International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey: Secure Data Aggregation in Wireless Sensor Networks

Priyanka Kamthe[1], Sanjeev J. Wagh[2]

[1]ME Computer Engineering, KJ College of Engineering, Pisoli, Pune-48, Savitribai Phule Pune University Pune, India

[2]Professor and Principal of KJ Collage of Engineering Pisoli, Pune , Savitribai Phule Pune University Pune, India

Abstract: ***Remote sensor systems (WSNs) are progressively utilized as a part of numerous applications, for example, spring of gushing lava and flame checking, urban detecting, and edge reconnaissance. In an extensive WSN, in-system information collection (i.e., joining incomplete results at middle of the road hubs amid message directing) altogether decreases the measure of correspondence overhead and vitality utilization. The exploration group proposed a misfortune versatile collection structure called abstract dissemination, which uses copy harsh calculations on top of multipath steering plans to precisely process totals (e.g., predicate tally or entirety). Be that as it may, this collection system does not address the issue of false subtotal qualities contributed by bargained hubs. This assault may bring about vast mistakes in the total figured at the base station, which is the root hub in the collection chain of command. they make the summation dispersion methodology secure against the above assault propelled by traded off hubs. Specifically, they display a calculation to empower the base station to safely process predicate includes or whole evensthe vicinity of such an assault. Total by sifting through the of bargained hubs in theaggregation hierarchy. In this paper, we present a survey of data aggregation algorithmsin wireless sensor networks. We compare different algorithms on the basis of performance measures such as security, Communication overhead and data accuracy. We conclude with possible future research directions.***

Keywords: Data aggregation, hierarchical aggregation, in network aggregation,sensor network security, synopsis diffusion, attack resilient.

1. Introduction

In-system information gathering can lessen the sum of correspondence and henceforth the vitality expended, particularly in huge WSNs. The fundamental thought is to join halfway results at moderate hubs amid message directing. One methodology is to develop a crossing tree established at the BS, and after that perform in-system total along the tree. The vital totals considered by the exploration group incorporate Count, and Sum. It is clear to sum up these totals to predicate Count (e.g., the quantity of sensors whose perusing is higher than 10 units) and Sum. In expansion, Average can be registered from Count and Sum. They can likewise effortlessly extend a Sum calculation to register Standard Deviation and Statistical Moment of any request. On the other hand, correspondence misfortunes coming about because of hub and transmission disappointments, which are basic in WSNs, can unfavourably influence tree-based collection approaches. To address this issue, we can make utilization of multi-way steering systems for sending sub-totals [5]. For duplicate insensitive totals, for example, Min and Max, this methodology gives an issue tolerant arrangement. Lamentably, for duplicate sensitive totals, for example, Count and Sum, multi-way steering prompts twofold including of sensor readings. As of late, a few specialists [7], [8] have displayed cunning calculations to tackle this twofold including issue. A vigorous and versatile collection system called rundown dissemination has been proposed for figuring copy delicate totals. This methodology utilizes a ring topology where a hub may have different folks in the total chain of command. Besides, each detected esteem or sub-total is spoken to by a copy obtuse bitmap called rundown.

Sr.No	*Paper Name*	*Technique*	*Advantages*	*Disadvantages*	*Results/Future Scope*
1	Scanning the Issue	**1.**computing, communications, and control systems in delivering automotive **2.**functions that meet both regulatory and consumer demands	improve vehicle safety and reduce fatalities	limited space	Traffic parameters such as traffic flow vehicle speed, and vehicle turn ratio at an intersection can be obtained fairly accurately.
2	Embedded Imagers: Detecting, Localizing and Recognizing Objects and Events in Natural Habitats	**1.**Imaging sensors	rapid motions against dynamic backgrounds with rapid illumination changes	large quantities of data	Temporal over-sampling can simplify the analysis of aslow process such as the avian nesting cycle
3	Synopsis Diffusion for Robust Aggregation in Sensor Networks	Tree topology is used	Energy improvement, accuracy, reliable	Double-counting sensor readings are done.	1. Extensive simulations, the significant robustness, accuracy, and energy efficiency improvements of synopsis diffusion over previous approaches.
4	Secure Data	Network aggregation of sensor	compromised nodes	existing	Security vulnerabilities of data

	Aggregation in Wireless Sensor Networks	data	can be used to inject false data that leads to incorrect aggregates	aggregation algorithms and systems do not include any provisions for security, and consequently these systems are vulnerable to a wide variety of attacks	aggregation systems,and present a survey of robust and secure aggregation protocols that are resilient toFalse data injection attacks.

2. Literature Survey

1. In this paper [1] the author studied the papers span a number of interdependent themes that include: architecture; systems; controls &communications, computing and embedded computers, safety, and intelligent vehicles. Even with the breadth of papers in this issue, they realize that there are a number of topics that are not included. Therefore, to ensure general coverage and, as a prolong to this special issue, they have dedicated the first article under the auspices of BScanning the Technology. [This introductory article mainly overviews the progress of electrical, electronics, software, and other relevant technologies that shape the modern automobile. Some of these technologies are described in more detail in the articles that comprise this special issue.Following this introductory article by the guest editors, the first invited paper is entitled BControl, Computing and Communication

2. In this paper [2], the author demonstrated that, imaging sensors, or "imagers," embedded in the natural environment enable remote collection of large quantities of data, thus easing the design and deployment of sensing systems in a variety of application domains. Yet, the data collected from such imagers is difficult to interpret due to a variety of "nuisance factors" in the data formation process, such as illumination, vantage point, partial occlusions, etc. These are especially severe in natural environments, where the objects of interest (e.g., plants, animals) have evolved to blend with

3. In this paper [4], the author use Jump by-bounce information total is an imperative strategy for decreasing the correspondence overhead and vitality use of sensor hubs amid the procedure of information accumulation in a sensor system. Be that as it may, in light of the fact that individual sensor readings are lost in the per hop total procedure, traded off hubs in the system might fashion false values as the total consequences of different hubs, deceiving the base station into tolerating spurious accumulation results. Here a principal test is: by what means can the base station acquire a decent guess of the combination result when a small amount of sensor hubs are traded off? To answer this test, author proposes SDAP, a Secure Hop-by hop Information Aggregation Protocol for sensor systems. The outline of SDAP depends on the standards of gap and-overcome and commits and-bear witness to. To begin with, SDAP utilizes a novel probabilistic gathering strategyto powerfully parcel the hubs in a tree topology into different coherent gatherings (sub trees) of comparable sizes. A commitment based jump by-bounce total is performed in every gathering to produce a gathering total. The base station then distinguishes the suspicious gatherings taking into account the arrangement of gathering totals. At last, each bunch under suspect takes part in a verification procedure to demonstrate the rightness of its gathering total. Our investigation and reproductions demonstrate that SDAP can accomplish the level of proficiency near a common jump by-bounce collection convention while giving certain affirmation on the reliability of the total result. Besides, SDAP is a broadly useful secure total convention material to different total capacities.

4. Late works on circulated, in-system conglomeration expect a favourable populace of members. Sadly, cutting edge appropriated frameworks are tormented by pernicious members. In this paper we exhibit an initial move towards unquestionable yet productive appropriated, in-system collection in antagonistic settings. Author portray a general structure also, danger model for the issue and afterward present confirmation outlines, a minimal check component that joins

Cryptographic marks and Flajolet-Martin representations to ensure adequate conglomeration mistake limits with high likelihood. We infer confirmation draws for check totals also, develop them for arbitrary examining, which can be utilized to give unquestionable approximations to an expansive class of data analysis inquiries, e.g., quantiles and substantial hitters. At last, they assess the commonsense utilization of confirmation draws, and watch that enemies can regularly be decreased to much littler infringement by and by than our most pessimistic scenario limits recommend.

In this paper [3], the authorPast methodologies for figuring copy delicate totalsin sensor systems (e.g., in TAG) have utilized a tree topology, keeping in mind the end goal to ration vitality and to maintain a strategic distance from twofold including sensor readings. On the other hand, a tree topology is not vigorous against hub and correspondence disappointments, which are basic in sensor systems. In this paper, they exhibit summary dissemination, a general structure for accomplishing essentially more precise and dependable answers by joining vitality effective multi-way directing plans with strategies that dodge twofold including. Abstract dissemination stays away from twofold including through the utilization of request and copy cold-hearted (ODI) abstracts that mini malistically compress middle of the road results amid in-system total. Author gives a shockingly basic test that makes it simple to check the accuracy of an ODI outline. They demonstrate that the properties of ODI summations and outline dissemination make verifiable affirmations of bundle conveyance. Author appeared that this property can, thusly, empower the framework to adjustmessage steering to element message

misfortune conditions, even in the vicinity of topsy-turvy joins. At last, they show, utilizing broad recreations, the critical vigor, exactness, also, vitality proficiency changes of abstract dissemination over past methodologies.

In this paper [7] the author studied that the data from the information the sensors gather. A way to deal with this information administration issue is the utilization of sensor database frameworks, exemplified by Tined and Cougar, which permit clients to perform conglomeration inquiries, for example, MIN, COUNT and AVG on a sensor system. Because of force and range imperatives, unified methodologies are by and large unreasonable, so most frameworks use in-system conglomeration to diminish system activity. In any case, these conglomeration techniques gotten to be data transfer capacity serious when consolidated with the shortcoming tolerant, multi-way directing routines frequently utilized as a part of these situations. For instance, copy delicate totals for example; SUM can't be registered precisely utilizing generously less data transfer capacity than express count. To stay away from this cost, they examine the utilization of inexact in-system accumulation utilizing little draws. Our commitments are as per the following: 1) they sum up well known copy heartless representations for approximating Tally to handle SUM; 2) they exhibit and investigate strategies for utilizing portrayals to create precise results with low communication and calculation overhead, and 3) author exhibit a broad exploratory approval of our routines.

In this paper[10], author studied that the security issues of in-network aggregation algorithms to compute aggregates such as predicate Count and Sum. In particular, Author showed the falsified sub-aggregate attack launched by a few compromised nodes caninject arbitrary amount of error in the base stations estimate of the aggregate. Authorpresented an attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack.

3. Conclusion

We have discussed a comprehensive survey of data aggregation algorithms in wireless sensor networks. Most of the existing work mainly focuses on the calculating data aggregates and not on security.We discussed the security issues of in network aggregation algorithms to compute aggregates such as predicate Count and Sum. In particular, we showed the falsified sub-aggregate attack launched by a few compromised nodes can inject arbitrary amount of error in the base station's estimate of the aggregate.

We conclude that, there is need of secure data aggregation technique in presence of attack.

References

[1] M. Liu, N. Patwari, and A. Terzis, "Scanning the issue," *Proc. IEEE*, vol. 98, no. 11, pp. 1804–1807, Apr. 2010
[2] T. Ko, J. Hyman, E. Graham, M. Hansen, S. Soatto, and D. Estrin, "Embedded imagers: Detecting, localizing, and recognizing objects and events in natural habitats," *Proc. IEEE*, vol. 98, no. 11, pp. 1934–1946, Nov. 2010
[3] S. Nath, P. B. Gibbons, S. Seshan, and Z. Anderson, "Synopsis diffusion for robust aggregation in sensor networks," in *Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2004, pp. 250–262.
[4] H. Yu, "Secure and highly-available aggregation queries in large-scalesensor networks via set sampling," in *Proc. Int. Conf. Inf. Process.Sensor Netw.*, 2009, pp. 1–12.
[5] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-byhop data aggregation protocol for sensor networks," in *Proc. ACMMOBIHOC*, 2006, pp. 356–367.
[6] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches:Verifiable in-network aggregation," in *Proc. 23rd Int. Conf. Data Eng.(ICDE)*, 2007, pp. 996–1005
[7] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in *Proc. IEEE 20th Int. Conf. DataEng. (ICDE)*, 2004, pp. 449–460.
[8] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1040–1052,J,2012
[9] Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact"Sankardas Roy , Mauro Conti SanjeevSetia, and Sushil Jajodia , IEEE Transactions On Information Forensics And Security, VOL. 9, NO. 4,APRIL2014