Prevention of Collusion Attacks in Wireless Sensor Networks Using Improved Iterative Filtering-Based System

Rufus Olalere Oladele
Dept. of Computer Science
University of Ilorin
Ilorin, Nigeria
rooladele@yahoo.com

Damilola Nnamaka Ajobiewe
Dept. of Computer Science
Federal College of Education (Special)
Oyo, Nigeria
ajobiewe.damilola2247@fcesoyo.edu.ng

Solomon Babatunde Olaleye
Dept. of Computer Science
Federal College of Education (Special)
Oyo, Nigeria
olaleye.solomon1115@fcesoyo.edu.ng

***Abstract*— Wi-Fi-enabled devices and other decentralized systems often share a huge amount of diverse data from a broad variety of sources. These networks, on the other hand, may be vulnerable to collusion attacks on some of their nodes. In literature, the concepts of trust and reputation are commonly used to combat the threat of a collusion assault. Iterative filtering is a notable algorithm that employs these concepts (IF). Despite the fact that IF is more resistant to collusion than other averaging techniques, complicated collusion attacks, such as those that require an opponent to have complete knowledge of the network and base station functioning, remain plausible. To combat sophisticated collusion assaults, IIF-based (iterative filtering-based) methods are necessary. The goal of this study was to create an iterative filtering-based system (IIF-B) capable of thwarting even the most sophisticated collusion attempts. Low-Energy Adaptive Clustering Hierarchy (LEACH) was employed by the study team to conserve energy. IIF-based system's discriminant function made use of recursive and Laureti discriminant functions. The data used in this study was created by filtering the sensor network's noise. The study's bias and variance-adjusted probability distribution replicated the errors that were made throughout the study. The suggested system's output was tested for accuracy using the Root Mean Square Error (RMSE) and Pearson Product Moment Correlation (PPMC). To determine how well the IIF-based system worked, its accuracy and iterations were compared to those of four other current algorithms. The researchers found that their IIF-based system was more resistant to collusion attacks than any of the other four IF algorithms examined.**

Keywords—collusion attack, wireless sensor network, improved iterative filtering-based system

I. INTRODUCTION

Networks of sensor nodes that monitor, record, and arrange the physical characteristics of the environment are known as Wireless Sensor Networks (WSNs). There are various novel applications that WSNs may be used for, according to Chou et al. (2012). A wide range of commercial, academic, and security applications also make use of them. Chou et al. (2012) identified WSNs as reaching a large amount of sensor nodes as well as a few mobile nodes. Hu et al. (2004), when it comes to wireless sensor networks (WSNs), there are two components: a base station and a collection of scattered sensors that communicate and interact via the detection of physical traits. The sensors are required for detecting, initial processing, and transmission. To facilitate decision-making, the BS receives, processes and delivers data to the end user (Puccinelli and Haenggi, 2005;Ye et al., 2005; Lindsey and Raghavendra, 2002).

Over the past two decades, several studies have focused on WSNs and their potential uses. Many challenges remain in WSN installation despite recent advances in the technology. Concerns around security, design, data collection, deployment, and network coverage are among the most important ones. Ahlawat (2013) argued that the need for more effective security mechanisms has increased considerably because of the continued growth of wireless sensor networks. Corroborating Ahlawat (2013), Wireless sensor networks (WSNs) have a limited power, processing, and communication capacity. First and foremost, Ajobiewe et al. (2014) emphasized that the security concerns of the sensor network should be addressed prior to any system design.

According to Bhuiyan and Wu, 2016, when it comes to security, WSNs are a far cry from traditional networks in that they are limited in resources and processing. To safeguard and secure messages in networked systems, security protocols have been used. Among the alternatives are hierarchical, data-centric, location-based, and QoS-based routing systems. Bhuiyan and Wu (2016) observed, aside from its identification of (El-Semary and Abdel-Azim, 2013), such protocols might be revealed by a clever collusion attack (a kind of assault wherein a node has a binding deal with an enemy or is penetrated by an adversary). Consequently, Jeong et al. (2013) observed that because current security methods are insufficient, new research areas and concepts to solve sensor network security have emerged. In addressing sensor network security, Akyildiz et al. (2002b), Akyildizet al. (2002a) proposed several network layer protocols to manage the natural limitations imposed on sensor nodes. This is to make use of sensor energy in order to extend the life of deployed wireless sensor networks (WSNs). WSNs are frequently made up of a large number of low sensor nodes with limited sensing, processing, and communication capabilities, according to Ozdemir and Xiao (2009). A smaller amount of data must be provided in order to maximize sensor longevity and bandwidth use, since sensor nodes have limited resources. Data aggregation has been driven to the forefront by the burden of data transmission. Sensor data aggregation,

as defined by Ozdemir and Yang (2009), is an effort to decrease data transfer by integrating and summarizing sensor data. Node compromise and data confidentiality and integrity are real dangers to sensor nodes in practical terms. Sensitive information is usually sent by WSNs in distant and dangerous locations; sensor nodes are vulnerable to security breaches, such as data confidentiality and integrity (Ozdemir and Yang, 2009).

A malicious attack on these aggregation approaches, in which the attacker has access to all observed data and may alter certain readings, is very vulnerable (Shah and Shukla, 2012). Averaging and iterative filtering are the most common methods for aggregating data from a sensor network. It's still possible for an attacker who knows all of the detected data and can manipulate some of them to take advantage of these aggregation approaches. A new technique for detecting and removing the effect of tampered data transferred across a network is provided in this study. The improved iterative filtering process may be used to successfully detect and delete the changed data, thereby ensuring the system's secrecy and security.

II. STATEMENT OF THE PROBLEM

In all modes of communication, ensuring the confidentiality, integrity, and availability of all communications in the midst of clever opponents is desired. The efficiency of information communication technologies seems threatened by the vulnerability of WSNs to different types of attacks (Kumar and Gambhir, 2014). Studies reported in (Sultana et al., 2013; Rezvani et al., 2014; Panah et al., 2015; Wang et al.,2016; Fang et al., 2019) agreed that systems unattended/ unprotected are often prone to security attacks. As a possible security technique for Wireless Sensor Networks, trust and reputation have recently been proposed. Because they handle both data trustworthiness and data aggregation difficulties, Iterative Filtering (IF) Algorithms have shown considerable promise in the assessment of the trustworthiness of acquired and reported data. It is possible for an adversary to have complete knowledge of the network and the functioning of the base station in order to exploit the IF approach, which is more resilient than other replacement methods or simple averaging techniques. As a result, the collusion attack issue was addressed using a variety of sophisticated filtering techniques.

III. SIGNIFICANCE OF THE STUDY

Batteries in WSNs are typically small and low-power. When it comes to creating and operating WSNs that are both cost and energy efficient, it is always a problem for designers and managers. Design and management of networks may greatly benefit from the usage of network design tools. As a consequence, if these technologies are used, the network's life expectancy will be greatly enhanced. Tools like these may benefit from this study. This study's technique, in particular, shows promise for combating sophisticated collusion assaults. Experimenting with the system built in this work might also provide data that can help guide the development of future technologies.

IV. REVIEW OF RELATED LITERATURE

Nodes in a Wireless Sensor Network (WSN) communicate with one another wirelessly and collect data about the surrounding environment in order to keep tabs on it. The sensor nodes can detect, act on, and regulate the data they collect. They are able to do this. In order for sensor nodes to communicate effectively, many different wireless techniques must be used (Akyildiz et al., 2002b). According to Ozdemir and Yang's (2008) citation of Yick et al. (2008), WSNs include hundreds or thousands of low-cost, low-power sensing devices. It is possible that these networks might be used in a wide range of military and civilian applications, including battlefield surveillance and environmental and health-care monitoring. Chou et al. (2012) states that wireless sensor networks are composed of tens or hundreds of thousands of tiny sensor nodes that function autonomously and, in many cases, do not have access to renewable energy resources, such as solar panels. In recent investigations in wireless sensor networks, new protocols specific to sensor networks have been developed. WSNs should be built with a wide range of considerations in mind, including coverage area, mobility, power consumption, and communication capability.

WSN applications, according to Yick et al. (2008), are divided into two categories: monitors and trackers. Monitoring applications include indoor/outdoor monitoring systems, health and medical surveillance, energy monitoring, inventories geolocation, industry and process automation, and seismographic and structure monitoring. Tracking software may be used to track objects, animals, people, and cars.

V. DATA AGGREGATION

The cognitive process of gathering and combining relevant data is known asdata aggregation (DA) (Dagar and Mahajan, 2013). Similarly, according to Dhand and Tyagi (2016), data aggregation is primarily used to eliminate duplication, reduce the number of transfers, and, most significantly, save energy. It is one of several methods that may assist decrease WSN energy usage and extend the network’s lifespan. However, DA faces many obstacles, one of which is security. Sensor nodes are network components in wireless sensor networks, and as such, cluster heads or data aggregators must be formed among the nodes to send the data gathered to the Base Transmission Station (BTS) for processing. The Cluster Head (the node with the greatest residual energy as their cluster head/aggregator) is chosen by the sensor nodes. The aggregator in turns treats the data collected from multiple nodes as a cluster of data that have come or been brought together with the same attributes, therefore, reducing issues of data traffic and saves energy.

As examined by Dagar and Mahajan (2013), there are four strategies for aggregation of data, namely:

i. **Centralized Approach:** this method entails sending data to a central node through the shortest feasible route path from each of the sensor nodes. The sensor node transmits

the packet data to the aggregator, which then combines the data from all of the nodes into a single packet. (Dagar and Mahajan, 2013).

ii. **Tree-based:** firstly, a Data Aggregating Tree (DAT) is formed. Then each data transmission minimum spanning tree is created. Each node having a parent node to forward its data.

iii. **Cluster-based:**the network is split into many clusters, each of which has a number of nodes. The cluster head conducts the aggregation and afterwards sends the result to the rest of the cluster. (Rezvani et al., 2014; Dhand and Tyagi,2016).

iv. **In-network Approach**: within wireless sensor networks, data aggregation is accomplished using a variety of protocols. When assessing the performance of a data aggregation technique, the structural design of sensor networks is crucial.

VI. COLLUSION ATTACK

Collusion Attack (CA) aims to discover two hash function input strings that yield the same hash result. Because hash functions in the literature have an unlimited input length and a specified output length, there is always the potential of two distinct inputs producing the same hash result. As a result, collusion refers to a scenario in which two distinct inputs yield the same hash output. It's a kind of security attack or threat in which a node intentionally or unintentionally forms a secret agreement with an enemy. According to Bhuiyan and Wu (2016), the adversary may obtain important information from the system and then conduct complicated assaults on the system via bogus data injection through one or more compromised nodes. Of course, the chances of collusion are low, particularly for functions with high output quantities.

Many security processes and techniques are predicated on the premise that individual nodes or network leaders are trustworthy and take reasonable precautions to keep their networks safe (authentication, verification, and so on.) the implementation of these protocols in communication systems (Bhuiyan and Wu, 2016). These techniques, however, may be revealed as a result of a clever collusion attempt, according to the authors. Collusion attack, as defined by Bhuiyan and Wu (2016), occurs when a node intentionally makes a secret agreement with an opponent, or is compromised by an attacker with extensive knowledge of transmission and aggregation algorithms. In the case of a collusion attack, the colluding node's behavior changes slightly, allowing the adversary to read or inject information (Bhuiyan and Wu, 2016).

Bhuiyan and Wu (2016) showed that certain adversary models were created with the understanding that cryptographic techniques alone would not be sufficient to thwart assaults. The authors looked at a Byzantine attack scenario in which an opponent might enter a group of sensor nodes and inject any bogus data via the compromised nodes, knowing that the attacker could also get cryptographic keys from the compromised nodes. Keeping two essential assumptions in mind:

i. When one of these sensor nodes is hacked, the attacker gains access to all of the data stored on them. Because an opponent can gain cryptographic keys from compromised nodes, a system cannot rely only on cryptographic procedures to protect itself from attacks.

ii. The adversary can send false data through the compromised sensor nodes to the aggregator with a purpose of changing the aggregate values.

The traditional view of security cryptography - based alone is insufficient for the unique features and new misbehaviors seen in sensor networks. When an attacker injects fake data via a collusion attack scenario, it may distort the findings of the honest aggregators, resulting in a skewed aggregate value for the base station. Chan, Perrig, and Song (2006) investigated detecting fraudulent aggregation operations by an adversary on data aggregator nodes receiving data from source nodes. As a result, neither the issue of data sources providing misleading data nor the problem of collusion were addressed in the study. When an attacker injects fake data via a collusion attack scenario, it may distort the findings of the honest aggregators. Chan, Perrig, and Song (2006) investigated detecting fraudulent aggregation operations by an adversary on data aggregator nodes receiving data from source nodes and producing erroneous aggregated results. Also On data aggregator nodes receiving data from source nodes, Chan, Perrig, and Song (2006) examined identifying fraudulent aggregation actions by an adversary. The standard perspective of security cryptography - based alone, according to Ganeriwal, Balzano, and Srivastava (2008), is insufficient for the unique characteristics and unexpected misbehaviors encountered in sensor networks.

VII. METHODOLOGY

Since the data necessary will be acquired on a regular basis, the study's initial phase recommends using LEACH (Low-Energy Adaptive Clustering Hierarchy) for cluster creation. Sensor nodes are shown to have varying levels of dependability, as well as hacked nodes that have both real and reputational value. All three phases' subgroups are detailed in detail. For the purpose of creating a reputation vector, however, this research established a new enhanced IF system that uses the dKVD-reciprocal, dKVD-Affine, Zhou and Laureti discriminant function. For the purpose of trust assessment, the existing IF algorithms for collusion node compromised attacks were tested. A novel mechanism for combating fake information assaults was devised at the cluster level (node network) and at the base station level. Additional IF techniques were presented, including a novel approach for geolocation and malicious node detection.

A better framework for dealing with the problem in IF algorithms was created as a result of this. Sensor noise characteristics such as bias and non-biased are estimated statistically in a way that is impervious to assaults on the

sample mean of sensor data, which is the basis for the proposed expansion. Based on the Root Mean Squared Error (RMSE), Pearson Product Moment Correlation is used to evaluate the improved approach (PPMC). Sections two and three go into great depth on the metric. The ability to exclude large chunks of data while yet guaranteeing that critical matches are not missed is provided by a filter mechanism. The sole trade-off to consider when developing filtering algorithms is whether or not the increased labor is justified by the time and energy saved for verification.

A good discriminant function is always needed to secure data and trustworthiness of data at the sensors. This study proposes an improved IF-based system that applies the dKVD-reciprocal and Laureti function with the aim of defining the suitable and applicable discriminant function that would be needed to compute a reputation vector. Using this concept, the new discriminant function to be used is as follows:
when dkvD is known as

$$w^{t+1} = \left(\frac{1}{m}\|x - r^{t+1}\|_2^2\right)^{-1} \quad i.e\ (p = -1/1) \qquad 1.0$$

&Laureti

$$w^{t+1} = \left(\frac{1}{m}\|x - r^{t+1}\|_2^2\right)^{-0.5} \quad i.e\ (p = -1/2) \qquad 1.1$$

Therefore, an unknown discriminant function for nth value can be expressed as;

$$w^{t+1} = \left(\frac{1}{m}\|x - r^{t+1}\|_2^2\right)^{-\frac{1}{n}} \qquad 1.2$$

when n is set to be - p (n = - p) Then,

$$w^{t+1} = \left(\frac{1}{m}\|x - r^{t+1}\|_2^2\right)^{-\frac{1}{p}} \qquad 1.3$$

whhen -p = 1 we have 1.0
when – p =2 we have 1.1
Therefore, (1.3) can be rewritten as

$$w^{t+1} \cong \sqrt[p]{\frac{1}{m}(x_i + r^{t+1})^2}[(x]_i, r^t) \in R^2 for\ 0 \le p \le n$$

a. Root Mean Square Error (RMSE)

The metric Root Mean Square Error (RMSE) is determined by the following formula:

$$Rms \quad Error = \sqrt{\frac{\sum_{t=1}^{m}\left(r_t - \hat{r_t}\right)^2}{m}}$$

Because RMSE is scale-dependent, it is used in this research, to evaluate the predictederrors of various algorithms used for a single dataset rather than across datasets.

b. Pearson Product Moment Correlation (PPMC)

The reputation vector correlation coefficient is computed and analyzed using PPMC. The PPMC is however determined by the:

$$PPMC\ (r) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2(y_i - \bar{y})^2}}$$

Note that r is the correlation coefficient, $x_i$stands for the value of the x-variable, is the mean of the value of the x-variable, y_i is the value of the y-variable and is the mean of values of the y-variable. It is worth to note that the best quality in computing similarity between two collections of vectors is why PPMC was chosen.

c. Compromise Detection Performance of Nodes and Base Stations

A node and base station technique was developed that used a binary classification methodology to categorize sensor nodes as compromised or uncompromised. However, based on the findings obtained, the contributions of the detected affected nodes were eliminated and the results from the non-compromised nodes were utilized. The accuracy of IIF-B is highly dependent on the node and base station compromise detection performance. To demonstrate this, we analyzed the model's RMS Error in the presence of a sophisticated assault. The discriminant function is set to affine, and the maximum number of compromised nodes is set at eight. Because the node compromise detection module is a binary classification approach, its performance should be evaluated by analyzing its accuracy for each experimental case. A higher metric value implies a more capable detecting module. Furthermore, a substantial attack, such as a sophisticated collusion attempt, would be identified by a considerable decline in network performance.

VIII. SIMULATION RESULTS

Each experiment includes an evaluation of precision based on the Root Mean Squared Error (RMS error) measure. The RMS error measure measures the actual signal values from sensor data in the presence of failures and collusion assaults. The tests are designed to assess the resilience and effectiveness of this method. As an alternative to a straightforward assault, a novel complex collusion attack against many current IF algorithms was proposed. An attacker with sufficient knowledge of the aggregation process might skew the aggregation process by compromising a few sensor nodes in a WSN. For IF algorithms to be more robust and accurate, it is important to take into account the dependability of sensor nodes early in

the design process. For the first time, researchers have taken into account concessions in the base station, which have previously been ignored, when developing an IF-based system with a new method of merging and withdrawing based on initial assumptions about aggregated values and variance reading distributions for each sensor. There were several earlier iterative filtering approaches offered for reputation systems that he compared his upgraded IF-based system to. Using the same values as when they were provided, the researcher tested alternative algorithms with the same results.

The stages of the resilient aggregation architecture, their connections, and the probability with actual variance. As previously mentioned, the aggregation approach operates in a succession of phases using batches of subsequent sensor data. Following the processes of aggregator integration and development, aggregation, and transmission, an initial assessment of the two noise characteristics of the sensor nodes, bias and variance, was provided; statistical data for measuring bias and sensory variability are presented.

a. Estimation of Biased Sensor and Unbiased Sensor Error

If the mean bias of all sensors is not zero, there is no way to explain it based on sensor data. Sensory bias in typical circumstances results from a lack of sensitivity in the creation and balancing of the sensors, as well as the fact that they may be placed in locations with a diverse range of natural surroundings and places where scalar experience may have a slightly different meaning. Because the primary goal is to acquire the most accurate estimate of the average value of the variable observed, it is fair to infer that the mean bias of all sensors is minimal (without faults or malicious attacks).

b. Result Accuracy and Precision without Attack

As noted previously in previous sections, the researcher believed that a node successfully decodes a received packet if its possible data rate exceeds a desired datarate threshold r_t and if all packet sending parameters are satisfied. As a result, dealing with scenarios of unbiased and biased sensory mistakes is essential in order to achievert in a restricted probability measure.

i. Unbiased Sensor Error

Different distributions of variance were measured in a circle of sensors and received like results. However, to report a case by sensory error s when t is given by ∼N (0, s σ^2)taking into account the different values of the basic sensor variance σ2. Sensor bais stem from imperfections in manufacturing and calibration of sensor nodes as well as the reality that they may be installed in different environmental conditions. Figure 1, shows the improved approach achieves the minimal possible variance, it also shows that there is a linear relationship for each of the curves.

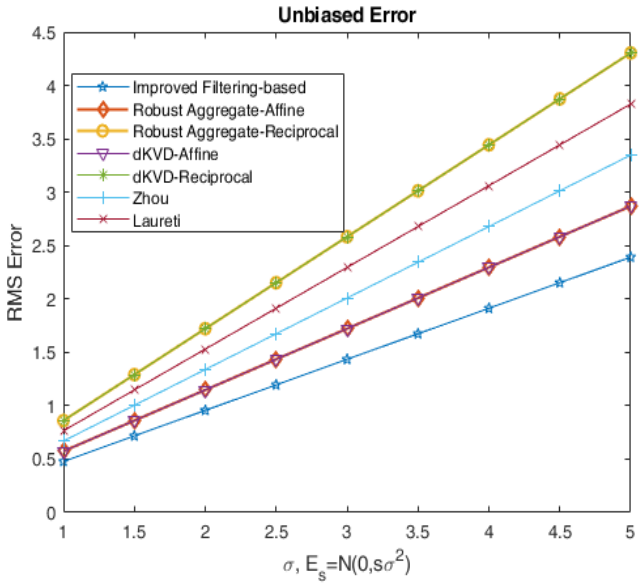

Figure 1:Unbiased sensor error

ii. Bias Sensor Readings

When unbiased sensor data is available, MLE is used to remove bias from biased sensor readings using the findings of the preceding measurement technique, which involves adding bias error into sensor readings formed by Gausian distribution using a variety of parameters. As a consequence, the inaccuracy of sensor's' at time't' is caused by ∼N (N(0, s σ^2)with the variance of the bias σ2b = 3 and heightening values for variances, where the variance of sensor s is equal to s×σ^2. The analysis in Figure 2 reveals the RMS for all algorithms of other IF algorithms, generates an error rate close to their errors in the unbiased scenario. It can be therefore concluded that the methods are stable against bias but fully stochastic noise.

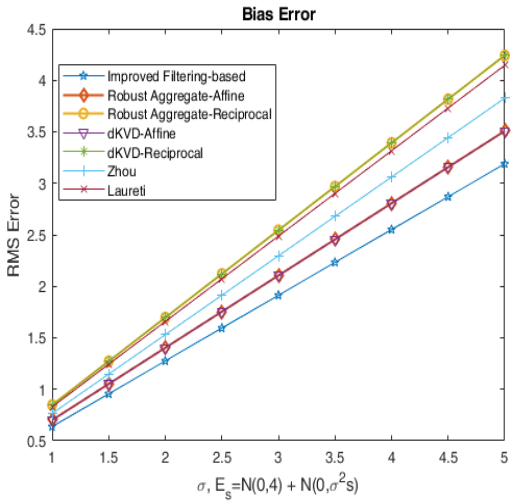

Figure 2:Bias sensor readings

iii. Correlated Noise

The information content of remote sensing is highly dependent on a variety of parameters, including spatial, stochastic, and non-stochastic noise. To evaluate the accuracy of data aggregation under varying degrees of noise, sensor noise measurements were generated using

various sigma values. A clear idea of the trend of correlated noise as we can see the least noise we got is in IIF-B method following the others like Robust Aggregate Affine, Robust Aggregate-Reciprocal, dKVD-Affine, dKVD Reciprocal, Zhou, Laureti. As the content of info in remote sensing depends largely on spatial, stochastic and non-stochastic noise, Figure 3, shows RMS error of the algorithms, indicating that our approach with the enhanced aggregate function improves dkvd-reciprocal algorithm for all values of variance.

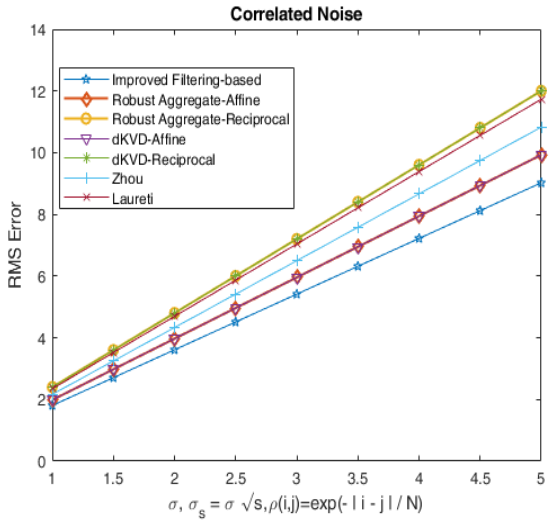

Figure 3: Correlated noise

iv. Result Accuracy and Precision with an Attack State

The adversary is supposed to utilize m (m< n) hacked sensor nodes to create the complex attacking conditions. To corrupt the simple average of all sensor data, the attacker creates deviation measurements from the first m - 1 compromised nodes. The variation in the algorithms utilized in the results suggests a strong correlation between the disparity between the algorithms and the attack. Thus far, this study has been able to accomplish some far-reaching goals by optimizing the lifespan of wireless sensor networks in order to make them more scalable, efficient, and balanced through the use of a secure data aggregation technique based on an improved iterative filtering-based system that eliminates data redundancy. The procedure is structured in three primary steps, beginning with clustering and aggregation formation and concluding with repeated filtering. However, if this technology is deployed in a network, network sensor nodes will survive longer and acquire more energy. Additionally, less data will be lost, maintaining the exceptional quality of information obtained.

IX. CONCLUSION

Although iterative filtering (IF) approaches integrate data aggregation with data trustworthiness assessment, they may be utilized for trust calculation. Although these algorithms are more resistant to collusion assaults and simple fake data injection attempts, they were not intended to account for more complex collusion tactics. Determine the durability of the IF algorithms in the event of failures and node breach collusion assaults is a critical problem that must be addressed. The challenges associated with employing IF algorithms for trust calculation in WSNs in the presence of faults and collusion attacks were the topic of this study, which contributed to the proposal of a better data aggregation scheme for such systems. The upgraded IF-based system outperforms the previous four IF algorithms in terms of reciprocal discriminant function accuracy. Additionally, it is immune to sophisticated collusion tactics. The findings of this experiment demonstrate that the original implementation of the IF approach converges to the skewed value given by one of the attackers after thirty rounds of iterations, beginning with an initial aggregate vector supplied by the new aggregate vector. Rather of depending on distorted data supplied by a few attackers, the approach iterates around 27 times and obtains a decent degree of accuracy.

X. RECOMMENDATIONS

The following recommendations are made:

i. The accurate portrayal of a network design scenario by network providers is crucial since it decreases energy consumption, expenses, and threats, while also extending the life of the network.

ii. Providers and designers of networks should implement the established system, as this will boost efficiency, as well as security, durability, and dependability.

REFERENCES

[1] M. Ahlawat,“Wireless sensor network-a theoretical review”, *International Journal of Wired and Wireless Communications*, vol. 1, no. 2, pp.1–19, 2013.

[2] D. N. Ajobiewe, W. K. Ofosu and O. A. Michael, O. A.“A wireless sensor network-based market parking scheme”, *International Journal of Computer Applications*, vol. 101, no.13, 2014.

[3] I. F. Akyildiz, W.Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, *IEEE Communications magazine*, vol. 40, no. 8, pp.102–114, 2002a

[4] I. F. Akyildiz, W.Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: A survey”, *Computer networks*, vol. 38, no. 4, pp.393–422, 2002b.

[5] Y. J. Al-Raisi, N. Alfadil and S. Aljahdali, “Increasing the reliability of the collected data in wireless sensor networks”, *In ISCA CAINE*, pp.290–297, 2011.

[6] H. Alzaid, E. Fooand N. J. M. Gonzalez, “Secure data aggregation in wireless sensor networks: A survey”, In Proceedings of the Sixth Australasian Information Security Conference (AISC 2008),*Australian Computer Society*,vol. 81, pp.93–105, 2008.

[7] M. Z. A. Bhuiyan and J. Wu,“ Collusion attack detection in networked systems”, In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/ DataCom/CyberSciTech), *IEEE*,pp.286–293, 2016.

[8] H. Chan, A. Perrig and D. Song, “Secure hierarchical in-network aggregation in sensor networks”, In Proceedings

of the 13th ACM conference on Computer and communications security, pp.278–287, 2006.

[9] C. T. Chou, A. Ignjatovic and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults", *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 8, pp.1525–1534, 2012.

[10] M. Dagar and S. Mahajan, "Data aggregation in wireless sensor network: A survey", *International Journal of Information and Computation Technology*, vol. 3, no. 3, pp.167– 174, 2013.

[11] G. Dhand and S. Tyagi, " Data aggregation techniques in wsn: Survey", *Procedia Computer Science*, vol. 92, no. :3, pp.78–384, 2016.

[12] A. M. El-Semary and M. M. Abdel-Azim, "New trends in secure routing protocols for wireless sensor networks" ,*International Journal of Distributed Sensor Networks*, vol. 9, no. 5, pp.25-26, 2013.

[13] W. Fang, W. Zhang, Q. Zhao, X. Ji, W. Chen and B. Assefa, "Comprehensive analysis of secure data aggregation scheme for industrial wireless sensor network",*CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 61, no. 2, pp.583–599, 2019.

[14] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks",*ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, pp.1–37, 2008.

[15] F. Hu, J. Ziobro, J. Tillett and N. K. Sharma, "Secure wireless sensor networks: Problems and solutions", *Rochester Institute of Technology, Rochester*, New York, USA, 2004.

[16] J. S. Jeong, M. Kim, K. H.Yoo, et al.,"A content oriented smart education system based on cloud computing",*International Journal of Multimedia and Ubiquitous Engineering*, vol. 8, no. 6, pp.313–328, 2013.

[17] S. Lindsey and C. S. Raghavendra, "Pegasis: Power-efficient gathering in sensor information systems. In Proceedings", *IEEE aerospace conference*, vol. 3, pp.3–3, 2002.

[18] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview", *Computer Networks*,vol. 53, no. 12, pp.2022–2037, 2009.

[19] A. S. Panah, R. van Schyndel, T. Sellis and E. Bertino, "In the shadows we trust: A secure aggregation tolerant watermark for data streams", In 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–9. IEEE, 2015.

[20] B. Przydatek, D. Song and A. Perrig, "Sia: Secure information aggregation in sensor networks", In Proceedings of the 1st international conference on Embedded networked sensor systems, pp.255–265, 2003.

[21] D. Puccinelliand M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing*", IEEE Circuits and systems magazine*, vol. 5, no. 3, pp.19–31, 2005

[22] M. Rezvani, A.Ignjatovic, E. Bertino and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks", *IEEE transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp.98–110, 2014.

[23] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan and N. Xiong, "Secure data aggregation in wireless sensor networks: A survey", In 2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), pp.315–320. IEEE, 2006.

[24] P. K. Shahand K. V. Shukla,"Secure data aggregation issues in wireless sensor network: A survey" ,*Journal of information and communication technologies*, vol. 2, no. 1, 2012.

[25] S. Sultana, G. Ghinita, E.Bertino and M. Shehab,"A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks",*IEEE transactions on dependable and secure computing*, vol.12, no. 3, pp.256–269, 2013.

[26] C. Wang, W. Zheng and E. Bertino," Provenance for wireless sensor networks: A survey", *Data Science and Engineering*, vol. 1, no. 3, pp.189–200, 2016.

[27] M. Ye, C. Li, G. Chen and J. Wu, "Eecs: an energy efficient clustering scheme in wireless sensor networks", In PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005, *IEEE*,pp.535–540, 2005.

[28] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey", *Computer networks*, vol. 52, no. 12, pp.2292–2330, 2008.