Analysis of Secure Data Aggregation Mechanisms with the Impact of Collusion Attacks in Wireless Sensor Networks

Anita A.Gosavi, Sonali U.Nimbhorkar

Abstract— Wireless Sensor Networks (WSNs) enables the collection of physical measurements over a large geographic area. Data from multiple sensors is aggregated at an aggregator node and only the aggregate values are forwarded to the base station .At present, limitations of the computing power and energy resource of sensor nodes causes data to be aggregated by extremely simple algorithms such as averaging. Aggregation using simple averaging method is highly vulnerable to node compromising attacks and through the compromised sensor nodes the attacker can send false data to the aggregator to change the aggregate values. Iterative filtering algorithms is 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. In this paper we analysed some secure data aggregation mechanisms and introduced a new complicated collusion attack with its impact on wireless sensor networks.

Index Terms— Averaging method,Collusion attacks,Computing power, Data aggregation, Energy resource, Iterative filtering algorithms, 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 [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].

Trust and reputation systems have an important role in supporting 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 [6][20]. An estimation of trustworthiness at any given instant represents an aggregate of the behaviour of the participants up to that instant and has to be robust in the presence of various types of faults and malicious behavior [7][9]. There are a number of ways for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can usually harm the performance of system [19].

Iterative Filtering (IF) 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 [21]. 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 [8], thus making wireless sensor networks less vulnerable.

2 RELATED WORK

This section describes the various data aggregation and data averaging techniques, network model and attack model.

2.1 Secure Data Aggregation Techniques

Several data agagregation techniques have been proposed to enhance data availability. Authors in [15], combines the aggregation functionalities with the advantages provided by 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 inconsistent data in the presence of multiple compromised nodes.

Y. Sun et al. [3], accomplish data trustworthiness by extending Josang's trust model. Based on the multilayer aggregation architecture of network, they design a trust-based framework for data aggregation with fault tolerance with a goal to reduce the impact of erroneous data and provide measurable trustworthiness for aggregated results.

H.-S. Lim et al. [4], addressed the important and challenging problem of assuring trustworthiness of sensor data in the presence of malicious adversaries. They developed a game theoretic defense strategy to protect sensor nodes from attacks and to guarantee a high level of trustworthiness for sensed data. The objective of the defense strategy is to ensure that sufficient sensor nodes are protected in each attack/defense round.

2.2 Network Model

The conceptual model proposed by Wagner in [25] is considered for sensor network topology. Fig. 1 shows assumption for network model in WSN. The sensor nodes are divided into seperate clusters, and each cluster has a cluster head which

acts as an aggregator. Data are periodically collected and aggregated by the aggregator. Authors in [1] 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. It also assume that each data aggregator has enough computational power to run an suitable algorithm for data aggregation.

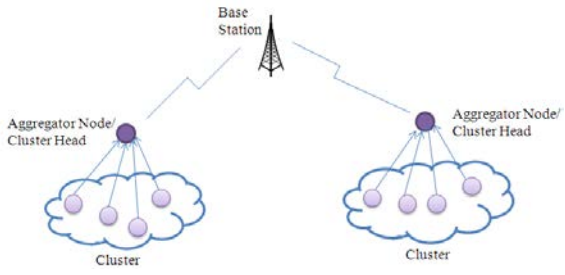

Fig.1. Network model for wireless sensor network

2.3 Data Averaging Technique

A computational efficient method to compute a weighted average (robust average) of sensor measurements is proposed in [2], which properly takes sensor faults and sensor noise into consideration. Authors assume that the sensors in the wireless sensor network use random projections to compress the data and send the compressed data to the data fusion centre [3]. Computational efficiency of this method is achieved by having the data fusion centre work directly with the compressed data streams and they only needs to perform decompression once to compute the robust average, thus greatly reducing the computational requirements.

2.4 Adversary Model

The past researchers [1][21] developes the attack models by considering the fact that they cannot rely on cryptographic methods forpreventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. The authors in, considers Byzantine attack model, where the adversary can compromise a set of sensor nodes and insert any false data through the compromised nodes [26]. Following are some assumptions made in this model

a) Sensors are deployed in a hostile unattended environment with some physically compromised nodes.
b) When a sensor node is compromised, all the information which is inside the node becomes accessible by the adversary. System cannot depend on cryptographic methods for preventing the attacks because the adversary may extract cryptographic keys from the compromised nodes [17].
c) Through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of changing the aggregate values.
d) All compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack.
e) The adversary has enough knowledge about the aggregation algorithm and its parameters.
f) The base station and aggregator nodes cannot be compromised by adversary node.

3 COLLUSION ATTACK SCENARIO

In this scenario ten sensors are assumed that report the values of temperature which are aggregated using suitable aggregation algorithm Most of the algorithms employ simple assumptions about the initial values of weights for sensors [16]. In suitable adversary model, an attacker is able to mislead the aggregation system through careful selection of reported data values. The collusion attack scenarios are as follows

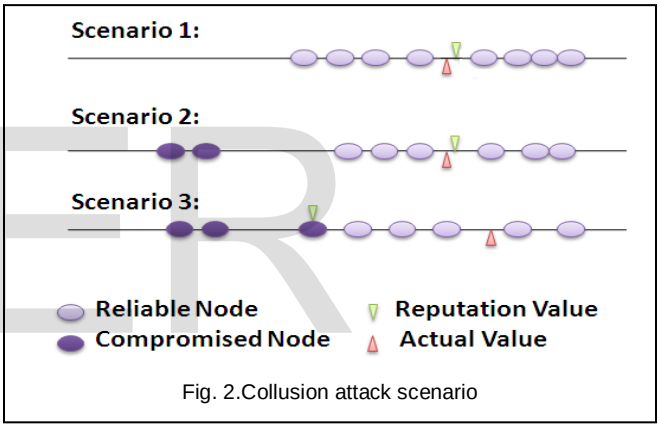

Fig. 2.Collusion attack scenario

1) In scenario 1, all sensors are trustworthy and the result of the aggregation algorithm is close to the actual value.
2) In scenario 2, first an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is twisted towards a lower value [22][23][24]. As these two sensor nodes report a lowervalue, aggregation algorithm penalises them and assigns to them lower weights, because their values are far from the values of other sensors.
3) In scenario 3, an adversary compromise three sensor nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity. It then computes the twisted value [25] of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings. In other words, two compromised nodes twist the simple average of readings, while the third compromised node reports a value very close to such twisted average [14].

3.1 Impact of collusion attack on Wireless Sensor Network

1) In collusion attack, attackers have a high level of knowledge about the aggregation algorithm and its parameters [10] hence they can conduct complicated attacks on wireless sensor networks by injecting false data through a number of compromised nodes.
2) Colluders attempt to twist the aggregate value by forcing aggregation algorithms to converge to twisted values provided by one of the attackers.
3) This attack is particularly dangerous for wireless sensor networks for two reasons [11].
   a) First, trust and reputation systems play critical role in wireless sensor networks as a method of resolving a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection [13], secure data aggregation, cluster head election, outlier detection.
   b) Second, sensors which are deployed in hostile and unattended environments [12] are highly vulnerable to node compromising attacks.

4 Conclusion

Data aggregation mechanisms along with data averaging techniques are analysed. Network model proposed by Wagner is described for sensor network network.Adversary models with their assumptions are reviewed. New sophisticated collusion attack scenarios along with its impact on wireless sensor networks is explained. 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 Dependable 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 Distributed 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.

[5] J.-W. Ho, M. Wright, and S. Das, "ZoneTrust: Fast zone-based node 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 sensor networks: Attack analysis and countermeasures", *Journal of Network 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 comment 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 Hypothesis Testing", *IEEE Transaction on Mobile Computing*, June 2011.

[11] M. Groat, W. He, and S. Forrest, "KIPDA: k-indistinguishable privacy preserving data aggregation in wireless sensor networks", in *INFOCOM'*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 Networks*, Feb. 2011.

[13] Y. Shen, W. Hu, R. Rana, and C.T. Chou, "Non-Uniform Compressive Sensing in Wireless Sensor Networks: Feasibility and Application," *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 sensor networks," *in Wireless Sensor Network Technologies for the Information 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, "TruAlarm: 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 International 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 System," *Proc. ACM/IEEE Ninth International Conf. Information Processing in Sensor Networks* , April 2010.

[19] 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*, 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.

[21] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," *in Proceedings of the 2009 IEEE international conference on Symposium on Information*, 2009.

[22] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto"Reputation-based Secure Data Aggregation in Wireless Sensor Networks" ,*Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies*,2008.

[23] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based

framework for high integrity sensor networks," *ACM Transaction* , Jun. 2008.

[24] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using Sensor Ranks for in-network detection of faulty readings in wireless sensor networks," *in Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*, 2007.

[25] D. Wagner, "Resilient aggregation in sensor networks," *in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*,2007.

[26] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," Department of Computer Science, Johns Hopkins University, Tech. Rep., 2007.