International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, July 2015
ISSN: 2395-3470
www.ijseas.com

SECURE AND ENERGY EFFICIENT DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

Pechetti Murali[1], M.Neelima[2], Dr.Y.Venkateswarulu[3]

[1]Mtech Student, CSE, Giet Engineering College, Rajahmundry, A,P, India
[2]Assoc Professor, Dept of CSE, Giet Engineering College, Rajahmundry, A,P, India
[3]Professor and HOD Dept of CSE, Giet Engineering College, Rajahmundry, A,P, India

ABSTRACT

To decrease the correspondence overhead and drag out the system lifetime information accumulation is utilized in remote sensor systems. Then again, a rival may bargain some sensor hubs, and utilization them to produce false values as the accumulation result. Past secure information conglomeration plans have handled this issue from diverse points. The objective of those calculations is to guarantee that the Base Station (BS) does not acknowledge any fashioned collection results. Be that as it may none of them have attempted to identify the hubs that infuse into the system fake collection results. Also, the greater part of them generally has a correspondence overhead that is, (best case scenario) logarithmic every hub. In this paper, we propose a protected and vitality effective information total plan that can distinguish the awful hubs with a steady every hub correspondence overhead. In our answer, all total results are marked with the private keys of the aggregators so they can't be modified by others. Hubs on every connection moreover utilize their pair-wise imparted key for secure correspondences. Every hub gets the total results from its parent (sent by the guardian of its parent) and its kin (through its parent hub), and confirms the collection aftereffect of the guardian hub. Hypothetical examination on vitality utilization and correspondence overhead concurs with our correlation based recreation examine over irregular information conglomeration trees.

INTRODUCTION

Remote sensor systems (WSNs) are getting to be progressively well known to give answers for some security-discriminating applications, for example, out of control bonfire following, military observation, and country security [1]. In sensor systems, a great many sensor hubs on the whole screen a range. As all the sensor hubs in a range normally distinguish regular phenomena, there is high repetition in the crude information. To spare vitality and drag out system lifetime, a proficient route is to total the crude information before they are transmitted to the base station as the sensor hubs are asset constrained and vitality obliged. Information accumulation [2–6] is a key standard to dispose of information repetition and decrease vitality utilization. Amid an ordinary information total procedure, sensor hubs are composed into a various leveled tree established at the base station the sensor hubs are regularly conveyed in threatening and unattended situations, and are not made carefully designed because of expense contemplations. So they may be caught by an enemy, which might self-assertively mess with the information to accomplish its own motivation. Along these lines, a vital issue in applying information collection is to stay

away from such altering so the base station can get the right information conglomeration result.

To meet this test, some work has been carried out [7–12] in the territory of secure information total. Case in point, Chan et al. [7] set forward a protected various leveled in-system conglomeration conspire that gives great and amazing security properties. This plan can confirm whether altering has happened on the way between a leaf and the root [7]. All things considered, it can't pinpoint the accurate hub where the altering has happened on account of altering. To the best of our insight, none of the current work has the capacity recognize the hubs that mess with the middle total results. To defeat this insufficiency, we exhibit a safe and vitality effective information total plan termed MAI [13] to successfully find the malevolent aggregators in remote sensor system

1. OVERVIEW OF DATA AGGREGATION:

Information accumulation has the profit to attain to transfer speed and vitality proficiency. There has been far reaching exploration [13–15] on information conglomeration in different application situations. These accumulation plans have been outlined without security as a primary concern. Notwithstanding, remote sensor systems are liable to be conveyed in antagonistic situations, for example, the combat zone, where a foe may trade off hubs and control the information. Secure information accumulation [16,17] is a hot exploration issue in a few applications. Fundamentally, there are two sorts of collection models, i.e., the single-aggregator model and the various aggregator models.

The creators in [8,9] explored secure information accumulation for the single-aggregator model. The protected data total (SIA) convention displayed by Przydatek et al. [8] was the first to propose the aggregate–commit–prove structure. In this model, the BS is the main aggregator. Du et al. [9] proposed a plan utilizing different witness hubs as extra aggregators to check the trustworthiness of the collected result. Concerning the single-aggregator model, the comparing plans don't give every jump collection. The numerous aggregator model utilizes more than one aggregator. Hu and Evans [12] exhibited a safe accumulation convention that is flexible to single aggregator trade off. In any case, this convention can't manage the circumstance where there exist two successive conniving bargained aggregator hubs in the tree. Yang et al. [10] proposed SDAP, which uses a novel probabilistic gathering strategy to powerfully subdivide a conglomeration tree into sub-trees of comparative sizes, each of which reports its total result. Suspicious gatherings partake in a validation methodology to demonstrate the rightness of its gathering total. Because of the factual nature, SDAP will most likely be unable to recognize the assaults that somewhat change the halfway conglomeration results. In the protection conservation domain, Castelluccia et al. [18] proposed another homo-morphic encryption plot in which the collection is completed by amassing the encoded information at middle sensors without decoding them, bringing about a larger amount security. He et al. [19] proposed two security saving information conglobe

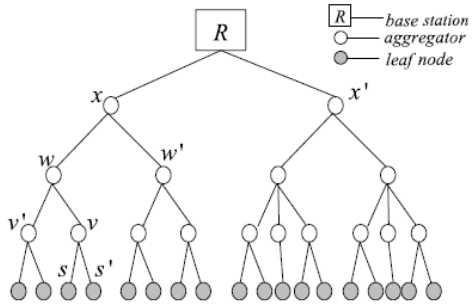

Fig 1: An example aggregation tree.

2. THE PROPOSED METHOD: SECURE AND ENERGY-EFFICIENT DATA AGGREGATION WITH NASTY AGGREGATOR NAMING (NAN)

In this segment, we show a safe and vitality proficient information total with frightful aggregator naming (NAN). For effortlessness, we depict our plan for the SUM total capacity. Notwithstanding, our outline helps different other conglomeration capacities, for example, MAX/MIN, MEAN, COUNT, etc. We apply our plan on the total tree demonstrated in Fig. 1.

Conglomeration duty: Before depicting the points of interest of the proposed plan, we first present the arrangement of the parcels transmitted amid the accumulation. Every hub has a related parcel to speak to its information that is transmitted to its parent. Such a bundle has the accompanying configuration:

⟨id, tally, esteem, signature⟩

whereid is the hub's ID, tally is the quantity of leaves in the sub-tree established at this hub, quality is the accumulation result figured over all the leaves in the sub-tree, and mark is a guarantee processed by the hub utilizing its privateThe packet for node ui can be inductively expressed as: ⟨u_i, C_i, V_i, S_i⟩

where S_i is a cryptographic hash function over the packet value. If u_i is a leaf node, then $C_i = 1$ and $V_i = r_{ui}$, where r_{ui}isthe data collected by node u_i. If u_i is an intermediate node havingchild nodes vj (j = 1, 2, . . . , k) with packets ⟨v_j, C_j, V_j, S_j⟩, then

$$C_i = \sum_{j=1}^{k} C_j, V_i = \sum_{j=1}^{k} V_j \qquad (1)$$

The pair-wise key shared between ui and its parent node is used to encrypt the packet. This encryption in practice provides not only confidentiality but also authentication. Using encryption saves the bandwidth that will otherwise be used for an additional message authentication code (MAC) [10].

AGGREGATION VERIFICATION

The motivation behind our plan is to empower every sensor hub to autonomously check whether its parent has done the right total operation. The confirmation is performed by recalculating the collection result utilizing its own particular worth and the qualities from all its kin, then contrasting the figured result and the one of its parent. In the event that an irregularity happens at a guardian hub, the guardian hub is recognized as a malevolent hub. Before we display the subtle elements of our check methodology, an abnormal state review of the procedure is presented as takes after. To start with, every sensor hub gets the estimations of all its kin (called kin qualities) and the collection aftereffect of its parent hub. At that point it autonomously confirms whether its parent's total result approaches the recalculated one in view of its own worth and the got kin qualities. If not, a caution is raised (for instance, utilizing show) to caution the whole system that the guardian hub is malevolent, and the pernicious hub can be ousted from the system through a certain technique. On the off chance that no caution is raised, all the

accumulation operations are right, and the last conglomeration result can be acknowledged by the BS. In what tails, we will show the itemized outline of the proposed plan.

(1) Dissemination of the kin parcels: To empower check, every sensor hub must get the estimations of its kin to recalculate the totaled estimation of its parent. In this way, every guardian hub is obliged to disseminate the duplicates of the kin parcels to all youngster hubs. After getting the kin bundles, every hub confirms their marks, which are utilized to guarantee that the guardian hub can't mess with the parcels of its youngster hubs in light of the fact that it doesn't know the private keys of its youngsters.

(2) Dissemination of guardian parcels: To figure out if the total operation is right or not, the tyke hubs need to know the first collection result acquired by its parent hub. In any case, a malignant guardian hub may mess around with the total result in the conglomeration stage, however send a right result to its youngster hubs in the confirmation stage so it can abstain from being recognized. In our plan, the grandparent hubs are included, which keep the guardian hubs from transmitting diverse qualities. Really, it is the grandparent hubs that send the guardian hubs' collected qualities to the youngster hubs. As demonstrated in the illustration (Fig. 1), w is the grandparent hub, v is the guardian hub, and s is the kid hub. The parcel w gets from v is indicated in mathematical statement 2.

$$v \rightarrow w\langle v,\ 2,\ Agg_v,\ \{H(v\|2\|Aggv)\}K^{-1}{}_v\rangle.| \quad (2)$$

This packet should be sent to the child node s in the verification phase. First, w encrypts the signature of v using its own private key. In other words, the signature of w in this packet is calculated over v's signature.

$$w \rightarrow v\langle v,\ 2,\ Agg_v,\ \{\{H(v\|2\|Agg_v)\}K^{-1}{}_v\}K^{-1}{}_w\rangle \quad (3)$$

v verifies the signature and then sends the packet to s and s′ .

The explanation behind the second signature including two private keys is to verify that not the grandparent hub or the guardian hub can mess with the bundle, so that the parcel must be the first one got in the conglomeration stage.

(3) Verification of the guardian's collection: After every sensor hub gets its kin qualities and its parent esteem, it can check the guardian's conglomeration if all the bundles pass the confirmations on their marks.

Every sensor hub runs the same process as did by its parent to infer the accumulation result. This is executable as the kin qualities give all the vital information to perform the collection. When it has registered the guardian total result, it looks at the recently inferred result against the one already got from its grandparent. In the event that these two outcomes are not indistinguishable, the kid hub promptly raises an alert telling different hubs in the system that its parent hub is vindictive. Just when all the confirmation succeeds, the BS acknowledges the accumulation result.

RESULTS AND DISCUSSIONS

To assess the execution for more general cases, we direct a reproduction study utilizing the NS-2 test system to contrast NAN and SHIA. In our tests, the hubs are haphazardly appropriated over a region. After the system is sorted out into a collection tree, we actualize the two plans on the same tree for different systems

administration scales. The system size n shifts from 50 hubs to 250 hubs. For n < 100, the appropriated zone is a 200×200m2 field; for 100 ≤ n < 200, the region is 300×300 m2; and for 200 ≤ n ≤ 250, it is 400 × 400 m2. For every mimicked topology, we modify the correspondence run so that all the sensor hubs are incorporated in the total tree. In our study, we consider a vitality show that sets 0.2818Wfor sending or getting an information bundle every unit of time, and 100 J of aggregate accessible battery power every hub. The information rate is 1 Mbps. We analyze the correspondence overhead and the vitality utilization of NAN with those of SHIA and the outcomes are accounted for in the accompanying subsection.

Fig. 2 demonstrates the correspondence overhead of NAN and that of SHIA under diverse system scales. We utilize packet*hop as the metric. As can be seen from Fig. 2, the overhead of NAN is much lower than that of SHIA. To further investigate the reliance of the execution on the extent of the collection tree, we report the normal correspondence overhead every hub in Fig. 3. As demonstrated in this figure, NAN outflanks SHIA regarding the normal measure of correspondences. Furthermore NAN displays a little change when n ranges from 50 to 250. The correspondence overhead is nearly identified with the system topology. It increments with the tree tallness for SHIA on the grounds that the off-way values need to transmit more jumps to achieve the leaf hubs, and it increments with the tree degree for NAN in light of the fact that the youngster hubs need to get additionally kin qualities to check the guardian hub when the tree degree is huge. In the reproductions, the hubs are arbitrarily conveyed in the region; subsequently, the trees composed over the hubs additionally have distinctive topologies for diverse system scales. That is the reason the overhead increments with the increment of the system size, yet at the same time vacillates at a few

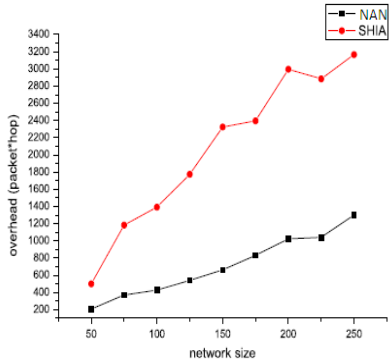

Fig 2: Communication overhead under different network scales

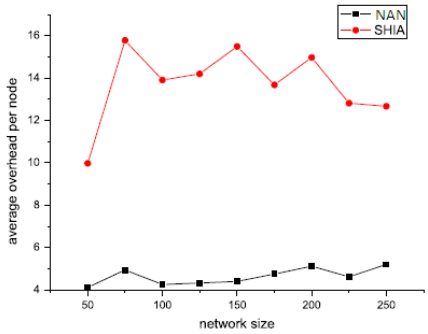

Fig 3: Average communication overhead per node.

Figs. 4 and 5 delineate the vitality utilization under diverse system scales. The rate of the remaining vitality in the bit of the force utilization for sensor hubs, and the correspondence overhead of SHIA is higher than that of NAN as talked about some time recently. Since the vitality utilization is nearly identified with the correspondence overhead, our outcomes demonstrate a general pattern of expanding with expanding the system size, with a few changes at a few focuses much the same as the outcomes

indicated in Fig. 2. In outline, the hypothetical and reproduction results both demonstrate that our proposed NAN is more proficient and successful than SHIA, as it can distinguish the malevolent aggregators with a much lower correspondence overhead.

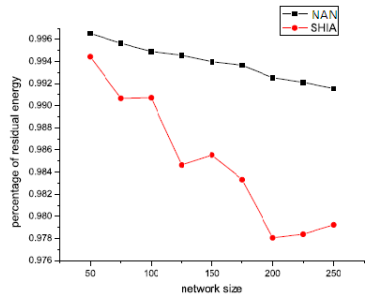

Fig 4: Percentage of the residual energy under different network scales

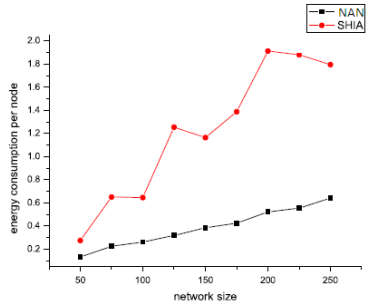

Fig 5: Average energy consumption per node.

CONCLUSIONS

In this paper, we propose a safe and vitality productive information total plan with pernicious aggregator recognizable proof in remote sensor systems. The objective of our proposed plan is to verify that not just does the BS not acknowledge produced conglomeration results, additionally the noxious aggregators messing with the middle results can be recognized. The antagonistic aggregators, after location, can be ousted from the system, henceforth lessening the harm of malevolent aggregators. Hypothetical investigation and broad reenactments have been directed to assess our plan. The outcomes demonstrate that our proposed plan is more secure and vitality effective than SHIA, a cutting edge secure progressive in-system total plan proposed in [7].

REFERENCES:

1. D. Culler, D. Estrin, M. Srivastava, Overview of sensor networks, IEEE Comput. 37 (8) (2004) 41–49.
2. D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, in: Proceedings of the ACM International Conference on Mobile Computing and Networking, MobiCom, 1999, pp. 263–270.
3. J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, D. Ganesan, Building efficient wireless sensor networks with low-level naming, in: Proceedings of the ACM Symposium on Operating Systems Principles, SOSP, 2001, pp. 146–159.
4. B. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in wireless sensor networks, in: Proceedings of the International Conference on Distributed Computing Systems (ICDCS) Workshops, 2002, pp. 575–578.
5. Y. Yu, B. Krishnamachari, V.K. Prasanna, Energy-latency tradeoffs for data gathering in wireless sensor networks, in: Proceedings of the IEEE Computer and Communications Societies, INFOCOM, 2004.
6. S. Madden, M.J. Franklin, J.M. Hellerstein, TAG: a Tiny AGgregation service for ad-hoc sensor networks, in: Proceedings of the Symposium on

Operating Systems Design and Implementation, OSDI, 2002.
7. H. Chan, A. Perrig, D. Song, Secure hierarchical in-network aggregation in sensor networks, in: Proceedings of the ACM Conference on Computer and Communication Security, CCS, 2006.
8. B. Przydatek, D. Song, A. Perrig, SIA: secure information aggregation in sensor networks, in: Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, Sensys, 2003.
9. W. Du, J. Deng, Y. Han, P.K. Varshney, A witness-based approach for data fusion assurance in wireless sensor networks, in: Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM, 2003.
10. Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: a secure hop-by-hop data aggregation protocol for sensor networks, in: Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, 2006.
11. Ralph Merkle, A certified digital signature, in: Proceedings on Advances in Cryptology, 1989, pp. 218–238.
12. L. Hu, D. Evans, Secure aggregation for wireless networks, in: Proceedings of the 2003 Symposium on Applications and the Internet Workshops, SAINTW, 2003.
13. C. Itanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, in: Proceedings of the ACM International Conference on Mobile Computing and Networking, MobiCom, 2000.
14. C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, Impact of network density on data aggregation in wireless sensor networks, in: Proceedings of the International Conference on Distributed Computing Systems, ICDCS, 2002
15. X. Tang, J. Xu, Extending network lifetime for precision constrained data aggregation in wireless sensor networks, in: Proceedings of the IEEE Computer and Communications Societies, INFOCOM, 2006.
16. Sankardas Roy, Mauro Conti, SanjeevSetia, SushilJajodia, Secure data aggregation in wireless sensor networks, IEEE Trans. Inform. Forensics Secur. 7 (3) (2012) 1040–1052.
17. M.K. Sandhya, K. Murugan, Secure data aggregation in wireless sensor networks using privacy homomorphism, in: Advances in Networks and Communications, 2011, pp. 482–490.
18. C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks, in: Proceedings of the International Conference on Mobile and Ubiquitous Systems, Mobiquitous, 2005.
19. W. He, X. Liu, H. Nguyen, K. Nahrstedt, T. Abdelzaher, PDA: privacy-preserving data aggregation in wireless sensor networks, in: Proceedings of the IEEE Computer and Communications Societies, INFOCOM, 2007.