Scientific Journal Impact Factor (SJIF): 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

A NOVEL APPROACH FOR PROTECTING INFORMATION ACCUMULATION IN OCCURRENCE OF COLLUSION ATTACKS FOR WSN

Arul Mozhi.K[1], Santhoshkumar.M[2], Srimadevi.S[3], Saranya.B[4]

[1]Department of ME-CSE Srinivasan Engineering College,Perambalur,,TamilNadu,India
[2]Assistant Professor/CSE Srinivasan Engineering College,Perambalur,Tamil Nadu,india
[3]Department of ME-CSE Srinivasan Engineering College,Perambalur,Tamil Nadu,India
[4]Department of ME-CSE Srinivasan Engineering College,Perambalur,Tamil Nadu,India

Abstract-Wireless sensor networks, there is a need for the toughness of observing and low cost of the sensor nodes. In wireless sensor nodes, there is a presence of the data which is collected by each sensor node. All these details are aggregated by the aggregator node. The aggregator node forwards to the base station based on the aggregate value. The average, max methods those are not using the secrecy methods hence they are compromised by the adversaries. The improved iterative filtering techniques by providing the initial approximation against the collusion robust and accurate and fast converging.

I. INTRODUCTION

Sensor networks are progressively deployed for requests such as wildlife habitat monitoring, forest fire prevention, and military surveillance. In these applications, the data composed by sensor nodes from their physical situation needs to be accumulated at a host computer or data sink for further analysis.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.Inappropriately, none of the above algorithms or schemes comprise any supplies for safety; as a result, they are vulnerable to many attacks that can be launched by unauthorized or compromised nodes.Compromised nodes can be used to presentation a wide variety of insider attacks that disturb the process of the sensor application and network. Due to a need for robustness of monitoring, wireless sensor networks (WSN) areusually redundant. Data from multiple sensors is aggregated at an aggregatornode which then forwards to the base station only the aggregate values. Atpresent, due to limitations of the computing power and energy resource of sensornodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and moreimportantly, malicious attacks. This cannot be remedied by cryptographicmethods, because the attackers generally gain complete access to informationstored in the compromised nodes. For that reason data aggregation at theaggregator node has to be accompanied by an assessment of trustworthiness ofdata from individual sensor nodes.

II. RELATED WORK

The consider the sensors which are deployed in hostile and unattended environments are highly susceptible to node compromising attacks.In the other prior work, the non iterative statistical sample estimation methods which are not robust against false data injection by a number of compromising nodes.In the other the employ a number of monitoring nodes which are running aggregation operations and providing a MAC value. In the other prior work, they proposed the scheme to detect the compromised nodes in the wireless sensor networks and then they apply the software attestation for the detected nodes. The proposed system, they have proposed the robust variance estimation method in case of skewed sample mean.They proposes the identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms.They proposed a novel method for estimation of sensor error’s which is effective in a wide range of sensors faults.They proposed an well-organized and vigorous aggregation method it exploits an approximation of noise parameters.They enhanced the IF scheme to protect against cultured collusion attacks by provided that an initial approximation of dependability of sensors using the inputs. , it should be close to the variance of the Maxi-mum Likelihood Estimator. However, such estimation should be achievedwithout supplying to the algorithm the variances of the sensors. The algorithm should also be robust in the presence of non-stochasticerrors, such as faults and malicious attacks, and, besides aggregating data,such algorithm should also provide an assessment of the reliability andtrustworthiness of the data received from the individual sensor nodes.

Trust and reputation systems have a significant role in supporting opera-tion of a wide range of distributed systems, from wireless sensor networks ande-commerce infrastructure to social networks, by providing an assessment oftrustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behaviour ofthe participants up to that moment and has to be robust in the presence of var-ious types of faults and malicious behaviour. There are a number of incentivesfor attackers to manipulate the trust and reputation scores of participants in adistributed system, and such manipulation can severely impair the performanceof such a system. The main target of malicious attackers are aggregationalgorithms of trust and reputation systems.Trust and reputation have been recently suggested as an effective securitymechanism for Wireless Sensor Networks (WSNs). Although sensor networksare being increasingly deployed in many application domains, assessing trust-worthiness of reported data from distributed sensors has remained a challengingissue. Sensors deployed in hostile environments may be subject to node compro-mising attacks by adversaries who intend to inject false data into the system.In this context, assessing the trustworthiness of the collected data and makingdecision makers aware of the trustworthiness of data becomes a challenging task. As the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing, and as the cost of such 2 technology drops, WSNs will be able to afford hardware which can implement both more sophisticated data aggregation and trustworthiness assessment algorithms; an example is the recent emergence of multi-core and multi-processor systems in sensor nodes.

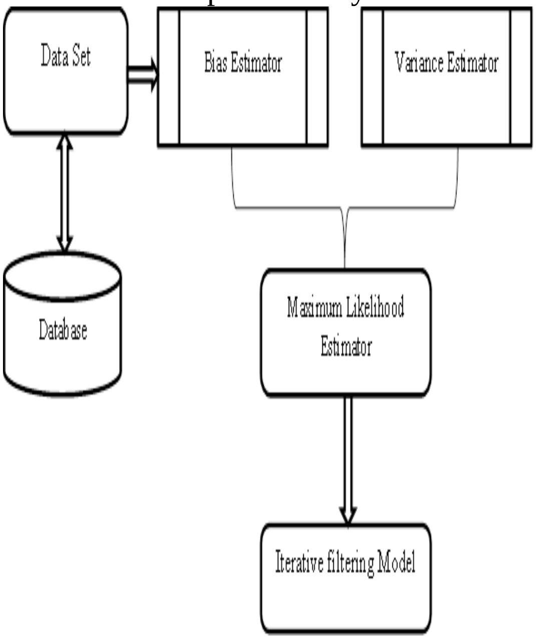

Figure 1 system architecture

III. SCOPE OF THE PAPER

security for data aggregation in sensor networks. Current aggregation schemes were designed without security in mind and there are easy attacks beside them. They proposed two algorithms. They are estimator algorithm and re-silent estimators and resilient aggregation algorithm. They surveyed numerous methods for making these combination structures more resilient beside certain attacks. And they suggested a mathematical framework for correctly estimating their security.

The aim of this paper is to survey secure data aggregation in sensor networks. Sensor links have been pro-posed for technical data collection, conservation monitoring, structure health monitoring, and intruder and are alarm schemes, and many other requests connecting dispersed communication with the physical setting. Many of these requests involve a dispersed system of sensors gauging the setting from many vantage opinions and then someway combining the calm data to form a global swift view that can be acted upon. So, data combination can be viewed as a significant structure block in sensor nets. Inappropriately, even however safety has been recognized as a major test for sensor. Due to limited computational power and energy resources of sensor nodes, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging.

However, such aggregation has been known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trust-worthiness of data and reputation of sensor nodes has become crucially important for WSN. As the performance of very low power processors dramatically improves and their cost is drastically reduced, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, which will make WSN less vulnerable to severe impact of compromised nodes. Iterative altering algorithms hold great promise for such a purpose. Such algorithms simultaneously 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 source. In this paper we demonstrate that a number of existing iterative altering algorithms, while signicantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce. To address this security issue, we propose an improvement for iterative altering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging. We believe that so modied iterative altering algorithms have a great potential for deployment in the future WSN. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. 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. They propose 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. They present our assumptions, discuss IF algorithms, describe a collusion attack scenario against IF algorithms, and state the problems that we address in this paper. In this paper we assume that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator.

IV. EXPERIMENTAL EVALUATION

A.Dataset Model

In this module, we are going to consider the INTEL LABdataset, which contains the following attributes those are, date, time, epoch, mote-id, temperature, humidity, light, voltage. And also consider the positioning detail dataset which contains the sensor id, x co-ordinate and y co-ordinate. This dataset is taken from the 54 sensors which are deployed in the Intel Berkeley research lab between February 28th and April 5th, 2004. Here we are taking the each sensor readings for the process.

B.Bias Estimation Model

In this module, the bias have to be estimated based on the Gaussian approximation. That is there is a need to evaluate the sensor bias which is mentioned by the b_s and the error term e^t_s is corresponds to the data what we considered in the dataset which is the data those are collected from the wireless sensor nodes. For that here we are evaluating the difference of such error between the considered errors. Then the compact form of equation is used to estimate the bias for considered data from the sensors.

C.Maximum Likelihood Estimation Model

In this module, have to extract the un-biasing sensor reading which are takes place with the help of the bias estimated result which calculated from the above module. After that have to consider the variance estimated result from the above module. And considers the extracted un-biasing sensor module to make the maximum likelihood estimation with the variance and with the extraction of the un-biasing sensor reading from the bias estimation.

D.Iterative filtering Model

In this model we are going to consider the above model output as the input for this model. Here we are considering with the initial values to estimate the trustworthiness of the each sensor based on the distance of the sensor readings. And have to evaluate the performance accuracy and efficiency. By this process we can make the estimation process in the initial level itself hence we can reduce the number of iterations for the estimations.

V. CONCLUSION

The considered novel collusion attack scenario against the number of prior algorithms.Then they proposes the IF algorithm with the initial approximation of the dependability of the sensor nodes in the network.Those are more precise and earlier meeting those algorithms.The process using the dataset which is a static process hence the process is notanalyzed correctly. So as the future extension have to analyze the process in the real time scinario in that we consider the data security may be loss while the transmission from the aggregator node to the destination. If the aggregator node is compromised means it can tranmit to any of the destination hence here the data will misused so there is the lack of the data security in the data aggregation process. For that we apply the combination of the encryption and password based encryption process. Hence here we may reduce the chance of the misusing of the data while the transmission from the aggregator to the destination.

REFERENCES

[1] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless ssensor networks: A comprehensive overview,” Comput. Netw.,vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of statistics : a concise course in statistical inference. New York: Springer.

[3] A. Jøsang and J. Golbeck, “Challenges for robust trust and reputation systems,” in Proceedings of the 5 th International Workshop on Security and Trust Management, Saint Malo, France,2009.

[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” ACM Comput.Surv., vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[5] 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,S. Gritzalis, T. Karygiannis, and C. Skianis, Eds. Troubador Publishing Ltd, 2009, pp. 105–128

.[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN '10, 2010, pp. 2–7.

[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multi core wireless sensor network:E2MWSN," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on,2011, pp. 1–4.

[8] 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.

[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," CoRR, vol. abs/1012.3793, 2010.

[10] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via Iterative Refinement," EPL (Europhysics Letters),vol. 75, pp. 1006–1012, Sep. 2006.

[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physical A Statistical Mechanics and its Applications, vol.371, pp. 732–744, Nov. 2006.

[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in SDM'12, 2012, pp. 612–623.

[13] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," in Proceedings of the 2009 IEE international conference on Symposium on Information Theory - Volume 3, ser. ISIT'09, 2009, pp. 2051–2055.

[14] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," ArXiv e-prints, Aug.2012.

[15] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment," in Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, ser. KDD '11, 2011, pp. 159–167.