Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.67 – 71

Secure Data Aggregation Technique for WSN

Jay Shihall, Viraj Shirwalkar, Kalpesh Patil, Saurabh Ajnadkar
K.K.Wagh Institute of Engineering Education & Research, Computer Engineering & SavitribaiPhule Pune University, Nashik
jayshihall124@gmail.com, virajshirwalkar@gmail.com, kalpesh33patil@gmail.com, saurabhajnadkar@gmail.com

Abstract— An aggregation of data from multiple sensor nodes done at the aggregating node consumes more energy and it has limited computational power. Aggregation is usually accomplished by simple methods such as averaging but highly vulnerable to node compromising attacks. Since wireless sensor networks are usually setup in protected manner, they are vulnerable. Thus, exact data and reputation of sensor nodes is crucial for wireless sensor networks. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of implementing stagy data aggregation algorithms, thus making wireless sensor networks less vulnerable. Iterative filtering algorithms are better to recover such problem. Such algorithms simultaneously aggregate data from multiple sources and provide exact of these sources. In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more thriving against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce. We propose an improvement for IF techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.

Keywords— Network-level, Sensor networks, Aggregation, Security, Node compromise

INTRODUCTION

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the

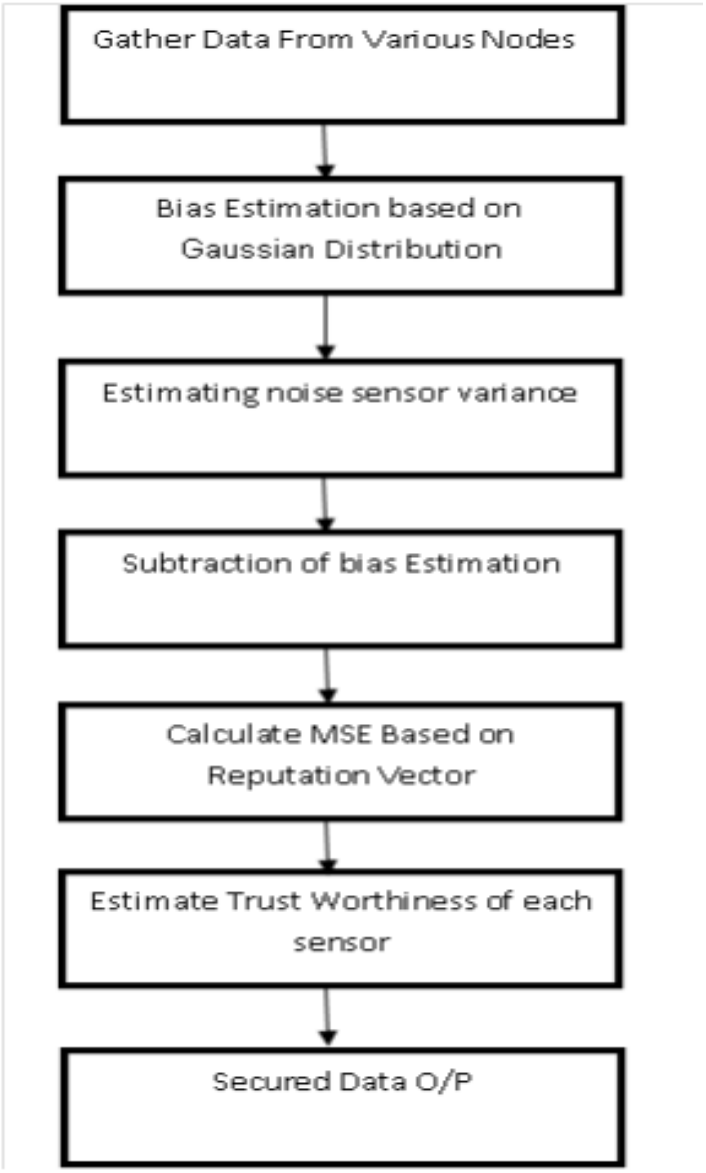
behaviour of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behaviour. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation severely impairs the performance of such a system. The main target of malicious attackers are aggregation algorithms of trust and reputation systems Trust and reputation have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs) Although sensor networks are being increasingly deployed in many application domains, assessing trustworthiness of reported data from distributed sensors has remained a challenging issues. 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 and announcing decision makers for the data trustworthiness 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 technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms; an example is the recent emergence of multi-core and multi-processor systems in sensor nodes . Aggregation has been used in many different areas of networking and security. Initially it was used for collecting data from multiple sensor nodes and send towards the base station. Later it has been also used for compressed data to return the result in common information of all data. The main reason for this was the noise in the text document.

Related Work

Earlier work represents the security vulnerabilities of data aggregation protocols for sensor networks and a survey of secure and resilient aggregation protocols for both single-aggregator and hierarchical systems. Also representing the security vulnerabilities of data aggregation protocols for sensor networks and a survey of secure and resilient aggregation protocols for both single-aggregator and hierarchical systems. The idea of the wsn that investigates the relationship between security and data aggregation process in wireless sensor networks. Also this concept represents the data decoding from multiple websites on the base of voting system. The rank is assigned to the raters and ratees using only the evaluation data, consisting of an array of scores each of which represents the rating of a ratee by a rater. It is also shown to be robust against various hypothetical types of noise as well as intentional abuses. It deals with several approaches for making these aggregation schemes more resilient against certain attacks.

Methodology

Due to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks (WSNs) are usually redundant. 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 cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes.



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. As we will see, such vulnerability to sophisticated collusion attacks comes from the fact that these IF algorithms start the iteration process by giving an equal trust value to all sensor nodes. In this paper, we 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. 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, we believe, also more robust under significantly more general circumstances; for example, 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. Since readings keep streaming into aggregator nodes in WSNs, and since attacks can be very dynamic (such as orchestrated attacks), in order to obtain trustworthiness of nodes as well as to identify compromised nodes we apply our framework on consecutive batches of consecutive readings. Sensors are deemed compromised only relative to a particular batch; this allows our framework to handle on-off type of attacks (called orchestrated attacks in) .This paper aims to illustrate the robustness of the proposed data aggregation method in the presence of sophisticated attacks. Moreover it depicts the collusion attack scenario that can circumvent all the IF algorithms tried. Moreover, the accuracy of the algorithms dramatically decreases by increasing the number of compromised nodes participated in the attack scenario. As explained before, the algorithms converge to the readings of one of the compromised nodes, namely, to the readings of the node which reports values very close to the skewed mean. This rightly demonstrates that an attacker with enough knowledge about the aggregation algorithm employed can launch a sophisticated collusion attack scenario which defeats IF aggregation systems. 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.

Result Table

Sr No.	Description	UML design observations
1.	**Problem description**	
	1) Input 2) Noise Parameter Estimation. 3) Maximum Likelihood Estimation. 4) Iterative Filtering 5) Result Let the system be described by S, S={D, I, NPE, MLE, IF, R}	Where S: is a System. D: is the set of Dataset. I : Input NPE : Noise Parameter Estimation MLE : Maximum Likelihood Estimation IF : Iterative Filtering R: Result.

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. There are three bodies of work related to our research: IF algorithms, trust and reputation systems for WSNs, and secure data aggregation with compromised node detection in WSNs. Our work is also closely related to the trust and reputation systems in WSNs. We have proposed a general reputation framework for sensor networks in which each node develops a reputation estimation for other nodes by observing its neighbors which make a trust community for sensor nodes in the network. That is a trust based framework which employs correlation to detect faulty readings. Moreover, they introduced a ranking framework to associate a level of trustworthiness with each sensor node based on the number of neighboring sensor nodes are supporting the sensor.

Conclusion

Thus in this paper, we introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, we will investigate whether our approach can protect against compromised aggregators. We also plan to implement our approach in a deployed sensor network image. This resultant image then can be used to enlighten the patients with the severity and necessity of the treatment.

REFERENCES

[1] S. Ozdemir and Y. Xiao, Secure data aggregation in wireless sensor networks: A comprehensive overview, Comput. Netw., vol. 53, no. 12, pp. 20222037, Aug. 2009.
[2] L. Wasserman, All of statistics : a concise course in statistical inference. New York: Springer.
[3] A. Jsang 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. 1:11:31, 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. 105128.
[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. 27.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN, in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 14.
[8] C. de Kerchove and P. Van Dooren, Iterative filtering in reputation systems, SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 18121834, 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. 10061012, Sep. 2006.

