A Study of Effective and Secure Data Aggregation protocol for WSN Presence of Collision Attacks

K. Venkata Lakshmi
PGScholar
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

Sri Lakshmi Kanagala
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

Abstract-*Network security involves the authorization of access to data in a network, which is controlled the network administrator. Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. Collision attack means 0the 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. As we have limited energy resources and computational power, data aggregation from multiple sensor nodes is done using simple methods such as averaging. WSN's are usually unattended they are highly vulnerable to node compromising attacks. WSN the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing. When the cost of such technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms. Data aggregation in WSN is usually done by easy methods like averaging, these strategies area unit at risk of sure attacks. This technique makes them not solely collision strong, however conjointly additional correct and quicker connection. But, our experiments show that our methodology works quite well for different varieties of errors with none modification. These algorithms simultaneously aggregate data from multiple sources and provide a trust estimation of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. In this paper we analyzed some secure data aggregation mechanisms and introduced a new complicated collision attack with its impact on wireless sensor network.*

Keywords: Collusion Attacks, Data aggregation, Iterative Filtering Algorithm, Wireless sensor networks.

1. 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. Their limitations cause sensor network to use a 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. Trust and reputation systems have an important role in supporting the operation of a wide range of distributed systems, from wireless sensor networks to social networks, by providing an estimation of trustworthiness of participants in such distributed systems. The collected information are delivered to one or extra sinks, generally via multi-hop communication. The nodes unit of measurement typically expected to figure with batteries and unit of measurement typically deployed to not-easily-accessible or hostile surroundings, generally in large quantities. It'll be difficult or inconceivable to change the batteries of the nodes. On the alternative hand, the sink is commonly created in energy. Since the energy is that the foremost precious resource among the, economical utilization of the energy to prolong the network fundamental quantity has been the most target of plenteous of the analysis on the. The communications among the has the several-to-one property in this information from AN outsized sort of nodes tend to be centred into many sinks. Since multi-hop routing is generally needed for distant nodes from the sinks to avoid wasting energy, the nodes near a sink are going to be burdened with relaying AN outsized amount of traffic from completely different nodes. The main target of malicious attackers is aggregation algorithms of the trust and reputation systems. Trust and reputation systems are very effective mechanism providing security for Wireless Sensor Networks (WSN's). Sensors which are in the hostile environment are susceptible to attacks where attackers inject false data into system. So, assessing trustworthiness of data and announcing it to decision makers is challenging task. To reduce energy consumption, many systems also perform in-network aggregation of sensor data at intermediate nodes enroots to the base station. Most existing aggregation algorithms and systems do not include any provisions for security and consequently these systems are vulnerable to a wide variety of attacks. In particular, compromised nodes can be used to inject false data that leads to incorrect aggregates being computed at base station. Two main security challenges in secure data aggregation are confidentiality and integrity. While traditionally encryption is used to provide end to end confidentiality in WSN, the aggregators in secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network; it complicates the existing security challenges. in sensor technology has made it possible to have very small, low powered sensing devices equipped with programmable compute, multiple parameter sensing and wireless message capability. Also, the low cost makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the consistency and accuracy of data and the area coverage. Wireless sensor networks offer information about isolated structures, wide-spread environmental changes, etc. Wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental situation, such as sound, temperature, and motion.

2. Related Work

Simple data aggregation is highly susceptible to node compromising attacks and produces invalid data. Also the existing system lack in accuracy and faster while aggregating data which decrease the performance in the presence of non-stochastic errors, such as faults and malicious attacks. By simple data aggregation it is easily affect by exploiting false data injection through a number of compromised nodes. Robust data aggregation is a

serious concern in WSNs and there are a number of papers investigating malicious data injection by taking into account the various adversary models. The main research is around: Iterative filtering algorithms, certainty and reputation systems for WSNs, and secure data aggregation with compromised node detection in WSNs. There are a number of published studies introducing IF algorithms for solving data aggregation problem. The paper intoduces six different algorithms, which are all iterative and are similar and the only difference among the algorithms is their choice of norm and aggregation function. proposed a slight different iterative algorithm. Their main differences from the other algorithms: 1) The ratings have a time-discount factor, so after time their importance will fade out; and 2) The algorithm maintains a black-list of users who are especially bad raters. Liao et al. proposed an iterative algorithm which beyond simply using the social network of users , also uses the rating matrix. We introduced the several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are still attackable to a novel sophisticated collusion attack we introduce. The performance of IF is approved by simulation on synthetically generated data sets. According to simulation results it clarify that the robust aggregation technique is effective in terms of robustness against the novel sophisticated attack as well as capable in terms of the computational cost. Based on biased and unbiased readings in specified location, the sensor errors are estimated. IF provides greater accuracy and better collusion resistance than the other method. Our work is related to three areas that are studied from the other reference such as IF algorithms, trust and reputation system for WSNs and secure data aggregation with compromised node detection in WSNs. There are many past literatures introduce the IF algorithms for solving data aggregation problem. In one of the prior work six different IF algorithms are proposed. They are all iterative and are similar to one another. The only difference is their choice of norm and aggregation function. A bias-smoothed tensor model based on a Bayesian model is introduced in another paper. The sensor complexity in this model is high due to its mathematical framework. The Existing filtering technique considered only the cheating behavior of adversaries, none of them take into account of collusion attack. Our work is also related to the trust and reputation systems in WSNs. It is a two tier framework for data management in the networks. This includes a number of proxy nodes for managing sensor readings from corresponding sensor nodes. Trust and Reputation concepts can be used to overcome the compromised node and secure data aggregation problems in sensor nodes. A combination of trust mechanisms, data aggregation and fault tolerance is also proposed to enhance data trustworthiness. Some of the prior works focus on detecting false aggregation on the cluster head. That is, data aggregator node obtaining data from source nodes and producing wrong aggregated values. The problem of false data being provided by the data sources and collusion attack is not addressed in these works.

3. EXISTING SYSTEM

Due The Problem of this system is to detect false temporal variation patterns in a continuous aggregation and also to verify the correctness of the observed temporal variation pattern in a time window by checking only a small part of aggregation results termed representative points. The representative points are selected to capture the temporal variation pattern of the aggregate.

In recent years, there has been an increasing amount of literature on IF algorithms for trust and reputation systems. The performance of IF algorithms in the presence of different types of faults and simple false data injection attacks has been studied where it was applied to compressive sensing data in WSNs.

In 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.

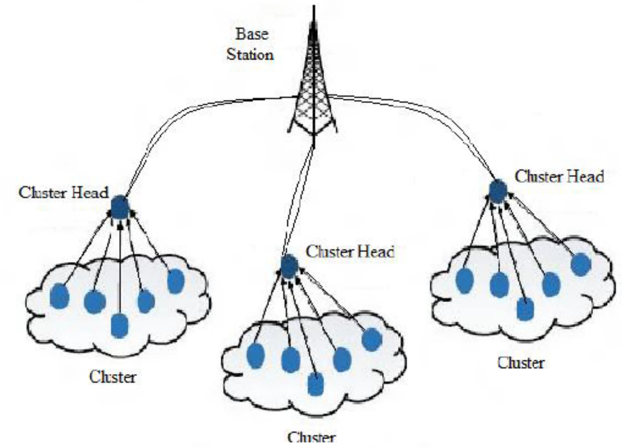
Disadvantages of Existing System

Although the existing IF algorithms consider simple cheating behavior by adversaries, none of them take into account sophisticated malicious scenarios such as collusion attacks.

In wireless sensor networking (WSN), when the environment is sensed the nodes are created, which transfer the collected data to the base station.

1. When the data in wireless sensor network are interrelated, multiple number of nodes available report similar readings to the base station.

2. When millions of redundant data are transmitted a very large amount of energy is wasted.



Network Model for WSN

4. PROPOSED SYSTEM

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 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. Design of an efficient and robust aggregation method inspired by the MLE, which utilizes 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

Advantages of Proposed System

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.

Cluster head are going to be responsible for administration of all different nodes within the several clusters and grouping the data from the nodes within the cluster and information transferring to the neighboring cluster head for huge amount of information updating and exchange.Other cluster nodes are going to be give opportunity to global and participate cost is once more calculated. There after the data aggregation approach is presumed as the collection of data and numerous problems defines from the user end are checked and sends into minimum level schemes by a query processor. Data are aggregate and collected is stored at a storage location to the database server. Finally at last the data is aggregated by data cube approach and each and every one the grouped data are going to be transfer to the base station.

5. Experimental Results

Service Provider

In this module, the Service Provider activates all the sensors and assigns temperatures to the sensor node, and backup temperature will be stored, uploads their data to the particular base station. It will store in node. The service provider, can view the attacked file by the Base Station, He can replace the injected fake temperature to the sensor node.

Router

In this module, the predicate count query is used to determine the total number of nodes whose sensor readings have some property in the network. And it is responsible for delivering the sensor readings to the Base stations.

If he founds fake temperature readings then it transfer the flow to Base Station. Before sending any file to receiver temperature will be verified, then send to particular base station.

In a router we can view the sensor temperature details and clear the details.

Base Station

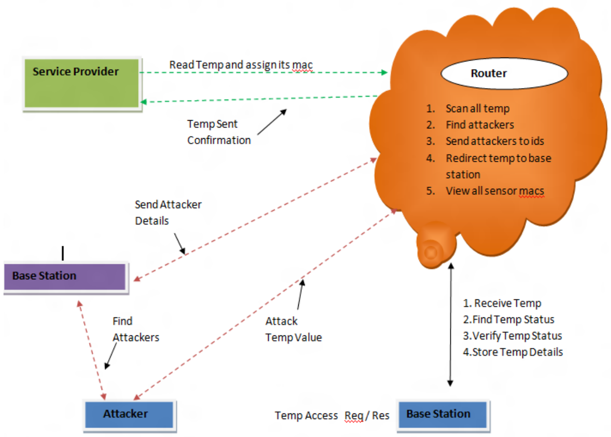
In this module, The base station collecting all sensor nodes (sn1, sn2, sn3, sn4, sn5….) and computing aggregation results at the base station (BS), in network aggregation allows sensor readings to be aggregated by intermediate nodes, which efficiently reduces the communication overhead. The Base Station used for checking the temperature status and to verifies the results through reliable random sampling achieved by data commitment and interactive proofs with the base station.

.

Attacker

Attacker is one who is injecting the fake temperature to the particular sensor node. And Router will identify the attackers, then stored in attacker list.

The main shortcoming of the IF algorithms in the proposed attack scenario is that they quickly converge to the sample mean in the presence of the attack scenario. In order to investigate the shortcoming, we conducted an experiment by increasing the sensor variances as well as the number of colluders. Fig5 represents the node placement in the network. The nodes are grouped into the cluster format. Each cluster has cluster head is called aggregator node. The objective of our experiments is to evaluate the robustness and efficiency of our approach for estimating the true values of signal based on the sensor readings in the presence of faults and collusion attacks. The user must register their login credentials and to select the assigning weight factors depending on the number of data have to be used. By using IF, the sensor error is estimated in a wide range of sensor faults and not susceptible to the described attack. It utilizes an estimate of the noise parameters obtained from sensor nodes. The enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensor using input. The aggregated data is performing a filtering operation. If any error occurs on the filtering process, first estimate the errors and calculate the new variance of data using MLE and finally transmit the aggregated data in a secured way.



It is clear that if the mean of the bias of all sensors is not zero, then there would be no way to account for it on the basis of sensor readings. On the other hand, bias of sensors, under normal circumstances, comes from imperfections in manufacture and calibration of sensors as well as from the fact that they might be deployed in places with different environmental circumstances where the sensed scalar might in fact have a slightly different value. Since by the very nature we are interested in obtaining a most reliable estimate of an average value of the variable sensed, it is reasonable to assume that the mean bias of all sensors is zero (without faults or malicious attack).

6. Conclusion

In this paper we have proposed the concept of We have introduced a sophisticated collusion attack scenario against a number of existing IF algorithms. Moreover, we have proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms robust against sophisticated collusion attacks. We plan to implement our approach in a deployed sensor network. Data aggregation mechanisms along with data averaging techniques are analyzed. Network model proposed by Wagner is described for sensor network. Adversary models with their assumptions are reviewed. As soon as computational power of very low power processors significantly improves, future aggregator nodes will be capable of performing more difficult data aggregation algorithms, in wireless sensor Network needs the high computational cost and power need for transmitting the data. To reduce that data aggregation technique is used in WSN. This data aggregation is done by using various simple methods such as averaging but this technique is highly vulnerable. In proposed system, we introduced Iterative filtering algorithms with initial estimation by giving weighted factors which makes algorithm collusion robust, accurate and fast converging. In future work, we will investigate whether it can protect against compromised sensor nodes in a deployed sensor network. Data aggregation mechanisms along with data averaging techniques are analyzed. As soon as computational power of very low power processors significantly improves, future aggregator nodes will be capable of performing more difficult data aggregation algorithms, thus making wireless sensor networks less vulnerable. In future an enhanced strategy against collusion attack is introduced which makes is not only collusion robust, but also more accurate and faster converging.

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 Dependa-ble and Secure Computing (TDSC) ,2014

[2] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults " , IEEE Transactions on Parallel and Distrib-uted Systems, August 2013.

[3] 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.

[4] 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. compromise detection and revocation in wireless sensor networks using sequential hypothesis testing " IEEE Transactions on Dependable and Secure Computing, july-aug. 2012.

[6] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sen-sor networks: Attack analysis and countermeasures", Journal of Net-work and Computer Applications, 2012

[7] S. Roy, M. Conti, S. Setia, , and S. Jajodia, "Secure data aggregation in wireless sensor networks", IEEE Transactions on Information Forensics and Security, 2012.

[8] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN", 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011.

[9] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a com-ment rating environment", in Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, 2011 .

[10] J.W. Ho, M. Wright, and S.K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hy-pothesis Testing", IEEE Transaction on Mobile Computing, June 2011.

[11] M. Groat, W. He, and S. Forrest, "KIPDA: k-indistinguishable priva-cy preserving data aggregation in wireless sensor networks", in IN-FOCOM'2011.

[12] R. Rana, W. Hu, T. Wark, and C.T. Chou, "An Adaptive Algorithm for Compressive Approximation of Trajectory (AACAT) for Delay Tolerant Networks," Proc. Eighth European Conf. Wireless Sensor Net-works, Feb. 2011.

[13] Y. Shen, W. Hu, R. Rana, and C.T. Chou, "Non-Uniform Compres-sive Sensing in Wireless Sensor Networks: Feasibility and Applica-tion," Proc. Seventh Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP),2011.

[14] V. Kumar, and S. Madria, "Secure data aggregation in wireless sen-sor networks," in Wireless Sensor Network Technologies for the Infor-mation Explosion Era. Springer, 2010.

[15] 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.

[16] 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 " ,IEEE International Conference on Data Mining , 2010.

[17] J. Bahi, C. Guyeux, and A. Makhoul, "Efficient and robust secure aggregation of encrypted data in sensor networks," in Fourth Inter-national Conference on Sensor Technologies and Applications, July 2010.

[18] R.K. Rana, C.T. Chou, S.S. Kanhere, N. Bulusu, and W. Hu, "Ear- Phone: An End-to-End Participatory Urban Noise Mapping Sys-tem," Proc. ACM/IEEE Ninth International Conf. Information Processing in Sensor Networks , April 2010.

[19] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputa-tion systems," in Proceedings of the 5 th International Workshop on Se-curity and Trust Management, 2009.

[20] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking, 2009.

AUTHORS

K. Venkata Lakshmi
PG Scholar
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam

Sri Lakshmi Kanagala
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam