International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

The Impact of Collusion Attacks in WSN with Secure Data Aggregation System

S.Bhargavi[1]& Vishnu Prasad Goranthala[2]

[1] M.Tech Computer Science &Engineering, E-mail: bhargavi.cherry3@gmail.com
[2] MISTE Assosciate Professor, Department of CSE, E-mail: vishnuprasad.goranthala@gmail.com
[1, 2] Balaji Institute of Engineering & Sciences Narsampet, Warangal, Telangana, India.

Abstract:

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 are 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 analyzed 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 network (WSN) is a collection of devoted autonomous sensor nodes that observed physical or environmental conditions differently, such as pollution levels, humidity, temperature, sound, wind direction, pressure, etc. To cooperatively deliver data through the network to a main destination. WSNs were initially designed to facilitate military applications such as battlefield surveillance; but its usages have since been drastically extended to monitoring machineries, industrial processes, health, and controls. The WSN consist of "nodes" which may be differ in numbers from a few to several hundreds or even thousands, where every node is in connection with at least one sensor (or sometimes several). The sensor node is equipped with a tiny processor, a small battery, a radio transceiver antenna, and situate of transducers that used to gather information. They describe the variations in the environment of the sensor node [3]. Topology for WSNs can vary from a simple star or mesh network to an advanced multi-hop wireless mesh network.

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 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. 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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

systems. An estimation of trustworthiness at any given instant represents an aggregate of the behavior of the participants up to that instant and has to be robust in the presence of various types of faults and malicious behavior. 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.

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. 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.

Hierarchical Secure Data Aggregation

The following are the issues that are related to the security in the data aggregation of WSN:

- Data Confidentiality: In particular, the fundamental security issue is the data privacy that protects the transmitted data which is sensitive from passive attacks like eavesdropping. The significance of the data confidentiality is in the hostile environment, where the wireless channel is more prone to eavesdropping. Though cryptography provides plenty of methods, such as the process related to complicated encryption and decryption, like modular multiplication of large numbers in public key based on cryptosystems, utilizes the sensor's power speedily.
- Data Integrity: It avoids the modification of the last aggregation value by the negotiating source nodes or aggregator nodes. Sensor nodes can be without difficulty compromised because of the lack of the expensive tampering-resistant hardware. The otherwise hardware that has been used may not be reliable at times. A compromised message is able to modify, forge and discard the messages. Generally, in wireless sensor networks for secure data aggregation, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation.
- Hop-by-Hop encrypted data aggregation: In this technique, the encryption of the data is done by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node that obtains the last encrypted aggregation result decrypts it.
- End to End encrypted data aggregation: In this technique, the aggregator nodes in between does not contain any decryption keys and can only perform aggregation on the encrypted data.

2. RELATED WORK

Several data aggregation techniques have been proposed to enhance data availability. By monitoring neighborhood's activities, each sensor node evaluates the behavior of its cell members in order to filter out the inconsistent data in the presence of multiple compromised nodes.

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and ecommerce 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 behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system. The main target of malicious attackers is 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 issue. Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system.

Data aggregation is considered as one of the basic dispersed data processing measures to save the energy

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

and minimize the medium access layer contention in wireless sensor networks. It is used as an important pattern for directing in the wireless sensor networks. The fundamental idea is to combine the data from different sources, redirect it with the removal of the redundancy and thereby reducing the number of transmissions and also saves energy. The inbuilt redundancy in the raw data gathered from various sensors can be banned by the in-network data aggregation. In addition, these operations utilize raw materials to obtain application specific information. To conserve the energy in the system thereby maintaining longer lifetime in the network, it is important for the network to preserve high incidence of the in-network data aggregation.

3. IMPLEMENTATION

3.1 Network model

The conceptual model proposed by Wagner in is considered for sensor network topology. Fig. 1 shows assumption for network model in WSN. The sensor nodes are divided into separate clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. Authors in 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 assumes that each data aggregator has enough computational power to run a suitable algorithm for data aggregation.

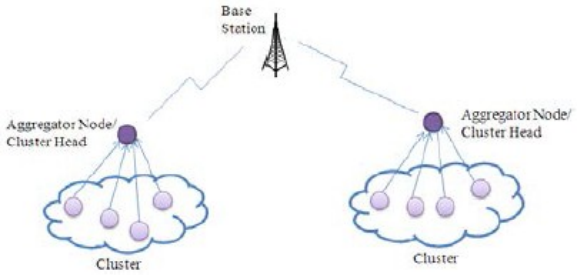

Fig.1. Network model for wireless sensor network

3.2 Data Averaging Technique

A computational efficient method to compute a weighted average (robust average) of sensor measurements is proposed 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. 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.

3.3 Adversary Model

The past researchers develop the attack models by considering the fact that they cannot rely on cryptographic methods for preventing 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. 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.
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.

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. 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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

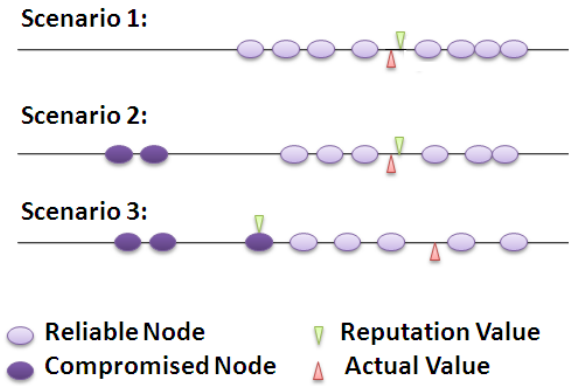

Fig. 2.Collusion attack scenario

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. As these two sensor nodes report a lower value, aggregation algorithm penalizes 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 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 com-promised nodes twist the simple average of readings, while the third compromised node reports a value very close to such twisted average.

4. CONCLUSION

In this paper, we study the data aggregation techniques in order to use them in WSN for reducing possibility of attacks. In other words, data aggregation can mitigate the impact of attacks in WSN 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. New sophisticated collusion attack scenarios along with its impact on wireless sensor networks are 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] M. Liu, N. Patwari, and A. Terzis, "Scanning the issue," Proc. IEEE, vol. 98, no. 11, pp. 1804–1807, Apr. 2010.

[2] Jukka Kohonen, ―Data Gathering in Sensor Networks‖, Helsinki Institute for Information Technology, Finland. Nov 2004.

[3] Gregory Hartl, Baochun Li, ―Loss Inference in Wireless Sensor Networks Based on Data Aggregation‖, IPSN 2004.

[4] Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, ―Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks‖, Draft Infocom2007 Paper.

[5] Bhaskar Krishnamachari, Deborah Estrin and Stephen Wicker, ―The Impact of Data Aggregation in Wireless Sensor Networks‖, Proceedings of the 22nd International Conference on Distributed Computing Systems – 2002.

[6] Kai-Wei Fan, Sha Liu, and Prasun Sinha, Structure-free Data Aggregation in Sensor Networks‖, IEEE Transactions on Mobile Computing – 2007.

[7] Cristobald de Kerchove and Paul Van Dooren. Iterative _ltering in rep- utation systems. SIAM J. Matrix Anal. Appl., 31(4):1812{1834, March 2010.

[8] Yanbo Zhou, Ting Lei, and Tao Zhou. A robust ranking algorithm to spamming. CoRR, abs/1012.3793, 2010.

[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.

S.Bhargavi pursing M.Tech in Computer Science Engineering from JNTU Hyderabad. Her research area includes Programming Languages, Data Base Management Systems, Mobile Applications, and Data Mining.

Vishnu Prasad Goranthala Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad, Master of Computer Applications from Osmania University Hyderabad. Currently working as an Associate Professor at Balaji Group of Institutions, Narsampet, Warangal, and has 12+ years of experience in Academic. His research areas include Information Security, Mobile and Cloud computing, Cryptography, Network Security.