IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Detection of False Sub Aggregated Data in Wireless Sensor Networks

B. Gowtham[1], A.L. Sreenivasulu[2]

M.Tech, Intell Engineering College, Anantapur[1]

Assistant Professor, Intell Engineering College, Anantapur[2]

Abstract: In wireless sensor networks data aggregation is one of the major issues. To aggregate the data a robust aggregation framework called synopsis diffusion which combines multi path routing algorithm to accurately aggregate the data in case of failures, Nodes are compromising due to the lack of physical protection. Compromised nodes are very vulnerable to attacks in sensor networks. By taking this is an advantage adversary can launch false data over the network. Here a novel light weight verification algorithm performed by the sink node or base station and that can determine any false sub-aggregate data in the aggregated data. It contributes to make synopsis diffusion approach in secure against attacks on compromised node which false sub-aggregate the data. Theoretical analysis and extensive simulations have been conducted and verified.

Index Terms: Base station, data aggregation, synopsis diffusion.

I. INTRODUCTION

Wireless sensor networks (WSNs) are serving in many areas, like, animal and bird monitoring, fire detection especially in forests, and for military people to expect the upcoming threats. When they are working in the above said fields sensor nodes constructs itself a multi hop network with the base station as the central control. Typically, a sensor node has many problems in terms of computation and power management. The best suitable method to collect the sensed information from the lower level nodes is transmitting the data by using intermediate nodes by allowing the intermediate nodes to read the sensed information. This method incurs more expensive in the form of communication overhead like energy consumption.

In WSNs, computing in-network aggregates in-network (i.e., performing the partial aggregation at intermediate nodes) contributing to reduce the amount of communication and energy consumption. Many in network aggregation techniques have been proposed are collected in the literature. The major aggregates were done by considering the Count, and Sum. Furthermore, Average can be computed from Count and Sum. A Sum algorithm can be also extended to compute Standard Deviation and Statistical Moment of any order.

Transmission failures are very common in WSNs due to its nature of deployment. This causes the failure of the tree based in network aggregation. To address this problem, many researchers have been proposed the use of multipath routing techniques to forward the sub aggregates. For aggregates such as Min and Max, which are duplicate-insensitive, this approach provides a fault-tolerant solution. However, Recently, many researchers have proposed intelligent algorithms to solve multipath approach problems such as double counting. A robust and scalable aggregation framework called synopsis diffusion has been proposed to compute duplicate-sensitive aggregates, like Count and Sum. This approach uses a ring topology where a node may have multiple parents in the aggregation hierarchy, and each sensed value or sub aggregate is represented by a duplicate-insensitive bitmap called synopsis.

II LITERATURE SURVEY

Several researchers have studied problems related to data aggregation in WSNs.

A. Non secure Data Aggregation

The tiny aggregation service (TAG) to compute aggregates, such as Count and Sum, using tree-based aggregation algorithms were proposed. Similar algorithms were proposed. Moreover, tree-based aggregation algorithms to compute an order-statistic also have been proposed. To address the communication loss problem in tree-based algorithms the authors designed an aggregation framework called synopsis diffusion to compute Count and Sum, which uses a ring topology. Some Authors in independently proposed very similar algorithms. These works use duplicate-insensitive algorithms for computing aggregates based on counting distinct elements in a multi set.

B. Secure Aggregation Techniques

Several secure aggregation algorithms have been proposed assuming that the base station is the only aggregator node in the network .It is not straightforward to extend these works for verifying in-network aggregation unless we direct each node to send an authentication message to the base station, which is a very expensive solution. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation. We are unable to extend this idea for verifying a synopsis because the synopsis computation is duplicate- insensitive. A verification algorithm for computing Count and Sum within the synopsis diffusion approach was designed

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

III PROPOSED ALGORITHM

VERIFICATION ALGORITHM

Now, we present a verification algorithm to detect the attacks discussed previously. A list of notations used is given in Table I.

Background

Recall that a compromised node launches the falsified sub aggregate attack by inserting one or more false "1"s in its fused synopsis. A straightforward solution to detect the falsified sub aggregate attack is as follows. BS broadcasts an aggregation query message which includes a random value, Seed, associated to the current query. In the subsequent aggregation phase, along with the fused synopsis, each node also sends a MAC towards BS authenticating its sensed value. Node uses Seed and its own ID to compute its MAC. As a result, BS is able to detect any false "1" bits inserted in the final synopsis. In particular, if node contributes to bits in its local synopsis, it generates a MAC, MAC, where is the key that node shares with BS and the format of is Seed . Each node sends a message where might be needed by BS to regenerate the MAC for the verification. We observe that this approach requires MACs to be forwarded to BS, and hence, this approach is not suitable for a sensor network. Our verification algorithm presented as follows also uses similar MACs but reduces the total number of them. Throughout this paper when we say a message contains a MAC , we also mean that the corresponding is attached to . To save space, we do not always explicitly mention this although we take into account the resulting additional byte overhead in the simulation experiments.

Detecting Falsified Sub aggregate Attack:
If we consider that a compromised nodes MAC reaches BS, then we can observer that the node cannot inject a MAC instead of another node without being detected by ensuring MAC. And also we observe that cannot vouch for a false "1" at bit due to the following reasons. It has to be done by appending in the bit list n. Results shows that the BS will detect its falsity after re-executing the Synopsis Generating Algorithm with parameters as and the sensed value. And also mention that in the previous process Bs generates exactly the similar synopsis as by ensuring the same seed. So, the final option is to inject a false "1" successfully is done by modifying.

Detecting Falsified Local Value Attack:
This paper present three cases of this attack and it address only case (iii) i.e., an independent sensors legitimate contribution is bounded as well as a compromised node falsifies the local value outside the bound. This attack will be detected by their verification algorithm presented previously. In section V-A, the node generates a MAC i.e., the key that nodes share with BS and Seed. The attack case (iii) can be possible when BS verifies a MAC which claims to be coming from node. The reported sensed value that it is out of bound will be checks by BS. When runs an attack case (iii) then the check wound not be succeed due to BS detecting the attack.

IV SIMULATION RESULTS

The network topology used a 30 30 grid with 900 sensor nodes, where one node is placed at every grid point and BS is placed at the center of the grid. Every node has communication radius as unit by allowing the shortest eight grid neighbors has to be reach. A unique ID is assigned at every sensor and every sensor accessing a integer uniformly distributed in the range of 0 to 250 units. The method of individual replications is used as simulation methodology. If not mentioned then every simulations were repeated 200 times with a different seed. It calculated the 95% confidence intervals as shown in the reported plot and the confidence intervals are within 5 of the reported value. It considered the simple packet loss model where packets are dropped with a fixed probability; if not motioned then the loss rate is set as 10%.

V. RESULTS AND DISCUSSION

Results shows that, count can be considered as a special case of Sum. It did not study the false positive rate of verification protocol. Integrity checks in node to node communication ensures that if no attack has launched then BS will receive at least one MAC for every of the rightmost "1" s in the final synopsis. A corrupted MAC can reach the BS. Where this problem is not protocol dependent. The verification protocol will complete in one epoch irrespective of the final result, where it did not experiment the latency in this simulation. Firstly it presents the following results for a single synopsis and it extended for multiple synopses. False Negative Rate: It considered the worst case attack scenario. In this the attacker knows the network topology and also the synopsis is calculated by every node. Thus the attacker can calculate the final synopsis when received by the BS. So, the attacker can able to check if it occurs in the final synopsis i.e., "1"s are present to the right of a "0" bit. The aim of the attacker is to maximize the value of Sum as much as possible while remaining undetected. So, the attacker will follow the strategy i.e., if occurs then it changes all "0"s at positions to "1"s otherwise it does nothing. The attack would be attack when the attacker modifies a bit after the bit, thus the protocol verifies the MACs of the rightmost "1"s. While the attacker knows that no bit to the left will be verified. For every "0" the attacker will change it to "1". By considering this worst case attack scenario, that an attack will not detected every time an event occurs. In this simulation, it experimentally evaluated that the probability for this event has to be occur. The verification protocol is simulated at different values of network size i.e., 20 20, 30 30, 40 40, 50 50 and 60 60 grid size and 4, 5, and 6. It simulated the verification protocol times for every combination of these parameters.

VI. CONCLUSION

This paper discussed the security issues of in network aggregation algorithm to calculate aggregates like predicate Count and Sum. And also it discussed how a compromised node can corrupt the aggregate estimate of the base station by focusing on the ring-based hierarchical

DOI 10.17148/IJARCCE.2015.41187

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

aggregation algorithms. This problem is addressed by presenting a lightweight verification algorithm which would enable the BS to check whether the calculated aggregate was valid. For future work, it designs an efficient attack-resilient computation algorithm. The successful computation of the aggregate even an attack has been presence by using this algorithm.

REFERENCES

1. Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia" Secure Data Aggregation in "wireless Sensor Networks" in Ieee Transactions On Information Forensics And Security, Vol. 7, No. 3, June 2012
2. J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in Proc. 2nd Int. Workshop Sensor Network Protocols Applications, 2003.
3. J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in Proc. IEEE Int. Conf. Data Engineering (ICDE), 2004.
4. S. Nath, P. B. Gibbons, S. Seshan, and Z. Anderson, "Synopsis diffusion for robust aggregation in sensor networks," in Proc. 2nd Int. Conf. Embedded Networked Sensor Systems (SenSys), 2004.
5. M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in Proc. 23rd Int. Conf. Data Engineering (ICDE), 2007.
6. M. B. Greenwald and S. Khanna, "Power-conservative computation of order-statistics over sensor networks," Proc. 23th SIGMOD Principles of Database Systems (PODS), 2004.
7. P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," J. Computer Syst. Sci., vol. 31, no. 2, pp. 182–209, 1985.

DOI 10.17148/IJARCCE.2015.41187