ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

SECUREROBUST DATA AGGREGATION METHOD FOR WIRELESS SENSOR NETWORK IN THE PRESENCE OF MALICIOUS USER

Uma Angadi*, Dr. G.F Ali Ahammed
* Dept of Computer Science & Engg, VTU PG Centre, Mysuru, Karnataka, INDIA.
Associate Professor, Dept. of Computer Science & Engg, VTU PG Centre, Mysuru, Karnataka, INDIA.

KEYWORDS: Collusion Attacks, Data Aggregation, Iterative Filtering Algorithms, Wireless Sensor Network.

ABSTRACT
Wireless sensor Networks (WSN) consists of sensor nodes these sensor nodes have the capability to sense and communicate. The capabilities of these nodes have certain limitations such as limited computational power, memory and communication resources. These wireless sensor networks can be used in many application such as military, disaster management and security. Due to limited resources it is very essential to curtail the amount of data transmission. One of the important techniques in wireless sensor networks is data aggregation. This algorithm it mainly focuses on enhancing the network lifetime and efficencey by gathering and aggregating data in an energy efficient manner. The purpose of this survey is to present a critical overview of different data aggregating algorithm in wireless sensor network. Also discussed the advantages and limitations of various data aggregating algorithm and compared them. And also discuss the which algorithm is used in data aggregation process to give the security for the data during the transmission .by using Iterative filtering algorithm to secure the data and iterative filtering algorithm hold great promise for such an purposes. In wireless sensor network data aggregation is highly vulnerable to node compromising attacks. This paper focuses on different approaches used for the purpose of secure data aggregation and Proposed work mainly concentrated on attacks on both cluster member as well as aggregator.

INTRODUCTION
Wireless sensor networks are being increasingly deployed in many application areas, however computational power and energy resources are two big challenges for Wireless sensor networks [1]. 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. To protect against this threat, it is important to establish trust levels for sensor nodes and adjust node trustworthiness scores [4][5].

For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN. Such an algorithm should have two features.

- In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. Thus, for example, if the noise present in each sensor is a Gaussian independently distributed noise with zero mean, then the estimate produced by such an algorithm should have a variance close to the Cramer- Rao lower bound (CRLB) [2], i.e, it should be close to the variance of the Maximum Likelihood Estimator(MLE).However such estimation should be achieved without supllying to the algorithm the variances of the sensors,unavailable in practice.
- The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node. The main goal of data aggregation method to gather and aggregate dta in any energy efficient manner so that network lifetime is enhanced.

Trust and reputation system have a significant role in supporting operation of a range of distributed systems from wireless sensor networks and e-commerce infrastructure to social networks,by providing an assement of trustworthiness of participants in such distributed systems.A trustworthiness assement at any given moment represents an aggregate of the behavior of the participants up to that moment and has to robust in the presence of various attacks and malicious users.There are number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system.The main target of the malicious attackers are aggregation algorithms of trust and reputation systems.Iterative Filtering algorithms are an attractive for WSNs because they solve the data aggregation and data trustworthiness assessment using single iterative

procedure.Suchtrustworhniess estimate of each sensor is biased on the distance of the readings of such a sensor from the estimate of the correct values ,obtained in the previous round of iteration by some from of aggregation of the readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round iteration their readings are given a lower weight.If the attackers have a high level of knowledge about the aggregation algorithm and its parameters,,they can conduct the sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes.This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection.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 the attackers.

LITERATURE REVIEW

This literature survey to propose the technique such aggregation is here to attain the data accuracy and also diminish the chance of collusion attacks before storing into the aggregator node.due to limited computational power and energy resources.data aggregation of aggregate the data from multiple sensor node is done at the aggregator node its data is send to the base station. However such aggregation is highly vulnerable to malicious attack. Iterative filtering algorithms hold great promise for such a function. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources frequently in a form of corresponding weight factors assigned to data provided by each source.

B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-rotaru, and H. Rubens, introduced [1] and "**Secure data aggregation in wireless sensor networks**".The proposed scheme is in Wireless sensor network (WSN) refers to a group of spatially dispersed. Collision attack means the group of nodes to access the illegal data. The data collected from individual nodes is aggregated at a base station or host computer. Due to limited computational power and power resources, aggregation of information from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is well-known to be highly vulnerable to node compromising attacks.Iterative filtering algorithms hold great promise for such a function. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources frequently in a form of corresponding weight factors assigned to data provided by each source. Data aggregation process can enhance the robustness and accuracy of information which is obtained by entire network. K. Hoffman, D. Zage, and C. Nita-Rotaru [2] introduced an "**Iterative Trust and Reputation Management Scheme" (ITRM).**The proposed ITRM is a robust mechanism to evaluate the quality of the service. Proposed algorithm can be applied to centralized schemes where a central authority collects the reports and forms the reputations of the service providers as well as report trustworthiness of the consumers. Proposed work is a bipartite graph based motivated by the iterative decoding of low-density parity-check codes. In this paper author compare of ITRM with previous known reputation management techniques which provide better result in terms of both robustness and efficiency.Trust and reputation have been recently suggested as an effective security mechanism for Wireless Sensor Network Although sensor networks are being increasingly deployed in many application domains, assessing trustworthiness of reported data from distributed sensors has remained a challenging issue. Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data becomes a challenging task.

J.-W. Ho, M. Wright, and S. Das[3],introduced, an**"Integrating Data Transmission Technique in Sensor Wireless Network Using Data Aggregation Method"**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. It 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. 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.

H. Liao, G. Cimini, and M. Medo[4],introduced an "**Data Aggregation Techniques Of Wireless Sensor Network Increasing Network Lifetime Using READA"**In wireless sensor networks (WSNs) the basic component is represented by the nodes . The sensor nodes consumes energy during sensing, processing and transmission. Aggregation of data from multiple sensor nodes which is done at the aggregating node is to be

performed by simple method such as averaging. In Wireless sensor network power and energy resources are limited. In this paper the monitoring system and READA technique will be used. The number of sensor nodes can detect simultaneously a single target of interest. Redundant and correlated data are collected. If every nodesends data to the base station, energy will be wasted and thus the network energy will be consume quickly. Redundancy Elimination for Accurate Data Aggregation (READA) uses a grouping and compression mechanism to remove duplicate data in the aggregated set of data to be sent to the base station without largely losing the accuracy of the final aggregated data. In wireless sensor network, security and energy efficiency issues are found.

M. C. Vuran and I. F. Akyildiz[5] introduced "**Spatial correlation-based collaborative medium access control in wireless sensor networks**"this paper shows how the spatial correlation can be exploited on the Medium Access Control (MAC) layer. Due to the spatial correlation between sensors nodes cause to undergo observed events, which may not be necessary for every sensor node to transmit its data. Paper proposed Spatial Correlation-Based Collaborative Medium Access Control in Wireless Sensor Networks which has two components: Event MAC (E-MAC) and Network MAC (N-MAC). E-MAC filters out the correlation in sensor records while N-MAC prioritizes the transmission of route-thru packets. CC-MAC provides high performance in terms packet drop rate, energy and latency. This paper considers only one type of phenomenon sensed by the sensor nodes. The quality of service requirement of various types of sensor information needs to be improved.

PROBLEM STATEMENT

In the prior work there is techniques are proposed to attain the reachable data security while the aggregation but there is not satisfying the data security and integrity or the accuracy of the process while they process with the sensor data after storing into the aggregator. Thus, we cannot rely on cryptographic methods for preventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes.

PROPOSED SYSTEM ARCHITECTURE

The proposed system is mainly to avoid the attacks availability on the each sensor nodes reading. An improvement is made on iterative filtering technique by providing an initial approximation which not only makes the algorithm collusion robust, but also faster converging. Iterative Filtering algorithms are an efficient and reliable option for wireless sensor networks because they solve both problems of data aggregation and data trustworthiness estimation using a single iterative procedure. This algorithm is for robust aggregation along with which different collusion attacks are identified and avoided in the proposed system. These attacks are described by estimating sensor's error and uses MLE for robust aggregation. The trustworthiness of nodes is estimated from their data aggregated from them. The computational cost is also reduced by the proposed method.this can be shown in fig 1.

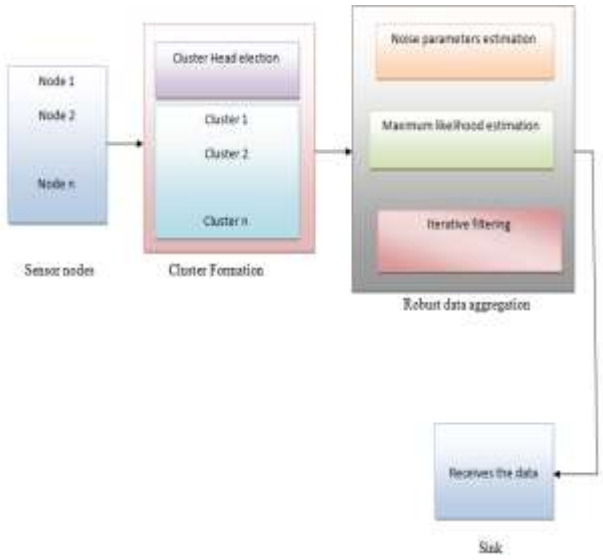

Fig.1. System Architecture For Proposed System.

SCOPE OF THE PAPER

A new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection 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. Although such proposed attack is applicable to a broad range of distributed systems, it is particularly dangerous once launched against WSNs for two reasons. First, trust and reputation systems play critical role in WSNs as a method of resolving 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, etc. Second, sensors which are deployed in hostile and unattended environments are highly susceptible to node compromising attacks. While offering better protection than the simple averaging, our simulation results demonstrate that indeed current IF algorithms are vulnerable to such new attack strategy. A solution for such vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors when the nature of errors is stochastic, such errors essentially represent an approximation of the error parameters of sensor nodes in WSN such as bias and variance. However, such estimates also prove to be robust in cases when the error is not stochastic but due to coordinated malicious activities. Such initial estimation makes IF algorithms robust against described sophisticated collusion attack, and, believe, also more robust under significantly more general circumstances; it is also effective in the presence of a complete failure of some of the sensor nodes. This is in contrast with the traditional non-iterative statistical sample estimation methods which are not robust against false data injection by a number of compromised nodes and which can be severely skewed in the presence of a complete sensor failure.

Robust aggregation technique is effective in terms of robustness against our novel sophisticated attack scenario as well as efficient in terms of the computational cost.

CONCLUSION AND FUTURE WORK

This paper presented an all-inclusive survey of data aggregation algorithms in wireless sensor networks. All of them focus on optimizing important performance measures such as energy consumption, network lifetime, data latency and data accuracy. The main features, the advantages and disadvantages of each data aggregation algorithm are described. In proposed work, secure and robust data aggregation is perform in presence of collusion attacks which are available in wireless sensor network. In proposed work, we consider attacks on both cluster member as well as aggregator.And also A novel collusion attack scenario is considered against the number of prior IF algorithms. An initial approximation of the trustworthiness of sensor nodes is proposed for an improvement of the IF algorithm. Furthermore, this have a novel data collection technique from the sensor reading data in the presence of the collusion attack and it prevents from the sensor faults. The whole performance will be evaluated in terms of time consumption. It makes the IF algorithms not only collusion robust but also gives more accurate and faster converging. In the future we will extend the proposed robust aggregation for protecting the aggregator node from the collusion attack and also plan to improve the data security while transmitting the data from the sensor node to the aggregator node.

REFERENCES

1. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-rotaru, and H. Rubens, “Secure data aggregation in wireless sensor networks,” Dept. Comput. Sci., Johns Hopkins Univ., Baltimore, MD, USA, Tech. Rep., 2004.
2. K. Hoffman, D. Zage, and C. Nita-Rotaru [2] introduced an “Iterative Trust and Reputation Management Scheme” (ITRM).” ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.
3. J.-W. Ho, M. Wright, and S. Das[3],introduced, an“Integrating Data Transmission Technique in Sensor Wireless Network Using Data Aggregation Method” in Proc. 6th ACM Int. Workshop Data Eng. Wireless Mobile Access, 2007, pp. 1–8.
4. H. Liao, G. Cimini, and M. Medo[4],introduced an “Data Aggregation Techniques Of Wireless Sensor Network Increasing Network Lifetime Using READA,” in Proc. 3rd Conf. Netw. Syst. Des. Implementation, vol.3, 2006, pp. 23–23.
5. M. C. Vuran and I. F. Akyildiz, “Spatial correlation-based collaborative medium access control in wireless sensor networks,” IEEE/ ACM Trans. Netw., vol. 14, no. 2, pp. 316–329, Apr. 2006.
6. L.-A. Tang, X. Yu, S. Kim, J. Han, C.-C. Hung, and W.-C. Peng, “Tru-Alarm: Trustworthiness analysis of sensor networks in cyber-physical systems,” in Proc. IEEE Int. Conf. Data Mining, 2010, pp. 1079–1084.

ISSN 2349-4506
Impact Factor: 2.265

7. J.-W. Ho, M. Wright, and S. Das, "Zone Trust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing," IEEE Trans. Dependable Secure Comput., vol. 9, no. 4, pp. 494–511, Jul./Aug. 2012.
8. S. Ozdemir and H. C¸ am, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749, Jun. 2010.
9. H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 278–287.