ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Review on Integrating Data Transmission Technique in Sensor Wireless Network Using Data Aggregation Method

Manisha Thakur, Prof. Roshani Talmale

M. Tech Student, Dept. of CSE, RTMNU, Nagpur, India

Professor, Dept. of CSE, RTMNU, Nagpur, India

ABSTRACT:Wireless Sensor Networks (WSNs) enables the collection of physical measurements over a large geographic area. Wireless sensor network are used to transmit the information from one sensor network to multiple sensor network. In wireless sensor network there are multiple data collect from different node. All these details are aggregate by using aggregate node. The aggregation node forward only one aggregation value to the base station In this paper we demonstrate several existing system by using interactive filtering algorithm. Interactive filtering technique providing not only the facilities against the collusion attack but also more accurate and faster converging. Iterative filtering algorithms are the most effective solution for such purpose. These algorithms simultaneously aggregate data from multiple sources and provide trust estimation of these sources, usually in a form of corresponding weight factors assigned to data provided by each source

KEYWORDS: WSN, COLLUSION ATTACKS, DATA AGGREGATION.

I. INTRODUCTION

Wireless sensor network and actor network are spatially distributed autonomous sensor to monitor and also transmit the data through the network to main location. sensor network are collection of sensor node which send sensed data to base station. Data aggregation using simple averaging scheme is more exposed to faults and malicious attacks. Their limitations causes sensor network to use simple algorithm called averaging for data aggregation. Data aggregation using simple averaging scheme is more exposed to faults and malicious attacks. An attacker can capture and compromise sensor nodes and launch a variety of attacks by controlling compromised nodes.

This cannot be prevented by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. Trust and reputation systems have an important role in wireless sensor networks. Data aggregation has emerged as basic approach in wireless sensor network in order to reduce the number of transmission of sensor node. Data aggregation is very simple method of merging the data from different node such as averaging. Typically, an aggregate value is computed at the data sink by applying the conforming combined function, e.g., MAX, COUNT, AVERAGE or MEDIAN to the collected data. In particular, a robust and scalable aggregation framework called Synopsis Diffusion has been future for calculating aggregates such as COUNT, SUM, UNIFORM SAMPLE and MOST FREQUENT ITEMS. The iterative technology are used to describe the situation in which a sequence of instruction is executed multiple times. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable

In future, WSNs need more sophisticated algorithms for data aggregation. Such algorithm should have two features as a major task. In the presence of stochastic errors such algorithm should produce accurate data which is match to the original data. Thus for example, if the noise present in each sensor is a Gaussian independently distributed noise with a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

zero mean, then the estimate produced by any technique used, should have a variance close to Cramer Rao Lower Bound (CRLB)

II. RELATED WORK

. In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce.Authors in [1], combines the aggregation function with the a reputation system in order to enhance the network life time and the accuracy of the aggregated data. By monitoring neighbourhood's activities, each sensor node evaluates the behaviour of its cell members in order to filter out the incon-sistent data in the presence of multiple compromised nodes.Authors in[2], describe data trustworthiness by extend-ing Josang's trust model. Based on the multilayer aggregation architecture of network, they design a trust-based framework for data aggregation with fault describe with a goal to reduce the erroneous data and provide correct trust-worthiness for aggregated results.

Authors in [3], challenging problem of assuring trustworthiness of sensor data in the presence of malicious adversaries. They developed a game theoretic defence strategy to protect sensor nodes from attacks and to guarantee a high level of trustworthiness for sensed data. The objective of the defence strategy is to ensure that sufficient sensor nodes are protected in each attack/defence round.Authors in [4], the past literature it was found that these algorithms exhibit better robustness compared to the simple averaging techniques; however, the past research did not take into account more sophisticated collusion attack scenarios. If the attackers have a high level of knowledge about the aggregation algorithm and its parameters, they can conduct sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes.Authors in [5],They designed a symmetric key homomorphic encryption scheme which is additively homomorphic to conduct the aggregation operations on the ciphertexts. Their scheme uses modular addition, so the scheme is good for CPU-bounded devices such as sensor nodes in WSN. Their scheme can also efficiently compute various statistical values such as mean, variance and deviation. However, since they used the symmetric homomorphic encryption, their aggregator can decrypt each individual sensor's data, and they assumed the trusted aggregator in their model.Authors in [9],state that a sensor node should not leak its readings to neighboring nodes. Moreover, in many applications, sensor nodes trans-mit highly sensitive data, e.g., secret keys; and therefore it is extremely important to build secure channels among sensor nodes. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Fur-thermore, routing information must also remain confiden-tial in certain cases as malicious nodes can use this information to degrade the network's performance. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality

III. PROPOSEDALGORITHM

This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced.In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one of the attackers. In this paper, we propose a solution for vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors.Identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms.A novel method for estimation of sensors' errors which is effective in a wide range of sensor faults and not susceptible to the described attack. Design of an efficient and robust aggregation method inspired by the MLE, which utilises an estimate of the noise parameters obtained using contribution above. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions We provide a thorough empirical evaluation of effectiveness and efficiency of our proposed aggregation method. The results show that our method provides both higher accuracy and better collusion resistance than the existing methods.To the best of our knowledge, no existing work addresses on false data injection for a number of simple attack scenarios, in the case of a collusion attack by compromised nodes in a manner which employs high level knowledge about data aggregation algorithm used.Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each sourceTo address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.In wireless sensor network, multiples nodes are connected to base station through the cluster. The cluster head in one cluster receive the data from different node and merge that data using aggregation techniques and send to the base station. Administrator receive that file and provide appropriate solution on that

IV. CONCLUSION

In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methodswhich makes the algorithms not only collusion robust, but also more accurate and faster converging.The Iterative Filtering algorithm in secure data aggregation is used to resolve a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection, secure data aggregation, cluster head election, outlier detection.

REFERENCES

1. S. Ozdemir and H. Cam, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks", *IEEE/ACM Transaction on Networking*, Jun. 2010.
2. Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks" , *IEEE Transaction on Dependable & Secure Computing* ,Nov. 2012.
3. H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A game theoretic approach for high-assurance of data trustworthiness in sensor networks " , *IEEE International Conference on Data Engineering (ICDE)*, April 2012..
4. Mohsen Rezvani, Student Member, IEEE, Aleksandar Ignjatovic, Elisa Bertino, Fellow, IEEE, and Sanjay Jha, Senior Member, IEEE, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE*Transaction on Dependable & Secure Computing*, January/February 2015.
5. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in
6. IEEE 2005
7. S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput.Netw.,
8. vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
   L. Wasserman, All of Statistics : A Concise Course in Statistical Inference New York, NY, USA: Springer,.
9. M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," School Comput. Sci. and Eng., Univ. New South Wales, Kensington, NSW, Australia, Tech. Rep. UNSW-CSE-TR-Jul2013
10. K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys,vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009

BIOGRAPHY

Manisha M.Thakur is a 3rd semester m.tech student in the Computer Science and Engineering Department, Tulsiramji gayakwad-Patil College of Engineering and Technology, Wardha Road Nagpur. She is doing her project in under the guidance of **Prof. Roshani Talmale**(department of computer science) in Tulsiramji gayakwad-Patil College of Engineering and Technology.