Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Secure Data Aggregation Technique in the Existence of Conspiracy Attacks for WSN

Gottipati Ravi Teja[#1], Maddali M. V. M. Kumar[*2]
[#1]P.G. Student, Department of MCA, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh
[*2]Assistant Professor, Department of MCA, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

***Abstract - Network security implicates the authorization of access to data in a network, which is precise the network administrator. Wireless Sensor Network (WSN) states to a set of spatially isolated and committed sensors for watching and recording the physical situations of the atmosphere and forming the collected data at a central location. Conspiracy attack means the set of nodes to access the illegal data. The data collected from different nodes aggregated at a base station or host computer. Due to imperfect computational power and power possessions, aggregation of information from several sensor nodes finished at the aggregating node is traditional accomplished by humble approaches such as averaging. Though, such aggregation well known to be highly vulnerable to node conceding attacks. Iterative filtering algorithms grasp inordinate promise for such a function. Such algorithms at the similar period aggregate data from several sources and arrange for trust impost of these sources frequently in a form of consistent weight factors assigned to data providing by each source. Data aggregation procedure can increase the robustness and precision of information, which obtained by entire network. In a wormhole attack, the attacker obtains packets at solitary point in the network, straight on them throughout a wired or wireless connection with less expectancy than the system links, and relays them to another point in the network. A distribute wormhole detection algorithm for WSNs, which identify wormholes built on the distortions they create in a network.***

***Keywords - Data Aggregation Technique, Conspiracy Attack, Wireless Sensor Networks, Iterative Filtering Algorithm***

## I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a pool of these nodes that have the facility to sense, process data and communicate with further via a wireless connection. Wireless sensor networks (WSN"s) the enhancement in sensor technology has prepared it probable to have very small, low powered sensing devices fortified with programmable compute, multiple parameter sensing and wireless message capability. In addition, the low cost makes it conceivable to have a network of hundreds or thousands of these sensors, thereby improving the consistency and accurateness of data and the area coverage. WSNs offer information about isolated structures, extensive environmental changes, etc. Wireless sensor network (WSN) is a network system comprised of spatially disseminated devices using wireless sensor nodes to observe physical or eco-friendly situation, such as sound, temperature, and gesture.

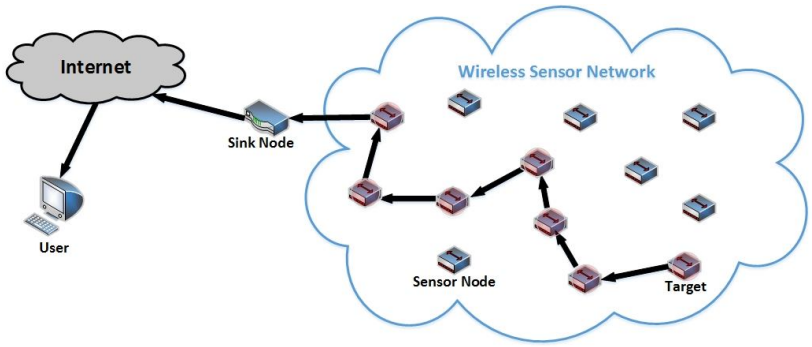


Fig. 1: An Operating System of a WSN

Faith and reputation systems have a significant role in supporting operation of a widespread of distributed systems, from wireless sensor networks and e-commerce substructure to social networks, by providing an assessment of dependability of participants in such distributed systems. A dependability assessment at any specified moment signifies an aggregate of the behaviour of the participants up to that moment and has to be robust in the Survival of some types of faults and malicious behaviour. There are a number of enticements for attackers to deploy the faith and reputation scores of participants in a distributed system, and such

manipulation can severely impair the recital of such a system. The main aim of malicious attackers are aggregation algorithms of faith and reputation systems.

A sensor network premeditated to do a set of high-level information dealing out tasks such as detection, track, or categorization. Measures of recital for these tasks well defined, including discovery of false alarms or misses, classification errors, and track quality. As the computational power of very low power processors dramatically increase, frequently determined by demands of mobile computing, and as the cost of such technology drops, WSNs will be able to afford hardware, which can contrivance more classy data aggregation and trust assessment algorithms; an example is the recent emergence of multi-core and multi-processor systems in sensor nodes. Iterative Filtering (IF) algorithms are a gorgeous option for WSNs because they solve both problems - data aggregation and data dependability assessment - using a single iterative procedure. Such dependability estimate of each sensor built on the distance of the readings of such a sensor from the estimate of the correct values, gotten in the earlier round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is frequently a weighted average; sensors whose readings suggestively differ from such estimate the assigned less dependability and subsequently in the aggregation progression in the present round of iteration their readings are gave a lower weight.

## II. LITERATURE WORKS

In this paper [3] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T, they present one privacy -preserving data aggregation scheme for additive aggregation functions, which can be extensive to approximate MAX/MIN aggregation function. The first method Cluster-based Private Data Aggregation (CPDA)-leverages clustering protocol and algebraic properties of polynomials. It has the benefit of incur less communication overhead. The second scheme Slice – Mix – AggRegaTe (SMART) builds on slicing techniques and the associative property of addition.

In [4] Carlos R. Perez-Toro, Rajesh K. Panta, Saurabh Bagchi in this paper RDAS, a strong data aggregation protocol that use a reputation-based advance to recognize and cut off cruel nodes in a sensor network. RDAS built on a hierarchical cluster form of nodes, where a cluster head clarify data from the cluster nodes to find out the location of an event. It uses the repetition rted by each node. RDAS is able to execute accurate data aggregation in the Existence of independently hateful and collude nodes, as well as nodes that try to compromise the integrity of the reputation system by lying about other nodes" behavior. In [1] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, our work is also closely related to the faith and prominence systems in WSNs. Authors proposed a general reputation framework for sensor networks in which each node develops a reputation estimation for other nodes by observing its neighbour's which make a trust community for sensor nodes in the network.

In [6] Suat Ozdemir, Yang Xiao presents Data aggregation is the procedure of summarizing and merging sensor data in direction to decrease the amount of data transmission in the network. As WSNs often deployed in isolated and hostile atmospheres to transmit delicate messages, sensor nodes are prone to node compromise attacks and security issues such as data privacy and truthfulness are very important. Hence, wireless sensor system protocols, e.g., data aggregation protocol must have deliberate with sanctuary in mind. This paper explores the affiliation between security and data aggregation process in WSNs. A classification of secure data aggregation procedure assumed by measuring the recent state-of-the-art work in this region. In addition, built on the existing study, the open research areas and future research directions in secure data aggregation concept provided.

In [8] X.-Y. Xiao, W. - C. Peng, C. - C. Hung and W. - C. Lee proposed a trust-based framework, which employs correlation to detect faulty readings. Moreover, they introduced a ranking framework to associate a level of dependability with each sensor node built on the number of neighbouring sensor nodes are supporting the sensor.

## III.NETWORK ARCHITECTURE MODEL

A WSN consists of small-sized sensor devices, which fortified with narrow battery power and are capable of wireless communications. When a WSN installed in a sensing field, these sensor nodes will be responsible for sensing irregular events or for collecting the sensed data of the environment. In the case of a sensor node distinguishing an irregular event or being set to occasionally report the sensed data, it will send the note hop-by- hop to a distinct node, named a sink node. The sink node will then inform the supervisor through the Internet.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

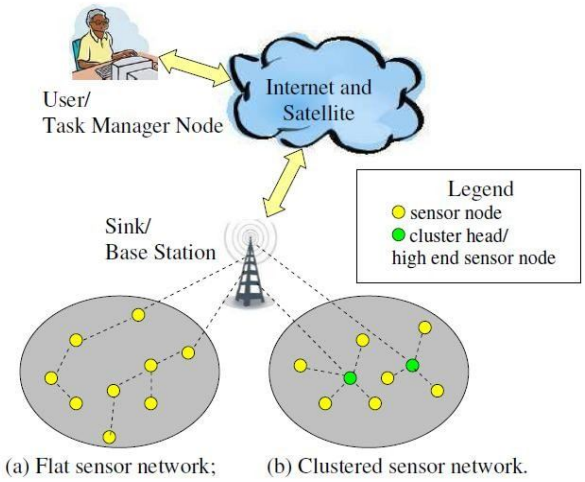


Fig. 1 Network model of a WSN

The sensor nodes separated into disjoint clusters, and each one cluster has a cluster head which acts as an aggregator. Data are periodically together and aggregated by the aggregator.

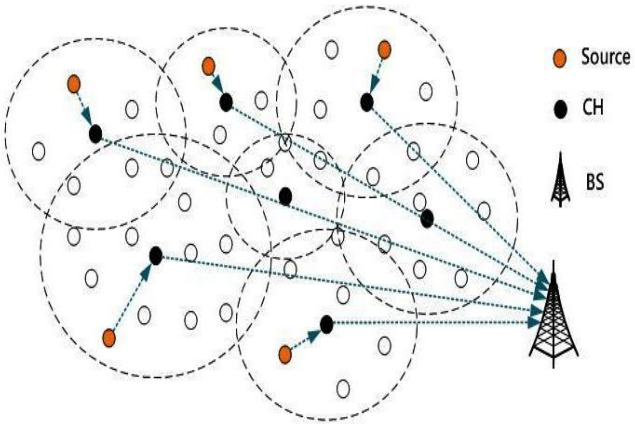


Fig. 3: Cluster Head Communication

In this paper take, for approved that the aggregator itself is not accepted and essence on algorithms, which make aggregation, secure when the specific sensor nodes permitted and might be conveyance false data to the aggregator. Assume that each data aggregator has enough computational power to run an IF algorithm for data aggregation.

*A. Conspiracy Attack in WSN*

Furthermost 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 adjacent to the actual value.

In scenario 2, a challenger conciliations two sensor nodes, and modifies the readings of these values such that the humble average of all sensor readings skewed towards a lesser value. As these two sensor nodes report a lower value, IF algorithm reprimands them and disperses to them lower weights, since their values are far from the values of other sensors. In further words, the algorithm is robust counter to false data injection in this scenario because the conceded 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.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

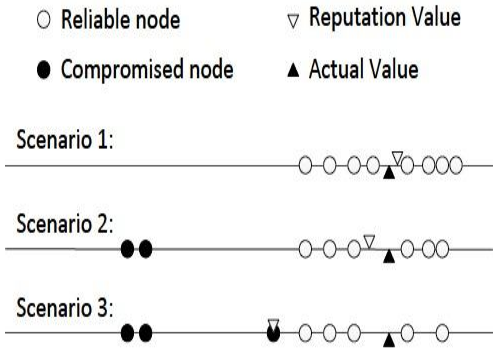


Fig. 4: Attack Scenario against IF Algorithm

In scenario 3, an antagonist employs three conceded nodes in direction to introduce a conspiracy attack. It listens to the reports of sensors in the network and inculcates the two conceded sensor nodes to report values far from the true value of the measured quantity. It then computes the skewed value of the humble average of all sensor readings and instructions the third conceded sensor to report such skewed average as its readings.

*B. Data Aggregation Technique Framework Overview*

In this part, present our robust data aggregation method. In direction to recover the recital of IF algorithms against the aforementioned attack scenario, we make available a robust initial estimation of the dependability of sensor nodes to be used in the first iteration of the IF algorithm.

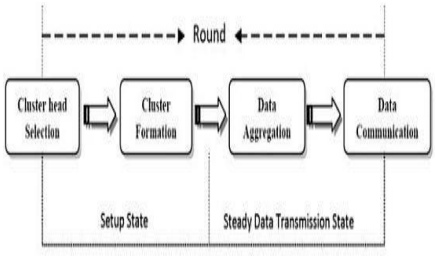


Fig. 5: Framework Overview of Data Aggregation Technique

Most of the traditional statistical estimation methods for variance involve use of the sample mean. For this reason, suggesting a robust variance estimation method in the case of skewed sample mean is a necessary part of our approach.

*C. Enhanced Iterative Filtering Algorithm*

IF algorithm is robust in contradiction of the simple outlier injection by the conceded nodes. An antagonist employs three conceded nodes in direction to launch a conspiracy attack. It listens to the reports of sensors in the network and instructs the two conceded sensor nodes to report values far from the true value of the measured quantity. It then computes the skewed value of the humble average of all sensor readings and instructions the third conceded sensor to report such skewed average as its readings.

In other words, two conceded nodes distort the node reports a value very adjacent to such distorted average thus making such reading appear to the IF algorithm as a highly dependable reading. As a result, IF algorithms will meet to the values provide by the third conceded node, because in the first iteration of the algorithm the third conceded node will achieve the highest influence, radically dominate the weights of all other sensors. Initial test vector based on the IF method provide a robust nature of the security system.

## IV. EXPERIMENTAL OUTCOMES

The objective of our research is to evaluate the robustness and efficiency of our approach for estimating the true values of signal based on the sensor readings in the Existence of faults and conspiracy attacks. For each experiment, we evaluate the accuracy based on Root Mean Squared error (RMS error) metric and efficiency based on the number of iterations needed for convergence of

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IF algorithms. Apply dKVD - Reciprocal, dKVD - Affine, Zhou, Laureti and robust aggregation approach to synthetically generated information. Although simply apply our robust framework to all existing IF approaches, in this paper study the improvement which addition of our initial dependability assessment method produces on the robustness of dKVD - Reciprocal and dKVD - Affine methods. The main shortcoming of the IF algorithms in the proposed attack scenario is that they quickly converge to the sample mean in the Existence of the attack scenario. In direction to investigate the shortcoming, we conducted an experiment by increasing the sensor variances as well as the number of colluders.

In this experiment, quantified the number of iterations for the IF algorithm with reciprocal discriminant function (dKVD - Reciprocal and Robust Aggregate - Reciprocal algorithms). The outcomes obtain from this experiment show that the original version of the IF algorithm quickly converges to the skewed values provided by one of the attackers, while starting with an initial reputation provided by our approach, the algorithms require around 29 iterations, and, instead of converging to the skewed value provided by one of the attackers, it provide a reasonable accuracy.

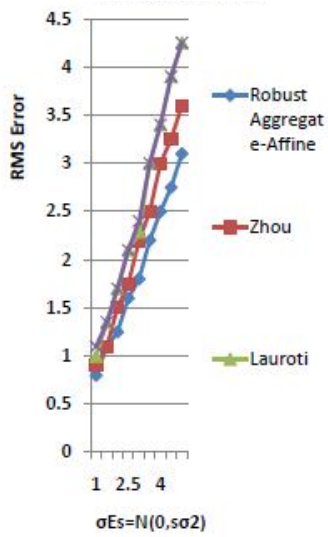


Fig. 6: Accuracy for Conspiracy Attack Scenarios

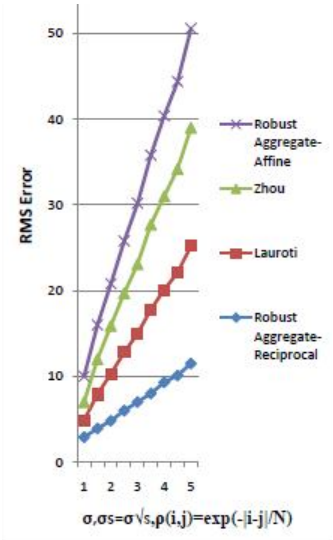


Fig. 7: Correlated Noise

The outcomes of this experiment illustration that the proposed initial reputation for the IF algorithm improve the efficiency of the algorithm in terms of the number of iterations until the process has converged. In other words, by providing this initial reputation, the number of iterations for IF algorithm decreases approximately 9% for reciprocal and around 8% for affine discriminant functions in both biased and unbiased conditions. This can be clarified by the detail that the new initial reputation is adjacent to the true value of signal and the IF algorithm needs fewer iterations to reach its stationary point.

## V. CONCLUSIONS

Conceded node provide a false data aggregated information to the aggregator node so the total information collected by the node should be wrong. This can be avoiding by implementing the iterative filtering algorithm introduced in the aggregator node for providing a security. Hope and reputation have been newly advised as an effective security apparatus for WSNs Iterative Filtering (IF) they solve both problems data aggregation and data reliability assessment using a single iterative procedure in direction to improve the recital of IF algorithms against the aforementioned attack scenario provide a robust initial estimation of the dependability of sensor nodes to be used in the first iteration of the IF algorithm. Proposed an improvement for the IF algorithms by providing an initial approximation of the algorithms not only conspiracy robust, but also more precise and faster converging.

## REFERENCES

[1] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation based framework for high integrity sensor networks,” ACM Trans. Sen. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.
[2] Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: a secure hop by hop data aggregation protocol for sensor networks,” in MobiHoc, 2006, pp. 356–367.
[3] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T. 2011. “Privacy preserving data aggregation for information collection “ACM Transaction Sensor Network. Article 6 (August 2011.DOI = 10.1145/1993042.199)3048.
[4] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance- based trustworthiness assessment in sensor networks,” in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN ¨10, 2010, pp. 2–7.

[5] S. Roy, M. Conti, S. Setia, , and S. Jajodia, "Secure data aggregation in wireless sensor networks," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1040–1052, 2012.
[6] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1–4.
[7] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita- rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," Department of Computer Science, Johns Hopkins University, Tech, Tech. Rep., 2004.
[8] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using Sensor Ranks for in-network detection of faulty readings in wireless sensor networks," in Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, ser. MobiDE" 07, 2007, pp. 1–8.