A Secure and Robust Wireless Sensor Networking for Ensuring Secure Data Aggregation to Face Collusion Attacks

1 P.V. Vidyullatha 2 Mrs. Bakiya Lakshmi 3 Mr. Pradosh Chandra Patnaik

1 M.Tech Student, Information Technology, Aurora’s Scientific Technological & Research Academy, Bandlaguda, Hyderabad, Telangana State, India.

2 Senior Assistant Professor, Aurora’s Scientific Technological & Research Academy, Bandlaguda, Hyderabad, Telangana State, India

3 Head of Dept. and Professor, Aurora’s Scientific Technological & Research Academy, Bandlaguda, Hyderabad, Telangana State, India

ABSTRACT: Security a network includes the authorization of accessibility to data in a network that is managed by the particular network administrator. Wireless sensor network (WSN) refers to a collection of spatially dispersed and committed sensors for tracking and recording the bodily situations of the environment and organizing the accumulated statistics at a centralized location. Collision assault refers to the organization of nodes to access the unlawful data. The data accumulated from individual nodes is aggregated at a base station or host node. Because of restricted computational energy and power resources, aggregation of information from more than one sensor nodes done on the aggregating node is typically executed by way of easy methods together with averaging. But such aggregation is known to be incredibly liable to node compromising attacks. Iterative filtering algorithms maintain outstanding promise for this sort of characteristic. Such algorithms concurrently aggregate information from a couple of assets and provide believe assessment of these sources often in a form of corresponding weight factors assigned to information supplied via each source. Data aggregation procedure can enhance the robustness and accuracy of statistics which is received by using whole network. In this paper we illustrate that numerous current iterative filtering algorithms, at the same time as considerably more robust in opposition to collusion attacks as the simple averaging strategies, are however susceptible to a novel sophisticated collusion attack we introduce. To deal with this safety issue, we endorse an improvement for iterative filtering techniques by way of providing an preliminary approximation for such algorithms which makes them no longer best collusion strong, however also more accurate and faster converging.

I. INTRODUCTION

A wireless sensor network (WSN) includes a set of these nodes which have the ability to sense, process data and communicate with every other node through a wireless connection. Wireless sensor networks, the improvement in sensor era has made it viable to have very small, low powered sensing devices geared up with programmable compute, more than one parameter sensing and wireless message functionality. Additionally, the low price makes it viable to have a network of loads or thousands of these sensors, thereby improving the consistency and accuracy of statistics and the area coverage. wireless
sensor networks provide statistics about remote systems, extensive-unfold environmental changes, etc. wireless sensor network is a network system created from spatially allotted devices the usage of wireless sensor nodes to screen physical or environmental scenario, which include sound, temperature, and motion.

![Fig.1. Data Aggregation in WSN’s](image)

Trust and Reputation systems have a significant position in supporting operation of a extensive range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by supplying an assessment of trustworthiness of individuals in such allotted systems. A trustworthiness evaluation at any given moment represents an aggregate of the behavior of the individuals up to that moment and must be strong within the presence of diverse styles of faults and malicious behavior. There are a number of incentives for attackers to manipulate accept as true with and reputation rankings of contributors in a disbursed device, and such manipulation can severely impair the overall performance of one of these devices. The main target of malicious attackers are aggregation algorithms of believe and recognition systems. A sensor network is designed to carry out a set of high level records processing duties along with detection, tune, or categorization. Measures of performance for those tasks are well defined, inclusive of discovery of fake alarms or misses, category mistakes, and track exceptional. because the computational energy of very low strength processors dramatically will increase, normally driven by way of demands of mobile computing, and as the price of such era drops, WSNs might be able to come up with the money for hardware that can implement extra state-of-the-art information aggregation and believe evaluation algorithms; an instance is the current emergence of multi-core and multiprocessor structures in sensor nodes. Iterative Filtering (IF) algorithms are an attractive option for WSNs due to the fact they clear up both issues - data aggregation and records trustworthiness assessment - the use of a single iterative manner. Such trustworthiness estimate of every sensor is based on the gap of the readings of the sort of sensor from the estimate of the appropriate values, received within the preceding spherical of new release by means of some shape of aggregation of the readings of all sensors. Such aggregation is normally a weighted common; sensors whose readings appreciably vary from such estimate are assigned much less trustworthiness and therefore inside the aggregation system within the present spherical of new release their readings are given a lower weight.

II. RELATED WORK

Strong data aggregation is a critical difficulty in WSNs and there are some of papers investigating malicious data injection by way of taking into account the numerous adversary models. There are three bodies of labor associated with our studies: IF
algorithms, trust and reputation structures for WSNs, and secure data aggregation with compromised node detection in WSNs.

Reputation and Trust standards can be used to triumph over the compromised node detection and cozy records aggregation troubles in WSNs. Ho et al. previous works proposed a framework to detect compromised nodes in WSN after which practice a software attestation for the detected nodes. They reported that the revocation of detected compromised nodes can't be carried out due to a high danger of fake effective inside the proposed scheme. The main idea of false aggregator detection inside the scheme proposed is to hire some of monitoring nodes which might be jogging aggregation operations and presenting a MAC value of their aggregation effects as a part of MAC inside the cost computed by using the cluster aggregator. High computation and transmission value required for MAC-primarily based integrity checking on this scheme makes it improper for deployment in WSN. Lim et al. proposed a sport-theoretical defense method to defend sensor nodes and to assure a high level of trustworthiness for sensed facts. Moreover, there may be a large extent of posted research within the location of at ease tiny aggregation in WSNs. These studies awareness on detecting false aggregation operations through an adversary, that is, on statistics aggregator nodes obtaining facts from supply nodes and generating wrong aggregated values. Consequently, they deal with neither the problem of false statistics being provided through the statistics resources nor the hassle of collusion. However, when an adversary injects fake data by means of a collusion attack scenario, it can affects the outcomes of the honest aggregators and hence the bottom station will get hold of skewed combination value. In this example, the compromised nodes will attest their fake records and consequently the base station assumes that all reviews are from sincere sensor nodes. Although the aforementioned research keep in mind false data injection for some of simple attack situations, to the first-class of our knowledge, no existing paintings addresses this trouble within the case of a collusion attack with the aid of compromised nodes in a way which employs high degree knowledge approximately information aggregation algorithm used.

III. FRAMEWORK
A. Network Model

A WSN includes small-sized sensor devices, which are equipped with restricted battery power and are successful of wireless communications. When a WSN is deployed in a sensing subject, those sensor nodes may be responsible for sensing odd events or for amassing the sensed facts of the surroundings. In the case of a sensor node detecting an peculiar event or being set to periodically file the sensed statistics, it'll ship the message hop-by-hop to a unique node, called a sink node. The sink node will then inform the supervisor via the Internet.

The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically together and aggregated with the aid of the aggregator.

B. Collusion Attacks in WNS’s

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 reliable and the result of the IF algorithm is close to the actual value. In scenario 2, an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is skewed towards a lesser value. As these two sensor nodes report a lower value, IF algorithm penalizes them and assigns to them lower weights, 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, an adversary employs three compromised nodes so that it will release a collusion assault. It concentrates to the reviews of sensors in the community and instructs the compromised sensor nodes to record values a long way from the true fee of the measured amount. It then computes the skewed cost of the simple average of all sensor readings and commands the third compromised sensor to file such skewed average as its readings.

C. Framework Overview

In order to get better the overall performance of IF algorithms towards the aforementioned assault state of affairs, we offer a sturdy initial estimation of the trustworthiness of sensor nodes to be used in the first new release of the IF algorithm.

Most of the conventional statistical estimation techniques for variance involve use of the sample suggest. For this cause, proposing a sturdy variance estimation method in the case of skewed sample mean is an crucial part of our method.

![System Architecture](image)

**A Robust data Aggregation Framework:**

Robust data aggregation is done at the cluster head, like Identification of a new sophisticated collusion attack which reveals a severe susceptibility of IF algorithms.

A method for estimation of sensors’ errors which is effective in a range of sensor faults which solve collusion attack as; Using MLE, it design an efficient and robust aggregation method, which utilizes an estimate of the noise parameters; Improved IF able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs.
D. Enhanced Iterative Filtering

IF set of rules is powerful in opposition to the simple outlier injection with the aid of the compromised nodes. An adversary employs 3 compromised nodes with the intention to launch a collusion assault. It listens to the reports of sensors within the community and instructs the two compromised sensor nodes to document values away from the true fee of the measured quantity. It then computes the skewed price of the simple average of all sensor readings and commands three compromised sensor to record such skewed average as its readings. In other words, two compromised nodes distort the easy common of readings, whilst third compromised node reviews a cost very near such distorted average accordingly making such analyzing appear to the IF set of rules as a noticeably reliable reading. As a result, IF algorithms will meet to the values provide through third compromised node, because in the first generation of the algorithm third compromised node will achieve the best impact, notably dominate the weights of all different sensors. Initial check vector primarily based on the IF technique provide a sturdy nature of the safety device.

IV. EXPERIMENTAL RESULTS

The goal of our experiments is to evaluate the robustness and efficiency of our approach for estimating the genuine values of signal based totally on the sensor readings in the presence of faults and collusion assaults. For every test, we compare the accuracy based on Root Mean Squared blunders (RMS blunders) metric and performance primarily based at the number of iterations wanted for convergence of IF algorithms. The predominant shortcoming of the IF algorithms in the proposed attack scenario is they quickly converge to the sample mean within the presence of the assault situation. In order to investigate the lack, we performed an test by increasing the sensor variances as well as the variety of colluders. In this experiment, quantified the range of iterations for the IF algorithm with reciprocal discriminant feature.

V. CONCLUSION

Compromised node will provide fake aggregated information to the aggregator node so the overall data collected by way of the node have to be incorrect. This can be prevented by enforcing the iterative filtering algorithm added within the aggregator node for supplying a safety. trust and reputation had been currently suggested as an powerful security mechanism for wireless Sensor Networks Iterative Filtering (IF) algorithms are an appealing option for WSNs due to the fact they remedy both troubles data aggregation and information trustworthiness evaluation using a only iterative process with a purpose to improve the overall performance of IF algorithms towards the aforementioned assault situation, provide a strong preliminary estimation of the trustworthiness of sensor nodes for use in the first iteration of the IF set of rules. Proposed an development for the IF algorithms with the aid of offering an initial approximation of the trustworthiness of sensor nodes which makes the
algorithms not simplest collusion sturdy, however additionally greater precise and quicker converging.

The results are shown in figure below.

![Graph showing results](image)

**REFERENCES:**


Author Details:

P.V.Vidyullatha, pursuing M.Tech in Information Technology, from Aurora’s Scientific Technological & Research Academy, Affiliated to Jawaharlal Nehru Technological University Hyderabad and Approved by AICTE, located at Bandlaguda, Hyderabad, Telangana State, India.

Email: pvvidyullatha1991@gmail.com
Phone: 7382448733

Mrs. Bakiya Lakshmi, Senior Assistant Professor, Aurora’s Scientific Technological & Research Academy, Affiliated to Jawaharlal Nehru Technological University Hyderabad and Approved by AICTE, located at Bandlaguda, Hyderabad, Telangana State, India.

Email: ubakiya2@gmail.com

Mr. Pradosh Chandra Patnaik, Head of Department, Aurora’s Scientific Technological & Research Academy, Affiliated to Jawaharlal Nehru Technological University Hyderabad and Approved by AICTE, located at Bandlaguda, Hyderabad, Telangana State, India.