International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Straining Attacker's Impact in WSN using Secure Data Aggregation

Akshaya Shah[1], Dr. K. N. Honwadkar[2]

[1, 2]Savitribai Phule's Pune University, Smt.Kashibai Navale College of Engineering, Vadgaon(BK),Pune-41, India

Abstract: ***Wireless sensor networks (WSNs) are significantly found in several purposes, such as volcano and fireplace tracking, metropolitan sensing, and border surveillance. In a large WSN, in-network information aggregation considerably reduces the total amount of connection cost and power consumption. The research community planned a loss-resilient aggregation construction called synopsis diffusion, which uses duplicate-insensitive algorithms on prime of multipath routing schemes to precisely compute aggregates. But, this aggregation construction does not handle the issue of false sub aggregate values led by compromised nodes. That attack might cause large mistakes in the aggregate computed at the beds base station that will be the main node in the aggregation hierarchy. In this paper, we make the synopsis diffusion approach secure against the above mentioned attack presented by compromised nodes. Particularly, we present an algorithm allow the beds base station to solidly compute predicate rely or sum even in the clear presence of this kind of attack. Our attack-resilient computation algorithm computes the true aggregate by filter out the benefits of compromised nodes in the aggregation hierarchy.***

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

1. Introduction

In many real world applications, such as fire monitoring, wild habitat monitoring, military surveillance etc, the Wireless Sensor Networks (WSNs) have been used increasingly in last decade [5], [13], [14], [21]. In WSNs, all the sensor nodes combines together and forms a multi-hop network, in which, the Base Station (BS) has all the control. Generally, a sensor node has issue in phrases of computation capability and power reserves. The BS desires to acquire the sensed information from the network. One popular way is allowing each sensor node to ahead their examining to the BS, probably via different advanced nodes. Ultimately, the BS functions the obtained data. Nevertheless, this approach is excessively costly with regards to transmission overhead. In-network knowledge aggregation [7], [16] may lower the total amount of transmission and thus the power eaten, particularly in big WSNs. The key strategy is to mix incomplete benefits at advanced nodes throughout concept routing. One method [7], [16] is to make a spanning pine seated at the BS, and then accomplish in-network aggregation over the tree. The essential aggregates regarded by the investigation neighborhood contain Depend, and Sum. It's simple to generalize these aggregates to predicate Count and Sum. Furthermore, Normal may be computed from Depend and Sum. We could also simply increase a Sum algorithm to compute Common Change and Mathematical Time of any order. Nevertheless, transmission deficits caused by node and sign problems, which are normal in WSNs, may adversely influence tree-based aggregation approaches. To handle this issue, we are able to utilize multi-path routing techniques for forwarding sub-aggregates [16]. For duplicate-insensitive aggregates such as for example Min and Max, this method supplies a fault-tolerant solution. Unfortunately, for duplicate-sensitive aggregates, such as for example Count and Sum, multi-path routing leads to double-counting of sensor readings. Lately, a few analysts [6], [18] have shown clever algorithms to resolve that double-counting problem. A strong and scalable aggregation platform named synopsis diffusion has been planned for research duplicate-sensitive aggregates. This process runs on the band topology in which a node might have numerous parents in the aggregation hierarchy. Additionally, each sensed value or sub-aggregate is displayed with a duplicate-insensitive bitmap named synopsis. The chance of node bargain presents more problems since all the active in-network aggregation algorithms have number provisions for security. An affected node may try to thwart the aggregation method by launching a few episodes, such as for example eavesdropping, jamming, concept falling, concept manufacturing, and therefore on. That report targets a subclass of those episodes in that your adversary seeks to trigger the BS to uncover a wrong aggregate. By relaying a fake sub-aggregate to the parent node, an affected node might lead a massive amount mistake to the aggregate. For example, throughout the Sum computation algorithm [6], [18], an affected node X may provide an arbitrary quantity of mistake in the last calculate of Sum by falsifying X's possess sub-aggregate. We send to the strike while the falsified sub-aggregate attack. In that report, we project an algorithm to firmly compute aggregates, regardless of the falsified sub-aggregate attack. Specifically, our algorithm includes two phases. The phases are as the following:

(i) In the very first phase, the BS derives a preliminary estimation of the blend centered on little authorization data acquired from the nodes.
(ii) In the 2nd phase, the BS requirements more authorization data from just a part of nodes while that part is set by calculate of the very first phase. At the conclusion of the 2nd phase, the BS may (locally) filter the fake benefits of the sacrificed nodes from the aggregate. The important thing remark which we use to decrease the transmission cost is that to confirm the correctness of the last summary (representing the blend

of the entire network) the BS does not require for authorization communications from most of the nodes.

(iii) It will be observed that while our algorithm is made having WSNs in mind, it's simple to give our alternative for secure aggregation issue running in a big degree spread program like a spread repository program within the Net [12]. Remaining paper is organized as follows: Section II gives the brief discussion about the related research that has been done in this field, whereas, section III concludes our survey.

2. Literature Survey

A system were proposed in [16], using the tree-based aggregation algorithms, called as Tiny Aggregation Service (TAG), in order to compute the aggregates, like Count and Average. Similarly, [7] also proposed alike algorithms to compute aggregates. Besides this, [11] proposed an algorithm to compute an order statistic, using the tree-based aggregation. An aggregation framework was designed in [17], called Synopsis Diffusion, to overcome the problem of communication loss in the tree-based algorithms. This used ring topology to compute Count and sum. Similar algorithm was proposed in [6]. These algorithms made use of the duplicate-insensitive algorithms in order to compute aggregates. For counting distinct elements in multi-sets, this works followed the [15]'s algorithm.

A few secure aggregation algorithms have been proposed accepting that the BS is the main aggregator node in the network [1], [2], [9]. These works did not consider in-network aggregation. Just as of late, the research community has been giving careful consideration to the security issues of various leveled aggregation. The primary assault versatile various leveled information aggregation protocol was outlined in [10]. Notwithstanding, this plan is secure when one and only malevolent node is available. A tree-based check calculation was planned in [3], [8] by which the BS can catch if the last total, Number or Entirety, is adulterated. A couple of check algorithms for registering totals inside the abstract dispersion methodology were outlined in [12] and [19]. As of late, a couple of novel protocols have been proposed for 'secure outsourced aggregation' [17]; nonetheless, as noted by the creators, these algorithms are not intended for WSNs.

In spite of the fact that [8], [3], [12] keep the BS from tolerating a false total, they don't promise the fruitful reckoning of the total in the vicinity of the assault. We further push that our former work [19] displays just a check calculation for the outline dissemination skeleton, which would fall flat in the vicinity of an assault. The confirmation period of SDAP [22] can be lavishly used to figure Include and Total the vicinity of a couple of traded off nodes. Yu [4] proposed a Dos-flexible aggregation calculation for figuring Number and Aggregate, which is focused around a novel tree testing system. In spite of the ill-disposed obstruction, this calculation can create rough guess of the target total. As of late, the same research bunch [18] has distributed one secure aggregation protocol that has the capacity pinpoint and disavow malignant nodes, significantly under Dos assaults. We awhile ago introduced an assault flexible aggregation calculation [13] for the rundown dissemination schema, yet the current assault strong calculation proposed in this paper is more proficient. We contrast our current work and all the earlier assault strong algorithms [4], [20], [22] in Segment V-F.

One method [7], [16] is to make a spanning pine seated at the BS, and then accomplish in-network aggregation over the tree. The essential aggregates regarded by the investigation neighborhood contain Depend, and Sum. It's simple to generalize these aggregates to predicate Count and Sum. Furthermore, Normal may be computed from Depend and Sum. We could also simply increase a Sum algorithm to compute Common Change and Mathematical Time of any order. Nevertheless, transmission deficits caused by node and sign problems, which are normal in WSNs, may adversely influence tree-based aggregation approaches. To handle this issue, we are able to utilize multi-path routing techniques for forwarding sub-aggregates [16].

3. Conclusion

We mentioned the protection problems of in-network aggregation algorithms to compute aggregates such as for example predicate Rely and Sum. Specifically, we revealed the falsified sub-aggregate strike presented with a several sacrificed nodes may insert arbitrary quantity of mistake in the beds base stations calculate of the aggregate. We have shown an attack-resilient computation algorithm which may promise the successful computation of the blend even yet in the clear presence of the attack.

References

[1] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys), 2003.
[2] D. Wagner, "Resilient aggregation in sensor networks," in Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN), 2004.
[3] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. ACM Conf. Comput. Commun. Security (CCS), 2006.
[4] H. Yu, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling," in Proc. Int. Conf. Inf. Process. Sensor Netw., 2009.
[5] James Reserve Microclimate and Video Remote Sensing [Online], 2006.
[6] Available: http://research.cens.ucla.edu/projects/2006/terrestrial/microclimate/defau%lt.htm
[7] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in Proc. IEEE 20th Int. Conf. Data Eng. (ICDE), 2004.
[8] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in Proc. 2nd Int. Workshop Sensor Netw. Protocols Appl., 2003.
[9] K. Frikken and J. A. Dougherty, "An efficient integrity-preserving scheme for hierarchical sensor aggregation,"

in Proc. 1st ACM Conf. Wireless Netw. Security (WiSec), 2008.
[10] L. Buttyan, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in Proc. 2nd IEEE Workshop Sensor Netw. Syst. Pervasive Comput., Mar. 2006.
[11] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security Assurance Ad Hoc Networks, 2003.
[12] M. B. Greenwald and S. Khanna, "Power conservative computation of order-statistics over sensor networks," in Proc. 23th SIGMOD Principles Database Syst. (PODS), 2004, pp. 1–11.
[13] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in Proc. 23rd Int. Conf. Data Eng. (ICDE), 2007.
[14] M. Liu, N. Patwari, and A. Terzis, "Scanning the issue," Proc. IEEE, 2010.
[15] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Environmental wireless sensor networks," Proc. IEEE, 2010.
[16] P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," J. Comput. Syst. Sci., 1985.
[17] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad hoc sensor networks," in Proc. 5th USENIX Symp. Operating Syst. Des. Implement. 2002.
[18] S. Nath, H. Yu, and H. Chan, "Secure outsourced aggregation via oneway chains," in Proc. 35th SIGMOD Int. Conf. Manag. Data, 2009.
[19] 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.
[20] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," IEEE Trans. Inf. Forensics Security, 2012.
[21] S. Roy, S. Setia, and S. Jajodia, "Attack-resilient hierarchical data aggregation in sensor networks," in Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN), 2006.
[22] 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, 2010.
[23] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAsP: A secure hop-by hop data aggregation protocol for sensor networks," in Proc. ACM MOBIHOC, 2006