International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 3 –SEPTEMBER 2014.

Synopsis Diffusion Approach Secure Data Aggregation by using Light Weight Verification for Monitoring Sensor Networks

V. Sreekalyani [*1], and M.Venkatesh Naik [#2]

[*] *Student, Dept of CSE, CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[#] *Asst Professor, Dept of CSE, CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[1]srikalyani.15.jntucea@gmail.com

[2]venkateshnaikm0@gmail.com

***Abstract*— Aggregators' can be untrusted or compromised. Hence, in WSN's a sensing service should be able to verify the correctness of aggregation results. A diverse set of aggregate functions (Count, Sum, Max, Min, etc), can have multiple hierarchically organized aggregators; can deterministically detect any malicious aggregation behaviour without communication with sensors. In-network data aggregation, a primitive for performing queries on sensor network data reduces the total message complexity of aggregate sensor queries. Inspite of message losses that result from transmission failures and message losses a robust aggregation framework called "synopsis diffusion" combines multipath routing schemes along with duplicate-insensitive algorithms to accurately compute aggregates.**

In this paper, the synopsis diffusion approach secures against attacks in which compromised nodes contribute false sub aggregate values. Using the verification protocol the base station determines whether the computed aggregate includes any false contribution.

Keywords: Verification protocol, in-network aggregation, synopsis diffusion, false sub aggregate attack.

I. INTRODUCTION

The secure in-aggregation protocols has a verification phase where the query result is broadcasted/disseminated to all sensors, so that every sensor has the opportunity to raise an alarm if it disagrees with the query result in case of a compromised node. In large scale WSNs, in-network aggregates, combines the partial results at intermediate nodes during message routing thereby significantly reducing the amount of communication overhead and hence the energy consumed. The significant aggregates include Count and Sum whereas the sub aggregates include the Max and Min. For multipath routing, aggregates Count and Sum, results in double-counting of sensor readings. Hence, robust and scalable aggregation framework called synopsis diffusion has been proposed to calculate Count and Sum. Synopsis diffusion approach uses ring topology in which a node can have multiple parents in the aggregation hierarchy, and each sensed value or sub aggregate is represented by a duplicate-insensitive bitmap called synopsis. We consider falsified sub aggregate attack, in which a compromised node relays a false sub aggregate to the parent node with the aim of injecting error to the final value of the aggregate computed at the base station.

The proposed verification protocol describes a very light overhead compared to all the existing attack resilient solutions. The verification algorithm proposed verifies the correctness of the computed aggregate at the base station. Also, the proposed protocol minimizes the communication overhead as the base station does not require receiving authentication messages from all of the nodes.

II. EXISTING SYSTEM

The existing in-network aggregation [2] can deliver real-time, efficient results but is hosted by untrusted aggregation infrastructure. A portal instead of performing data collection and query processing, it delegates these tasks to a third party called aggregator, provides aggregation services. Outsourced aggregation services have multiple benefits such as periodically reporting the data, collecting data to a centralized portal which incurs overhead on the network. Also outsourced aggregation faces security challenges such as untrusted, compromised, malicious aggregators.

The existing one-way-chain based protocols [4] such as uniform samples; Top K-Readings, top K-groups, etc are free from false positives and false negatives.

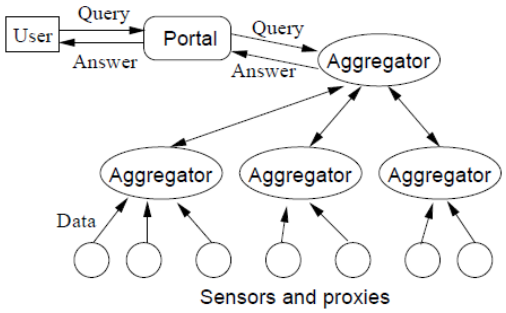

Figure 1: Model of secure outsourced aggregation.

Proof-sketch aggregation [3] can is based on the push-based data collection model, also supports Count-related aggregates.

Most of the aggregation algorithms assume that all intermediate nodes are trusted. One of the existing algorithms Hu and Evans [5] assumes that a single node is malicious. The other aggregation approach Secure Information Aggregation (SIA), provides a statistical security property under the assumption of a single-aggregator model. This form of aggregation reduces communications only on the link between the aggregator and the base station, and is not scalable to large multihop sensor deployments. Another aggregation-verification scheme for the single-aggregator model uses a threshold signature scheme which ensures that at least t of the nodes agrees with the aggregation result.

Tree-based aggregation [1] approaches are not resilient to communication losses resulting from node and transmission failures. To overcome this, multipath routing techniques for forwarding sub-aggregates have been proposed. Duplicate-sensitive aggregates, such as Count and Sum, multipath routing leads to double-counting of sensor readings. A robust and scalable aggregation framework called synopsis diffusion has been proposed for computing duplicate-sensitive aggregates. Although, the existing verification protocols prevent the base station from accepting a false aggregate, they do not guarantee the successful computation of the aggregate in the presence of the attack. Attack-resilient computation algorithms empower the base station to filter out the false contributions of the compromised nodes from the aggregate. A compromised node is capable of launching several attacks such as eaves dropping, jamming, message dropping, message fabrication and so on with the aim of injecting error to the final value of the aggregate computed at the base station.

III. PROPOSED SYSTEM

In the proposed implementation, we design a Verification algorithm to compute aggregates, such as Count and Sum, and to enable the base station to verify if the computed aggregate is valid. The major objective is to minimize the communication overhead involved and verify for the correctness of the aggregate of the whole network. Also, this secure aggregation can be supported for query processing in a large scale distributed database system over the Internet. The synopsis Diffusion uses a ring topology; during the query distribution phase, nodes form a set of rings around the base station (BS) based on their distance in terms of hops from BS.

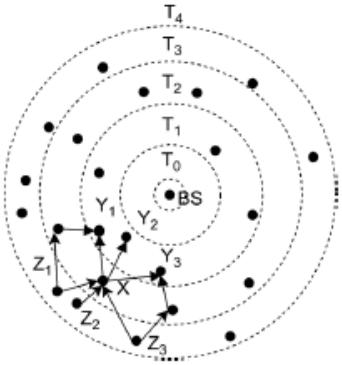

Fig 2: Synopsis diffusion over a ring topology

In this work, we assume a centralized base station that with the sensor nodes forming a multihop network. To authenticate a message to BS, a node X sends a Message Authentication Code (MAC) generated using the key K_X.

Assume that in a given range of WSN's a compromised node launches the falsified sub-aggregate attack by inserting one or more *false* "1"*s* in its fused synopsis. This falsified sub-aggregate attack can be detected 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 $B^{X,}$ each node *X* also sends a MAC towards the base station. 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. A MAC sends a message along with the local synopsis. L'. In the implementation, the total numbers of MAC's are reduced.

BS verifies the final synopsis if it receives one valid MAC for each "1" bit in the synopsis. The advantage of this approach is that BS does not need require to receive authentication messages from all of the nodes which contribute to bit i. reduces the communication overhead per node. By this, the communication overhead can be reduced as each node forwards one MAC each for at most bits in the synopsis, where k is a small constant i.e., authenticates the rightmost "1" bits in the final synopsis. Proportionally, the higher the value of k, the greater is the probability that the algorithm can detect a false "1" bit in the final synopsis.

The proposed algorithm can be implemented in two phases:

- *Query Dissemination phase* - BS broadcasts the name of the aggregate to compute, a random number Seed and the chosen value of "test length", *k.*

$$BS \rightarrow \rightarrow * : \langle F_{\text{agg}}, \text{Seed}, k \rangle.$$

- *Aggregation phase* – aggregation phase of the original synopsis diffusion protocol sent along with some authentication messages.

When a node X broadcasts $\hat{B^X}$ to its parents, for each of the rightmost k "1"s in $\hat{B^X}$ it also forwards one MAC.[2] The corresponding message is as follows:

$$X \rightarrow * : \langle \hat{B^X}, \mathfrak{M}^X \rangle$$

where $\mathfrak{M}^X$ represents a set of k MACs, $\{M_{I^X}, M_{I^X}, \ldots, M_{I^X}\}$ with I_i^X denoting the index of the jth rightmost "1" bit in B^X.

X randomly selects the K MACs from the pool of MACs received from its child nodes or generated by itself.

The pseudo code for Verifiable aggregation algorithm is a s follows:

Algorithm 1: VerifiableAggregation(X, Q^X, k)

begin

receive $\{\langle \hat{B^{X_1}}, \mathfrak{M}^{X_1} \rangle, \langle \hat{B^{X_2}}, \mathfrak{M}^{X_2} \rangle, \ldots, \langle \hat{B^{X_d}}, \mathfrak{M}^{X_d} \rangle\}$ from d child nodes;

$\hat{B^X} = \hat{Q^X} \| \hat{B^{X_1}} \| \hat{B^{X_2}} \| \ldots \| \hat{B^{X_d}}$; /* aggregate received synopses with local one */

I_j^X = the index of the jth rightmost "1" bit in $\hat{B^X}$, $for\ 1 \leq j \leq k'$, where k' is the largest such integer not higher than k; /* $\hat{B^X}$ may have fewer than k "1" bits where $k' < k$. */

generate one MAC for bit I_j^X $in\ \hat{Q^X}$, for $1 \leq j \leq k'$;

construct the union $\mathfrak{M}$ of the received MACs and the self-generated ones;

randomly select $\mathfrak{M}^X$ = $\{M_{I_1^X}, M_{I_2^X}, \ldots, M_{I_{k'}^X}\}$ from $\mathfrak{M}$;

broadcast$\langle \hat{B^X}, \mathfrak{M}^X \rangle$ to parents;

end

If the algorithm receives one valid MAC for each of the rightmost "1"s present in $\hat{B}$, the verification succeeds and is accepted. Otherwise, the verification fails.

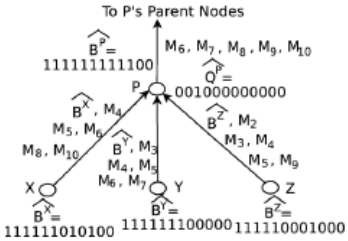

Fig 3: Aggregation phase of verification algorithm

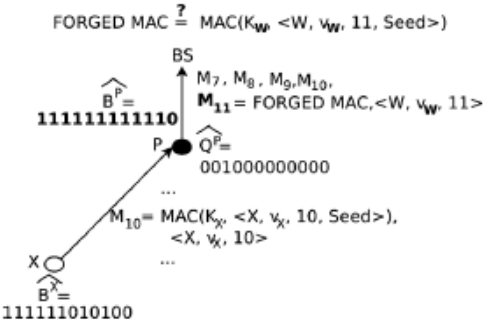

Fig 4: Example of MAC forging during aggregation phase

In case of device failure or due to some error, if the incorrect MAC is generated, the MAC computation algorithm produces an incorrect result with probability *P*. When this incorrect MAC reaches the base station, it will not pass through the verification step, hence ends with a "*failure*".

IV. CONCLUSION

The implemented verification protocol prevents the base station from accepting a false aggregate; also guarantees the successful computation of the aggregate in the presence of the attack. The implemented verification protocol has a very light overhead involved compared to the existing attack resilient solutions. In our protocol each node forwards at most *K* MACs for each synopsis. Our algorithm produces an approximate estimate of the aggregate, where the amount of error is reduced if the number of synopses used, *m* is increased.

REFERENCES

[1] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia,Secure Data Aggregation in Wireless Sensor Networks, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 3, JUNE 2012.

[2] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. ACM Conf. Computer and Communications Security (CCS), 2006.

[3] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in Proc. 23rd Int. Conf. Data Engineering (ICDE), 2007.
[4] S. Nath, H. Yu, and H. Chan, "Secure outsourced aggregation via one-way chains," in Proc. 35th SIGMOD Int. Conf. Management of Data, 2009.
[5] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security and Assurance in Ad hoc Networks, 2003.