Enhanced Filtering Technique to Filter False Data in Wireless Sensor Networks

[1]S.D.Manojna, [2]Dr CH.Satyanarayana
[1,2]Dept. of CSE, Jawaharlal Nehru Technological University Kakinada, Eg dt, AP, India

Abstract
As a result of confined computational power and vitality resources, aggregation of data from various sensor hubs done at the aggregating hub is regularly mastered by fundamental methodologies, for instance, averaging. However such total is known to be highly vulnerable to hub compromising assaults. Since WSN are, for the most part unattended and without modified safe gear, they are exceptionally helpless to such attacks. Consequently, finding unwavering quality of data and reputation of sensor hubs is crucial for WSN. As the execution of low power processors radically upgrades, future aggregator hubs will be fit for performing more modern data all out computations, subsequently making WSN less vulnerable. In this we demonstrate that few existing iterative isolating counts, while in a general sense more solid against connivance strikes than the direct averaging strategies, are by and by susceptive to a novel modern agreement assault we exhibit. To address this security issue, we propose a change for iterative separating procedures by giving a hidden theory to such counts which makes them agreement strong, and more exact and quicker combining.

Keywords
WSN, Robust Data Aggregation, Collusion Attacks

I. Introduction

Because of a requirement for robustness of observing and ease of the nodes, Wireless Sensor Networks (WSNs) are generally repetitive. Information from various sensors is aggregated at an aggregator node which then advances to the base station just the total qualities. At present, because of constraints of the registering force and vitality asset of sensor nodes, information is accumulated by to a great degree basic calculations, for example, averaging. Be that as it may, such conglomeration is known not extremely powerless against issues, and all the more critically, malignant assaults. This can't be helped by cryptographic techniques, in light of the fact that the aggressors by and large increase complete access to data put away in the traded off hubs. Consequently information accumulation at the aggregator hub must be joined by an appraisal of reliability of information from individual sensor nodes. Consequently, better, more complex algorithms are required for information accumulation later on WSN

II. Literature Survey

[1] we propose a computational proficient technique to register a weighted average (which we will call robust average) of sensor estimations, which properly takes sensor deficiencies and sensor commotion into thought. We accept that the sensors in the WSN use random projections to pack the information and send the compacted information to the information combination focus. Computational proficiency of our technique is accomplished by having the information combination focus work specifically with the compacted information streams. The key preferred standpoint of our proposed technique is that the information combination focus just needs to perform decompression once to figure the robust average, in this way extraordinarily lessening the computational necessities. We apply our proposed strategy to the information gathered from two WSN deployments to show its productivity and exactness.

[2]we propose a zone-based node compromise location and renouncement plan in remote sensor systems. The principle thought behind our plan is to utilize successive speculation testing to identify suspect locales in which traded off nodes are likely put. In these suspect locales, the system administrator performs programming confirmation against sensor nodes, prompting the recognition and renouncement of the traded off nodes. Through quantitative examination and simulation tests, we demonstrate that the proposed plan identifies the traded off nodes with a little number of tests while diminishing false positive and negative rates, regardless of the fact that a generous portion of the nodes in the zone are compromised.

III. Problem Definition

In the past composing it was found that these algorithms demonstrate better power appeared differently in relation to the straightforward averaging methods; in any case, the past examination did not consider more refined plot assault circumstances. In case the aggressors have an anomalous condition of finding out about the collection computation and its parameters, they can coordinate refined strikes on WSNs by exploiting false data implantation through different exchanged off nodes.

IV. Proposed Approach

We propose an answer for vulnerability by giving an underlying trust estimate which depends on a vigorous estimation of errors of individual sensors. Recognizable proof of another complex intrigue assault against IF based notoriety frameworks which uncovers a severe vulnerability of IF algorithms. A novel technique for estimation of sensors' errors which is powerful in an extensive variety of sensor faults and not helpless to the described attack. Outline of a productive and hearty conglomeration strategy inspired by the MLE, which uses an estimate of the noise parameters got utilizing commitment above. Upgraded IF plans ready to ensure against modern agreement attacks by giving an underlying assessment of dependability of sensors utilizing inputs from commitments

V. System Architecture

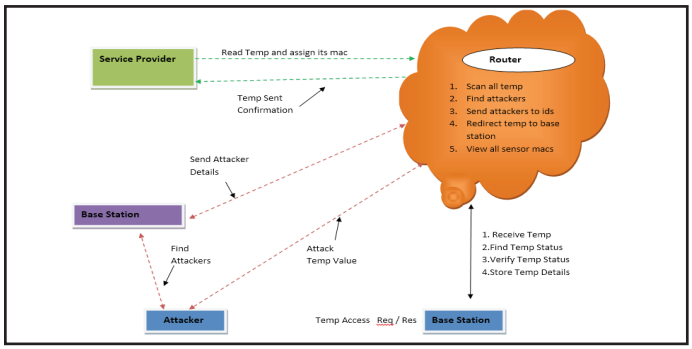


Fig. 1:

VI. Proposed Methodology

A. Sender

The Sender institutes each one of the sensors and allocates temperatures to the sensor node, and backup temperature will be secured, exchanges their data to the particular base station. It will store in node. The Sender, can see the attacked record by the Base Station, He can supplant the implanted fake temperature to the sensor node.

B. Network

The predicate check inquiry is used to choose the total number of nodes whose sensor readings have some property in the framework. Besides, it is accountable for passing on the sensor readings to the Base stations. In case he builds up fake temperature readings then it trade the stream to Base Station. Before sending any record to beneficiary temperature will be affirmed, then send to particular base station. In a framework we can see the sensor temperature purposes of interest and clear the subtle elements.

C. Base Station

The base station collecting all sensor nodes (sn1, sn2, sn3, sn4, sn5….) and computing aggregation results at the base station (BS), in network aggregation allows sensor readings to be aggregated by intermediate nodes, which efficiently reduces the communication overhead. The Base Station used for checking the temperature status and to verifies the results through reliable random sampling achieved by data commitment and interactive proofs with the base station.

D. Attacker

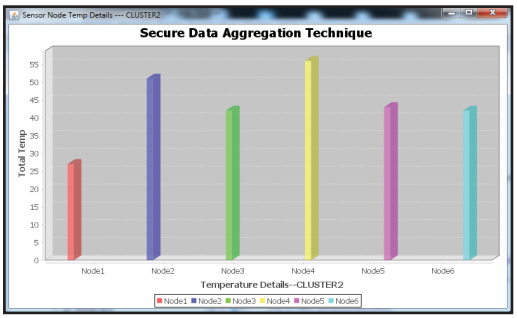
Attacker is one who is injecting the fake temperature to the particular sensor node. And Router will identify the attackers, then stored in attacker list.

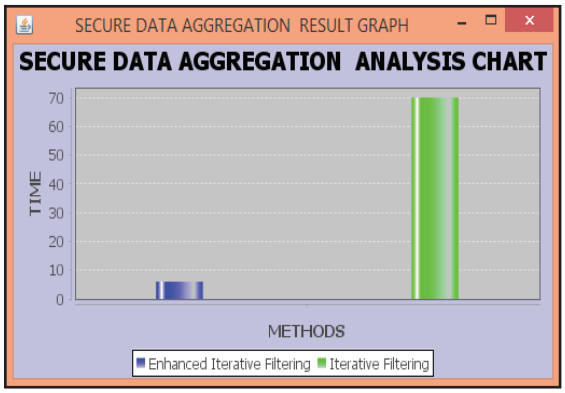
VII. Algorithm

A. Enhanced Iterative Filtering Algorithm

STEP 1: BS forwards the query to clustered sensor nodes
STEP 2: Clustered sensor nodes forwards randomly selected MAC for each 1 bit in BS.
STEP 3: BS verifies the received MAC of sensor nodes and confirms only 1 bit indicated received final value.
STEP 4: Otherwise BS reset to zero indicates invalid MAC.
STEP 5: BS demand the clustered sensor nodes to send bits as well as corresponding MAC.
STEP 6: After receive the request from BS each clustered sensor nodes forward to its parent MAC.
STEP 7: BS receives the MAC any bit in synopsis and valid HMAC is received is set to 1

VIII. Results





This result graphs indicate the detection of compromised sensor nodes in different clusters and the efficiency of the technique aganist existing methods.

IX. Conclusion

We introduced a novel collusion attack circumstance against different existing IF algorithms. Moreover, we proposed a change for the IF algorithms by giving a hidden conjecture of the constancy of sensor hubs which makes the calculations agreement intense, and in addition more correct and speedier joining. In future work, we will investigate whether our strategy can secure against exchanged off aggregators.In this paper, we identify distinct design issues for secure continuous aggregation in WSNs.An efficient verification scheme is proposed to protect the authenticity of the temporal variation patterns in the aggregation results.Compared with the existing secure aggregation schemes, our scheme only need to check a small portion of aggregation results in a time window and, thus, greatly reduces the verification cost.

X. Future Work

In future introduce cryptographic methods to avoid compromising attacks and develop new algorithms to prevent packet dropping, Sybil, sink hole attacks in cluster based wireless sensor networks

References

[1] S. Ozdemir, Y. Xiao,"Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw., Vol. 53, No. 12, pp. 2022–2037, Aug. 2009.
[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,
[3] A. Jøsang, J. Golbeck,"Challenges for robust trust and reputation systems," In Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.
[4] K. Hoffman, D. Zage, C. Nita-Rotaru,"A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, Vol. 42, No. 1, pp. 1:1–1:31, Dec. 2009.
[5] R. Roman, C. Fernandez-Gago, J. Lopez, H. H. Chen, "Trust and reputation systems for wireless sensor networks," In Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,
[6] H.-S. Lim, Y.-S. Moon, E. Bertino,"Provenance-based trustworthiness assessment in sensor networks," In Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, X. Liu,"Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," In Proc. 7th Int. Conf. Wireless Commun., Netw.

Mobile Comput., 2011, pp. 1–4.
[8] C. de Kerchove and P. Van Dooren, "Iterative filtering in reputation systems," SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.
[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.
[10] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," Europhys. Lett., vol. 75, pp. 1006– 1012, Sep. 2006.
[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A: Statist. Mech. Appl., vol. 371, pp. 732–744, Nov. 2006.
[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputationbased ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.
[13] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.
[14] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," in Proc. 20th Int. Conf. Found. Intell. Syst., Aug. 2012, pp. 405–414.
[15] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment," in Proc. 17th ACM SIGK

Ms.S.D.Manojna is a student of JNTUK College of Engineering kakinada. Presently she is pursuing her M.Tech [Software Engineering] from this college and she received her B.Tech from Pragati Engineering college, affiliated to JNTUK University, Kakinada in the year 2014. Her area of interest includes Computer Networks and database systems, all current trends and techniques in Computer Science.

Dr.Ch.Satyanarayana, Professor and Director & Academic Planning (DAP) JNTUK Kakinada.He is an excellent teacher and received his PHD (CSE) from JNTUK university, MTech & BTech from Andhra university. He worked as professor for 4 years, associate professor for 6 years and assistant professor for 6 years .His area of interest include Image Processing, networking and security.