Comparison of the effect of different Discriminant Functions on the convergence rate of IF Algorithm for secure data aggregation technique in presence of collusion attacks

Supriya
Mtech Student, Electronics and Communication Engineering,
Punjabi University, Patiala, India

Dr. Manjeet Singh Patterh
Professor, Electronics and Communication Engineering,
Punjabi University, Patiala, India

Abstract- Wireless Sensor Networks are subjected to hostile and malicious environments, so they are vulnerable to collusion attacks leading to compromised nodes and hence false data injection. Hence there is a need for secure data aggregation techniques. Iterative Filtering Algorithms provide secure data aggregation by providing trustworthiness values to the nodes in the form of weight factors. Role of discriminant function, for calculating weights, is very important in IF algorithm. Different discriminant functions could provide different converging rates leading to different efficiencies. In this paper, we compare the effect of different discriminant functions on the convergence rate of IF Algorithm.

Keywords – Wireless Sensor Networks, Collusion attacks, Data aggregation, Iterative Filtering Algorithms, Discriminant Function, convergence rate

I. INTRODUCTION

Wireless Sensor Networks (WSN) are geographically distributed sensors using which physical or environmental factors, such as temperature, sound, pressure, force, intensity etc. are monitored and then cooperatively passed on through the network to a main location. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one or many sensors. The purpose of data aggregation algorithms is to accumulate and aggregate data in a constructive way so that system lifetime is improved.

A. Overview of Data Aggregation

Data aggregation collects the most critical data from the sensors and makes it available to the sink in an energy efficient manner with minimum data latency. Data aggregation is a technique widely used in Wireless sensor networks. Data coming from multiple sensor nodes is aggregated and passed on to the aggregator node. Data aggregation is a process of aggregating the sensor data using aggregation procedures.

B. Need for Data Aggregation

A base station along with a number of small wireless sensor nodes form what is called a wireless sensor network. Infinite amount of energy is presumed to be associated with the base station, making it secure while only a limited energy is presumed to be associated with the sensor nodes making them insecure. The sensor nodes collect the information about various physical parameters by surveying a topographical area. The base station then receives this monitored and audited information via hop by hop transmissions. A suitable cumulative function is then applied on the received data to aggregate the information at intermediary sensor nodes to preserve energy. This helps in minimizing the network traffic and hence energy consumption is also minimized. Developing energy-efficient data aggregation algorithms is critical so as to enhance network lifetime. The aggregation algorithms however increase the

already existing security challenges for wireless sensor networks and require new security techniques. Providing security to aggregate data in wireless sensor networks is known as secure data aggregation in WSN.

C. Collusion Attacks

Collusion attacks refer to the exploitation of WSNs by attackers by injecting false data through a number of biased nodes. This sophisticated attack is possible when the attackers having a high level of prior knowledge about the cumulation algorithm and its parameters. Thus the main target of malicious attackers is aggregation algorithms of trust and reputation systems.

D. Need for Secure Data Aggregation Techniques

Because of a lack of an unlimited availability of energy and power, accumulation of data from multiple sensor nodes is commonly achieved by simple methods such as averaging. Since wireless sensor networks are set up in hostile, malicious and unprotected environments, they are highly vulnerable to the attacks induced by the biased nodes. Thus, assuring trustworthiness of data and reputation of sensor nodes is imperative for WSN. So the aggregation methods such as averaging, being obnoxious to such attacks, are unreliable. Hence Secure Data-Aggregation Techniques are required to prevent corruption of data by malicious attackers [1].

E. Different Techniques used for Data Aggregation

1) Data Aggregation and Dilution by Modulus Addressing in Wireless Sensor Networks.

In this method, data aggregation by the nodes was done in accordance with the rules given in an SQL Statement. This method reduced the network traffic by 60% on an average [4].

2) Distributed Data Compression and Hierarchical Aggregation

In this method, the energy consumption is minimized by defining a distributed compression problem with constraints related to energy costs for a single sink and then a hierarchical model consisting of multiple sinks, compressors, and sensors is proposed and optimized [5].

3) Clustered Aggregation Technique

This technique reduced the network traffic by reducing the number of transmissions. Here, spatial correlation of sensor data was employed to provide approximate results to queries relating to aggregation. Since the nearby nodes usually report almost similar values so a cluster of such nodes was formed. Only one value per cluster was relayed up the aggregation tree [6].

4) Structure Free Data Aggregation

Efficient data aggregation was achieved without the maintenance of a structure [7].

F. Different Techniques used for Trust and Reputation Management

1) An Iterative Algorithm for Trust and reputation management

In this algorithm, an iterative procedure is used to collect reports and provide reputation values to service providers and also to rate the consumers. This procedure involves the iterative decoding of the parity-check codes [8].

2) Game-Theoretic Approach

In this approach, data trustworthiness is assured by using a protection strategy to prevent sensor nodes from attacks. The difference between the accepted value and the original sensed value is kept below a certain threshold by protecting sufficient number of sensor nodes [9].

3) Integration of false data detection with data aggregation

In this technique, Data aggregation and authentication protocol, called DAA, is used. Here, the sensor nodes, apart from the aggregator nodes, also perform data aggregation and hence authenticate the data. Thus, these nodes verify the aggregated data rather than the plain data [10].

G. Iterative Filtering

IF Algorithms serve the purpose by providing trustworthiness values to the nodes in the form of weight factors. IF Algorihms are an optimum and excellent option for WSN's because they use iterative procedure to solve both the problems of data aggregation and trustworthiness assessment[11]. The trustworthiness rating of a sensor is obtained as a measure of the deviation of the readings of a sensor from the estimated values obtained in preceding iteration by some type of accumulation. Less trustworthiness and consequently a smaller weight is assigned to the sensors whose readings notably differ from such estimate and hence their contribution to the overall aggregate value decreases automatically, thus ensuring accuracy and robustness in the final reported value.

H. Discriminant Function

In IF Algorithms, the discriminant function is of great importance as it is used to calculate weights and as such the selection of a proper discriminant function is very important so as to increase robustness, convergence rate and hence the efficiency of IF Algorithm. A number of Discriminant functions have been proposed. These are-

- Reciprocal: $g(d) = d^{-k}$
- Laureti : $g(d) = d^{-0.5}$
- Exponential: $g(d)= e^{-d}$
- Affine: $g(d)=1-k_l d$ where $k_l > 0$ is chosen so that $g(\max_i \{ d_i^{(l)}\}) = 0$

In this paper, we compare these four discriminant functions in terms of convergence rate. Convergence rate is calculated in terms of number of rounds required to stabilize the reputation vector r. As and when, the reputation vector r stabilizes , the calculated weights are the final weights.

I. Collusion Attack Scenario

In most of the IF algorithms, the initial weights to the sensors are assigned on the basis of simple assumptions. We consider a threat model wherein an attacker lures the aggregation algorithm through prudent selection of reported data values. Suppose ten sensors report values of temperature which are aggregated using IF Algorithm. We will be comparing the effect of different discriminant functions being used in IF Algorithm. We consider an attack scenario where two sensor nodes are biased by a malicious attacker and their readings are modified such that the average of all readings is now deviated towards a lower value. So the two sensor nodes on account of reporting a lower value, are allocated lower weights by the IF Algorithm, because their values are very different from the values of other sensors . Hence on account of lower weights assigned to these nodes, their overall contribution decreases. Thus the algorithm is robust against false data injection.

II. IMPLEMENTATION OF IF ALGORITHM WITH DIFFERENT DISCRIMINANT FUNCTIONS

Table 1 shows the temperature values reported by 10 sensors. These values are aggregated using Iterative Filtering Algorithm.

A. USING RECIPROCAL DISCRIMINANT FUNCTION i.e. g(d)=1/d

In Table 2, IF Algorithm was implemented using Reciprocal Discriminant Function and it was observed that with reciprocal discriminant function i.e. g(d)=1/d, the algorithm converges in 8 rounds.

B. USING LAURETI DISCRIMINANT FUNCTION i.e. $g(d)=d^{-0.5}$

In Table 3, Laureti Discriminant Function was used to implement IF Algorithm and it was observed that with thisdiscriminant function i.e. $g(d)=d^{-0.5}$,the algorithm again converges in 8 rounds.

C. USING EXPONENTIAL DISCRIMINANT FUNCTION i.e. $g(d)=e^{-d}$

In Table 4, Exponential Discriminant Function was used to implement IF Algorithm and it was observed that the algorithm converges in 10 rounds.

D. USING AFFINE DISCRIMINANT FUNCTION i.e. $g(d)= 1-k_l d$

Table 5 shows that IF Algorithm converges in just 2 rounds by using Affine Discriminant Function.

III.CONCLUSION

In this paper, an attack plot was considered, wherein the attacker reforms the values of two sensor nodes such that the aggregation of all sensor readings results in a biased lower value. Then IF Algorithm was implemented on these sensor readings using different discriminant functions and the effects of different discriminant functions on the convergence rate of IF Algorithm were studied and it was concluded that the fastest convergence rate is achieved by using Affine Discriminant Function.

REFERENCES

[1] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions on dependable and secure computing, Vol. 12, No. 1, January/February 2015.

[2] Doddappa Kandakur, Ashwini BP, "Survey: Robust Data Aggregation Techniques in Wireless Sensor Networks", International Journal of Engineering and Techniques - Volume 1 Issue 4, July-Aug 2015.

[3] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha, "Credibility Propagation for Robust Data Aggregation in WSNs", Technical Report UNSW-CSE-TR-201414 May 2014.

[4] Erdal Cayirci, "Data Aggregation and Dilution by Modulus Addressing in Wireless Sensor Networks", IEEE Communications Letters, Vol. 7, No. 8, August 2003.

[5] Seung Jun Baek, Gustavo de Veciana,and Xun Su, "Minimizing Energy Consumption in Large-Scale Sensor Networks Through Distributed Data Compression and Hierarchical Aggregation", IEEE Journal on selected areas in Communications, Vol. 22, No. 6, August 2004.

[6] SunHee Yoon and Cyrus Shahabi, "Exploiting Spatial Correlation Towards an Energy Efficient Clustered Aggregation Technique (CAG)" .

[7] Kai-Wei Fan, Sha Liu, and Prasun Sinha, "Structure-Free Data Aggregation in Sensor Networks", IEEE Transactions on mobile computing, Vol. 6, No. 8, August 2007.

[8] Erman Ayday, Hanseung Lee and Faramarz Fekri, "An Iterative Algorithm for Trust and Reputation Management", ISIT 2009, Seoul, Korea, June 28 - July 3, 2009.

[9] Hyo-Sang Lim , Gabriel Ghinita, Elisa Bertino , Murat Kantarcioglu, "A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks", 2012 IEEE 28th International Conference on Data Engineering.

[10] Suat Ozdemir and Hasan Cam, "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010.

[11] C. de Kerchove and P. Van Dooren, "Iterative filtering in reputation systems," SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

TABLE 1

	Sensor readings										Aggregate Values
instant	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	
t=1	19.7336	19.6160	19.7728	20.2040	20.4196	19.4494	20.1354	19.0084	13.2001	13.5609	

TABLE 2

round	Sensor weights										t=1
1	1	1	1	1	1	1	1	1	1	1	18.5100
2	0.6679	0.8175	0.6271	0.3485	0.2742	1.1332	0.3785	4.0260	0.0355	0.0408	19.3392
3	6.4291	13.0528	5.3192	1.3372	0.8567	82.3622	1.5775	9.1377	0.0265	0.0300	19.4850
4	16.1762	58.2409	12.0702	1.9342	1.1448	790.5790	2.3637	4.4031	0.0253	0.0285	19.4721
5	14.6	48.3	11.1	1.9	1.1	1941.9	2.3	4.7	0.0000	0.0000	19.4580
6	13	40	10	2	1	13482	2	5	0.0000	0.0000	19.4505
7	10	40	10	0.0000	0.0000	809110	0.0000	0.0001	0.0000	0.0000	19.4494
8	0.0000	0.0000	0.0000	0.0000	0.0000	6.5142E+9	0.0000	0.0000	0.0000	0.0000	19.4494

TABLE 3

round	**Sensor weights**										**t=1**
1	1	1	1	1	1	1	1	1	1	1	18.5100
2	0.8173	0.9042	0.7919	0.5903	0.5237	1.0645	0.6152	2.0065	0.1883	0.2021	19.2888
3	2.2484	3.0566	2.0663	1.0927	0.8844	6.2280	1.1812	3.5659	0.1642	0.1746	19.4824
4	3.9813	7.4864	3.4438	1.3859	1.0670	30.2800	1.5315	2.1096	0.1592	0.1689	19.5212
5	4.7075	10.5457	3.9742	1.4645	1.1131	13.9325	1.6281	1.9502	0.1582	0.1678	19.5716
6	6.1739	22.5360	4.9708	1.5813	1.1793	8.1815	1.7738	1.7755	0.1569	0.1664	19.6129
7	8.2828	319.2408	6.2526	1.6917	1.2396	6.1174	1.9138	1.6543	0.1559	0.1652	19.6186
8	8.6984	379.3614	6.4866	1.7083	1.2485	5.9089	1.9351	1.6387	0.1558	0.1651	19.6186

TABLE 4

round	Sensor weights										t=1
1	1	1	1	1	1	1	1	1	1	1	18.5100
2	0.2238	0.2943	0.2030	0.0567	0.0261	0.4138	0.0712	0.7801	0.0000	0.0000	19.4258
3	0.9096	0.9645	0.8866	0.5458	0.3725	0.9994	0.6044	0.8401	0.0000	0.0000	19.6982
4	0.9987	0.9933	0.9944	0.7743	0.5943	0.9400	0.8260	0.6214	0.0000	0.0000	19.7793
5	0.9979	0.9737	1.0000	0.8350	0.6637	0.8969	0.8809	0.5520	0.0000	0.0000	19.8029
6	0.9952	0.9657	0.9991	0.8514	0.6837	0.8825	0.8954	0.5319	0.0000	0.0000	19.8098
7	0.9942	0.9631	0.9986	0.8561	0.6894	0.8782	0.8994	0.5261	0.0000	0.0000	19.8117
8	0.9939	0.9624	0.9985	0.8574	0.6911	0.8870	0.9005	0.5245	0.0000	0.0000	19.8123
9	0.9938	0.9622	0.9984	0.8578	0.6916	0.8766	0.9009	0.5240	0.0000	0.0000	19.8125
10	0.9938	0.9621	0.9984	0.8579	0.6917	0.8765	0.9010	0.5239	0.0000	0.0000	19.8125

TABLE 5

round	Sensor weights										t=1
1	1	1	1	1	1	1	1	1	1	1	18.5100
2	0.9645	0.9645	0.9645	0.9645	0.9645	0.9645	0.9645	0.9645	0.9645	0.9645	18.5100