leads to incorrect aggregates being computed at base station. Two main security challenges in secure data aggregation are confidentiality and integrity. While traditionally encryption is used to provide end to end confidentiality in WSN, the aggregators in secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data.Thus, while data aggregation improves energy efficiency of a network; it complicates the existing security challenges.

In future, WSNs need more sophisticated algorithms for data aggregation. Such algorithm should have two features as a major task. 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 a zero mean, then the estimate produced by any technique used, should have a variance close to 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 technique the variance of the sensors unavailable in practice. The technique must be robust in the presence of non-stochastic errors, such as faults and malicious attacks and besides aggregating data; also provide an assessment of the reliability and trustworthiness of the data received from the sensor nodes. Identification of a new sophisticated collusion attacks against IF based reputation system which reveals a severe vulnerability of techniques. The novel method for estimation of sensor errors which is effective in a wide range of sensor faults and not susceptible to the described attack. Design of an efficient and robust aggregation method inspired by the MLE, which utilizes an estimate of the noise parameters obtained. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs.

The performance of IF is validated by simulation on synthetically generated data sets. The simulation results illustrate that the robust aggregation technique is effective in terms of robustness against the novel sophisticated attack scenario as well as efficient in terms of the computational cost. The sensor errors are estimated based on biased and unbiased readings in specified location. IF provides both higher accuracy and better collusion resistance than the other methods.

II. EXISTING SYSTEM

Due to limited computational power and energy resource, aggregation of data from multiple sensor nodes is done at the aggregating node is usually accomplished by simple methods such as averaging. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes. It however complicates the already existing security challenges for wireless sensor networks and requires new security techniques tailored specifically for various purposes. Providing security to aggregate data in WSN is 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.

A. Disadvantages

1. Simple data aggregation is highly vulnerable to node compromising attacks and produces invalid data.
2. Lack in accuracy and faster while aggregating data.
3. Degrade of performance in the presence of non-stochastic errors, such as faults and malicious attacks.
4. By simple data aggregation it is susceptible to exploiting false data injection through a number of compromised nodes.

III. PROPOSED SYSTEM

The main goal of data aggregation algorithm is to gather and aggregate data in an energy efficient manner so that network life time is enhanced. Wireless Sensor Network offers an increasingly, attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Iterative Filtering technique provides a solution for a major problem regarding with data aggregation in WSN.IF, 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. By demonstration it is proved that iterative filtering techniques are more robust against collusion attacks than the simple averaging methods, to a novel sophisticated collusion attack. To address this security issue, an improvement for iterative filtering techniques is done by providing an initial approximation for such technique which makes them not only collusion robust, but also more accurate and faster converging.

A. Advantages

1. IF based reputation system which reveals a severe protection against any non- stochastic errors, such as faults and malicious attacks.
2. IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors.

3. IF improves accuracy and faster while aggregating data.
4. IF raises performance in the presence of non-stochastic errors, such as faults and malicious attacks.

II. SYSTEM ARCHITECTURE

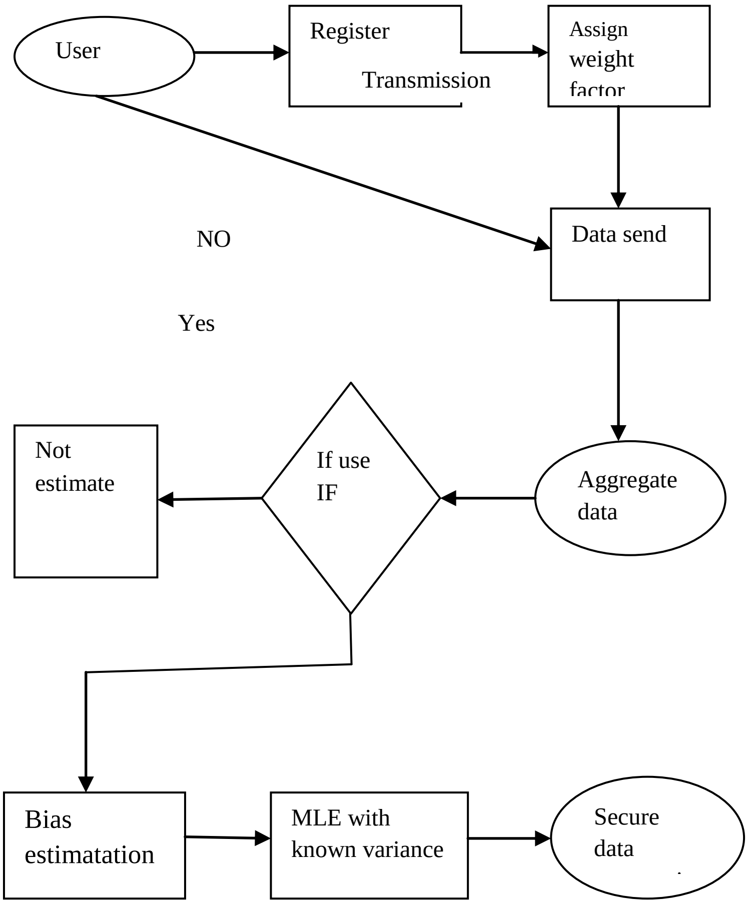

Fig 4.1 System Architecture

A. System Description

The architecture diagram for the proposed system is shown in Fig 4.1. After registration in the network if the user is valid they can enter into the existing network topology. The user must register their login credentials and to select the assigning weight factors depending on the number of data have to be used. By using IF, the sensor error is estimated in a 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 by providing an initial estimate of trustworthiness of sensor using input. The aggregated data is performing a filtering operation. If any error occurs on the filtering process, first estimate the errors and calculate the new variance of data using MLE and finally transmit the aggregated data in a secured way.

IV. MODULES DESCRIPTION

The four modules for secure data aggregation using IF are:

A. Node creation with weight factors assigned to source.

B. Data aggregation in multiple sources.
C. Find bias and unbiased readings using IF.
D. Secure data aggregation using IF.

A. Node creation

In this module the weighted factor is assigned to each source in the network. The individual id specifies the node location 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 the number 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 which information is gathered and expressed in a summary form, for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups. The network is formed and the aggregate node collects 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 such vulnerability 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 sensor nodes 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 maximum likelihood inference on partially observed dynamical systems. Stochastic reputations to the unknown parameters are used to explore the parameter space. Compare the different iterative value to provide the rank for each iteration. The highest rank iteration occurs more error and then this error is avoided using IF technique.

V. RESULTS

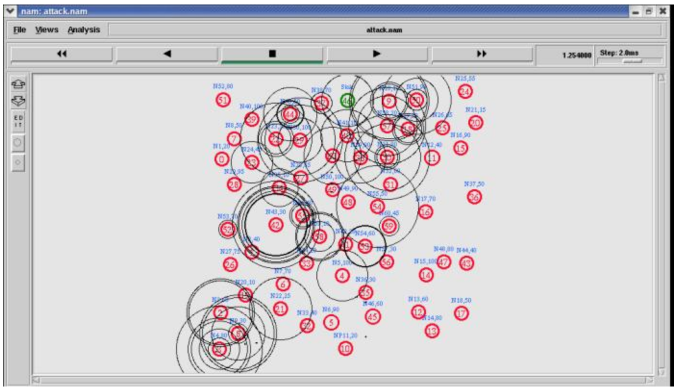

Fig 4.1 Packet Drop in Existing System

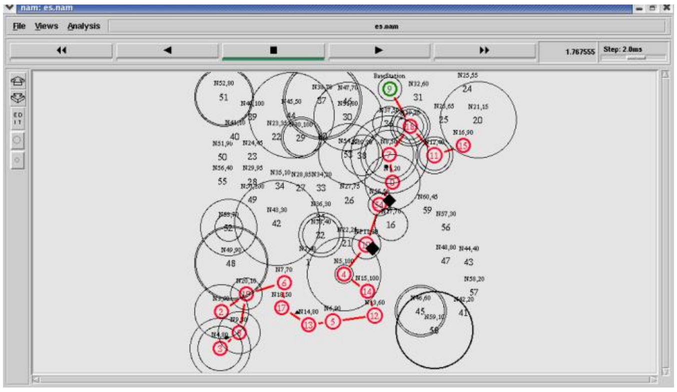

Fig 4.2 Data Aggregation

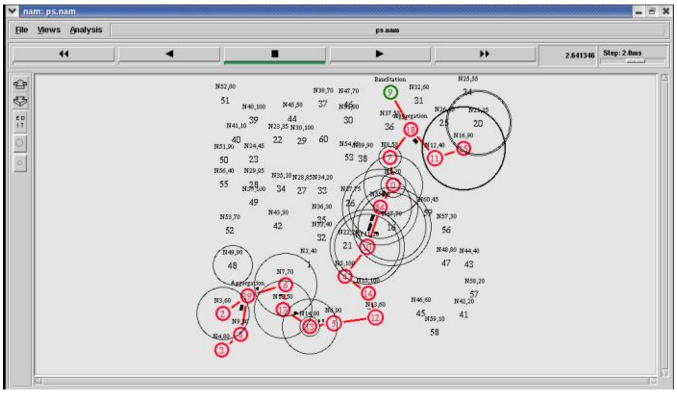

Fig 4.3 Secure data aggregation method

A graph is plotted between time and packet size to study the packet delivery ration in the proposed system and is shown in Fig 6.4. The result interpretation shows that the delivered packet size increases linearly with respect to time and hence the packet delivery ratio is increased.

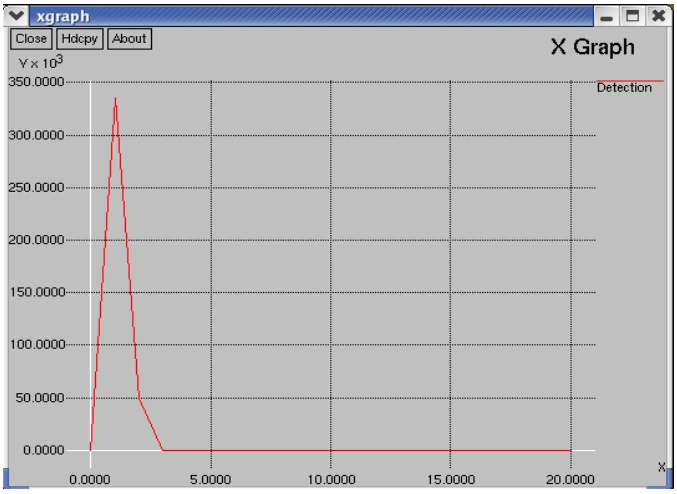

Fig 4.4 Graph Variations using IF.

A graph is plotted between time and packet size to study the delay in the proposed system and is shown in Fig 6.5. The result shows secure data aggregation method using. When the time is between 0.000 ms to 2.000 ms and there is a fall in packet size till 4.000 mb and again there is a raise in packet size and reaches its peak position of 35.000 mb at time 6.000 ms the delay in packet size starts decreasing gradually.

VI. CONCLUSION

In wireless sensor network computational cost and energy need high level for transmitting the data. So that the data aggregation technique is used in WSN. This technique is done by using various simple methods such as averaging but this data aggregation is highly vulnerable. The Iterative Filtering algorithm in secure data aggregation is used to resolve a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection, secure data aggregation, cluster head election, outlier detection, etc. This algorithm not only for collusion robust but also more accurate and faster converging.

REFERENCES

[1]S.Ozedemir and Y.Xiao,(Aug.2009)”Secure data aggregation in wireless sensor networks:A comprehensive overview,”Comput.Netw., vol.53,no.12,pp.2022-2037.
[2]L.Wasserman,All of statistics:a concise course in statistical inference.New York:Springer.
[3]K.Hoffman,D.Zage and C.Nita-Rotaru(Dec.2009), “A survey of attack and defence techniques for reputation systems,”ACM Comput.Surv,vol.42,no.1,pp.1:1-1:31.
[4]H-S.Lim,Y-S.Moon and E.Bertino(2010) ”Provenance-based trustworthiness assessment in sensor networks,” in proceedings of seventh International Workshop on Data Management for sensor Networks,ser.DMSN,pp.2-7
[5]Y.Zhou,T.Lei and T.Zhou(2010) ”A robust ranking algorithm to spamming”,CoRR,vol.abs/1012.3793.
[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 ,and M.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 on Networked Systems Design & Implementation - Volume 3, ser. NSDI’06, 2006, pp. 23–23.