Apr - Jun © 2017 Transactions; 4(14): 548-553

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Research Article

A Novel Data Aggregation Methodology for Secure Data Gathering in Wireless Sensor Networks

Ajay Sriramoju

Corresponding Author:
babuack@yahoo.com

DOI:
http://dx.doi.org/
10.17812/IJRA.4.14(91)2017

Manuscript:
Received: 8th Apr, 2017
Accepted: 17th May, 2017
Published: 30th June, 2017

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

In Wireless Sensor Network (WSN), data aggregation is used to have efficient data transfer between sensor nodes and base station. Data aggregation makes use of aggregate functions such as Count and Sum in order to reduce communication overhead and improve performance of WSN besides making it energy efficient. Thus, the network lifetime is increased. However, it is understood from the literature that there are many attacks launched on aggregation functions. Thus, it is inevitable to have secure aggregation in WSN. If not the aggregated data might have false contributions in sensing. There is relationship between security and data aggregation. When data aggregation process is not secured, it results in biased or compromised data collection that leads to potential risks to real world sensor applications. The aim of this paper is to investigate secure aggregation techniques and provide a new scheme based on iterative filtering that enhances secure data aggregation process. NS2 simulations are used to demonstrate proof of the concept.

Keywords: Wireless Sensor Network, data aggregation, security, aggregate functions

RANDSTAD TECHNOLOGIES, Senior Programmer Analyst 312 Sunrise Dr, Carnegie, PA 15106 - USA

IJRA - Year of 2017 Transactions:
Month: April - June
Volume – 4, Issue – 14, Page No's:548-553
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2017: 4(14)548-553

DOI: 10.17812/IJRA.4.14(91)2017

International Journal of Research and Applications
Apr - Jun © 2017 Transactions 4(14): 548-553

eISSN : 2349 – 0020
pISSN : 2394 – 4544
www.ijraonline.com

COMPUTERS RESEARCH ARTICLE

A Novel Data Aggregation Methodology for Secure Data Gathering in Wireless Sensor Networks

Ajay Sriramoju

RANDSTAD TECHNOLOGIES, Senior Programmer Analyst
312 Sunrise Dr, Carnegie, PA 15106 - USA

ABSTRACT

In Wireless Sensor Network (WSN), data aggregation is used to have efficient data transfer between sensor nodes and base station. Data aggregation makes use of aggregate functions such as Count and Sum in order to reduce communication overhead and improve performance of WSN besides making it energy efficient. Thus, the network lifetime is increased. However, it is understood from the literature that there are many attacks launched on aggregation functions. Thus, it is inevitable to have secure aggregation in WSN. If not the aggregated data might have false contributions in sensing. There is relationship between security and data aggregation. When data aggregation process is not secured, it results in biased or compromised data collection that leads to potential risks to real world sensor applications. The aim of this paper is to investigate secure aggregation techniques and provide a new scheme based on iterative filtering that enhances secure data aggregation process. NS2 simulations are used to demonstrate proof of the concept.

Keywords: Wireless Sensor Network, data aggregation, security, aggregate functions

1. INTRODUCTION

Wireless sensor nodes (WSNs) are widely used in different real world applications. They include both civilian and military applications. The applications include military surveillance, monitoring places, monitoring patients, forest fire detection, studying wildlife habitat, and monitoring of householders' behaviour to mention few. As there are technology innovations, WSNs are used for diversified applications. In sensor nodes, data aggregation is an important activity. It is the process of combining results at intermediate nodes during the routing of messages. It will reduce amount of data to be transferred. Therefore, the data aggregation techniques are used to have efficient data dissemination. Multiple sensor nodes can sense data and send to base station. A typical sensor node appears as follows.

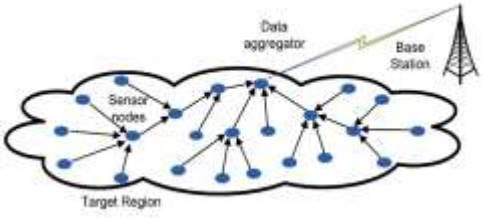

Figure 1 – Sample sensor network with data aggregation [1]

As shown in Figure 1, sensor nodes are spread across certain place. There is sink node to which all sensor nodes send sensed data. The sink node needs to have data stored and that can be accessed by legitimate users through Internet. In this scenario, when data is redundant while sending to base station. This increases network overhead. To overcome the problem many researches including [2] and [3] explored secure data aggregation in WSN. When data aggregation process is not secured, it results in attacks and the attackers mimic the changes to be genuine. Thus, it is very important to investigate into the attacks and counter measures pertaining to secure data aggregation. When data is not aggregated securely, it results in potential situation where the sensed data might have attack information injected by adversary.

When data sensed by different sensors is aggregated, it results in energy efficiency. The rationale behind this is that aggregation functions

have the capability to reduce the bulk of sensed data and before sending it to base station. Compromised nodes in WSN can inject false aggregates that pollute originally sensed data. This kind of attack is known as falsified sub aggregate attack [2]. Concealed data aggregation was explored in [4] where the data packets are subjected to encryption before being aggregated. Different encryption keys are used in order to encrypt packets. Based on the encryption keys the base station can perform decryption besides classifying packets. Data integrity and confidentiality are achieved by using Elliptic Curve Cryptography (ECC). There are many security requirements in WSN such as data confidentiality, data integrity, data freshness, source authentication, and availability. The interaction with data aggregation process includes availability of data aggregators, Sybil attacks against aggregators, alterations in aggregated data, and aggregation of encrypted data [1].

As discussed above, it is understood that data aggregation in WSN needs to be secured. Many existing algorithms provide solutions to the problem of attacks in WSN to disrupt aggregation process. Iterative filtering [2] is widely used in WSN for protecting data aggregation process. However, the prior techniques could not withstand sophisticated collusion attacks. In this research, a new iterative filtering algorithm is built to overcome the drawbacks. The proposed iterative filtering algorithm is implemented using NS2 simulations.

2. RELATED WORKS

As explored in [5], hierarchical sensor aggregation for efficient communication over WSN. According to them sensor nodes are involved in data aggregation within the network and send the results to base station. This was found to increase life time of network besides reducing communication overhead and energy consumption. They modified and improved previously available scheme known as integrity-preserving scheme for secure data aggregation in WSN. They also used a novel commitment structure for reducing node congestion. They tested their approach using aggregate functions such as COUNT, SUM and AVERAGE. In [13] made a review of data aggregation techniques used in WSN. They explored security needs of WSN and the possible relationship between data aggregation and security.

WSN security needs include source authentication, data confidentiality, availability, data freshness and data integrity. The data aggregation process involves both aggregation tasks and possible attacks launched by adversaries. Aggregation of encrypted data is the process of aggregation of encrypted data. There is need for changes in aggregated data. There is need for handling Sybil attacks launched by attackers besides considering availability of data aggregators [13]. They classified data aggregation approaches into two categories. They are known as tree-based data aggregation and cluster-based data aggregation. Tree-based data aggregation techniques are widely used for distributed data aggregation. Energy efficient tree construction for data aggregation is the main issue with tree based approaches.

Data aggregation process involves construction of a tree that includes base station and sensor nodes. Distance of the sensor nodes from base station and residual energy level of sensor nodes are the criteria in making decisions pertaining to choosing parent in the process of constructing tree. Each cluster is made up of a group of clusters. Every cluster has a cluster head which is involved in sending data to base station. The sensor nodes send data to cluster head. Data aggregation is taken place at each cluster and the aggregated data is sent to base station.

In [12], it explored outsourced aggregation services to third parties known as aggregators. However, aggregators are treated as untrusted and even they might be compromised as they are maintained by third parties. They proposed a framework known as SECOA which has many underlying secure protocols for achieving security in the context of outsourced aggregation. They employed one-way chains with unified use of them. Their approach supports large number of functions for aggregation. As it is outsourcing aggregation process, every sensor is subjected to very less communication overhead and that is workload-independent. The review of literature [1]-[21] showed different means of data aggregation. In this paper we proposed a novel approach for the same.

3. DATA AGGREGATION

Data aggregation is a process of combining data collected by sensors using simple averaging method or any such aggregation technique. The data collected by sensor nodes at a level are aggregated by other nodes in different level. The aggregated data is moved to next level. The next level data is combined with the data that have been aggregated and forwarded to the node. Figure 1 illustrates this phenomenon. There are multiple aggregator nodes that act as both sensor nodes and aggregator nodes. A sensor node can sense data from surroundings and send it to the base station directly or to its nearest neighbour. This each sensor can act as sender and receiver. Sensor nodes can also aggregate data. However, data aggregation has loop holes that are exploited by adversaries to inject false data into the network. The aim of secure data aggregation mechanism is to avoid such attacks make the network to produce genuine data.

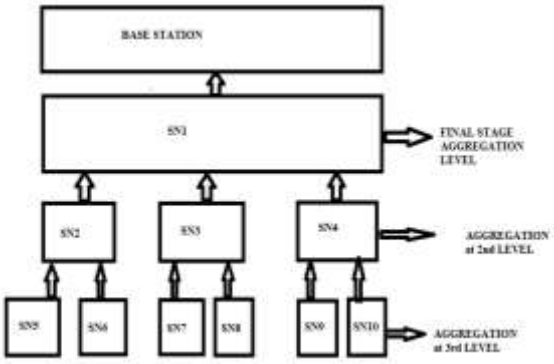

Figure 2: Data Aggregation Mechanism

The sensor node named SN1 is nearby base station. Let us consider this as level 1. Just below this level, SN2, SN3, and SN4 are in the next level. Afterwards SN5 to SN10 are in the next level. This way, different levels may exist in the real world sensor network. The sensor nodes such as SN5 to SN10 send their sensed to data to the above level neighbours. For instance the data sensed by SN5 and SN6 are sent to SN2. At SN2 the data is aggregated. In the same fashion the data of SN7 and SN8 are aggregated at SN3. Similarly the data of SN9 and SN10 are aggregated at SN4. From level 2, the aggregated data is forwarded to level 1 where SN1 is. At SN1 again the data that comes from SN2, SN3 and SN4 are aggregated along with the data sensed by SN1. Then the final aggregated data reaches base station. The problem with this architecture is that the aggregators may be subjected to attacks. Adversaries can launch false data injection attacks in order to pollute the data being sent to base station. This is done for monetary or other gains. This needs to be prevented. This is the reason secure data aggregation is needed.

4. SECURE DATA AGGREGATION WITH ITERATIVE FILTERING

Iterative filtering is the process of checking data at every level and ensures that the falsified data is identified and the nodes that are compromised are identified. When such malicious nodes are detected, the data from such nodes is avoided. The mechanism is illustrated in Figure 3.

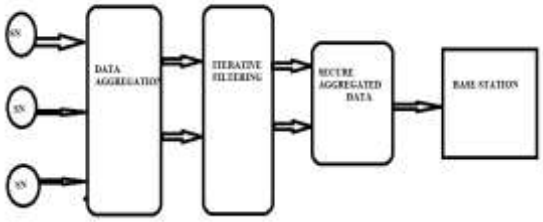

Figure 3: Secure Data Aggregation with Iterative Filtering

Sensor nodes are sending sensed data to their neighbour towards base station. The neighbour sensor node is able to aggregate data. However, the iterative filtering process makes a model of it and continuously checks whether any false data is injected into the network. Then the secure aggregated data reaches base station. The iterative filtering process is achieved by using the following algorithm.

5. SIMULATION RESULTS

NS2 simulations are used to implement the proposed secure data aggregation method. The simulations visualize the creation of WSN and the process of secure data aggregation. The sensor nodes are arranged as different layers and they communicate with base station. The data collected by the sensor nodes are aggregated before sending to base station. This is the mechanism that helps reduce communication and computation overhead in WSN. Thus the life of network is also increased.

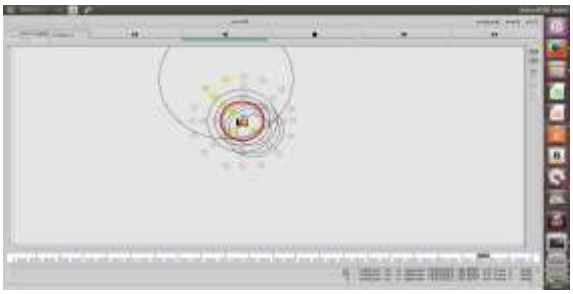

Figure 4 - Simulation Showing WSN Formation

As shown in Figure 4, the simulation shows the formation of WSN with number of layers and base station. The nodes send the sensed data to base station generally. However, the data collected to base station is aggregated for performance improvement in WSN.

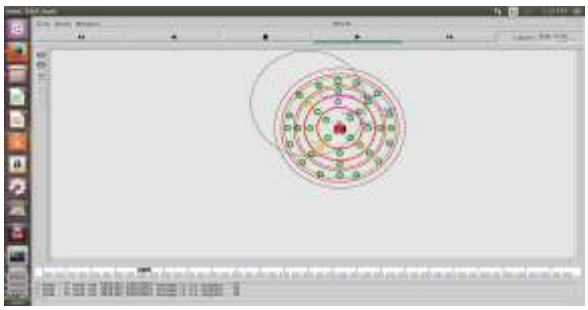

Figure 5 - WSN with Different Layers and Protocol Propagation

As shown in Figure 5, it is evident that there are different layers in the formed network. The base station is located in the middle. The simulation also considers an attacker model which demonstrates injection of falsified data as part of attack.

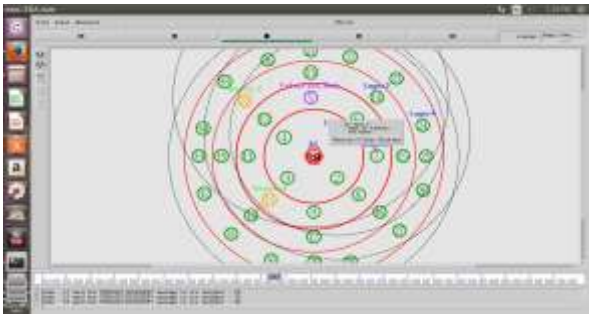

Figure 6 - WSN with Protocol Propagation in Each Layer

As shown in Figure 6, it is evident that the layers in the WSN are involved in the functioning of the network. The source nodes are labelled. The nodes that are sensing data and the nodes that are acting as source nodes demarcated besides showing protocol propagation.

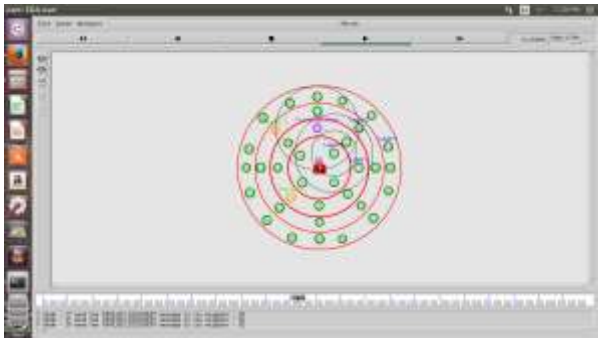

Figure 7 - Simulation of WSN with topology discovery

As shown in Figure 7, the simulation continued with the presence of different layers in the WSN. The layers spread from base station towards outside. The falsified node is labelled as 5. Through this node adversaries can launch false data injection attacks.

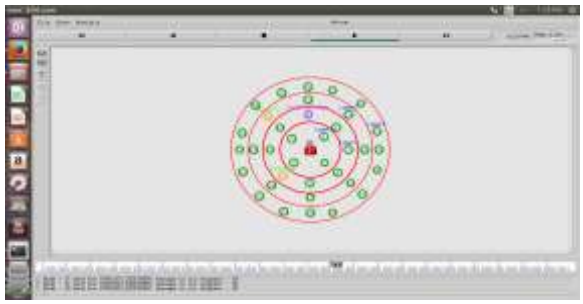

Figure 8 - Simulation Results Continued

As shown in Figure 8, there was communication among nodes such as node 17, node 19, node 29, node 30 and node 32.

Figure 9 - WSN Simulation Continues

As shown in Figure 9, there is protocol propagation and the attacks on the WSN for injecting falsified data are prevented to ensure secure data aggregation.

Figure 10 - Secure Data Aggregation Continues

As shown in Figure 10, secure data aggregation process continues to protect the WSN from attacks that can send falsified data to base station.

6. CONCLUSIONS AND FUTURE WORK

In this paper, the problem of secure data aggregation is studied in wireless sensor networks. It is understood that wireless sensor networks are vulnerable to various kinds of attacks including the attacks on the data aggregation. Attackers can inject false data into the network in order to have intended benefits. To overcome this problem many solutions came into existence. All the solutions focused on the secure data aggregation mechanisms. The existing iterative filtering algorithms were effective in secure data aggregation. However, they were not able to withstand collusion attacks. To overcome this problem an improved iterative filtering approach is followed to ensure that collusion attacks are addressed. Extensive simulations using NS2 revealed that the proposed solution is useful to have secure data aggregation in WSN.

REFERENCES

[1] Alemdar, H. and Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks.* 54, p2688–2710.

[2] Alzaid, H., Foo, E., Nieto, J. G. (2007). Secure Data Aggregation in Wireless Sensor Network: a Survey. Australian Computer Soceity, p1-13.

[3] Bhattacharya, D. (2014). Secure Data Aggregation in Wireless Sensor Networks. IJERA, 4 (4), p116-120.

[4] Castelluccia, C., Chan, A. C., Mykletun, E., and Tsudik, G. (2009). Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks. ACM Transactions on Sensor Networks, 5(3), p1-36.

[5] Frikken, K. B. and Dougherty IV, J. A. (2008). An Efficient Integrity-Preserving Scheme for Hierarchical Sensor Aggregation. *ACM*, p1-9.

[6] Huang, S., Shieh, S. and Tygar, J. D. (2010). Secure encrypted-data aggregation for wireless sensor networks. Wireless Networks, p1-13.

[7] Karlof, C., and Wanger, D.2003. Secure routing in wireless sensor networks: attacks and counter measures. Elsevier, Ad Hoc Networks, p1-23.

[8] Kevin Ashton. 2013. An Introduction to the Internet of Things (IoT). Lopez Research LLC,p1-6.

[9] Law, Y. W., Palaniswami, M., and Phan R. C. (2009). Secure Data Aggregation in Wireless Sensor Networks. Springer-Verlag, p1-27.

[10] Li, H., Lin, K. and Li, K. (2011). Energy Efficient and high security data aggregation in wireless sensor networks. Elsevier, Computer Communications, 34, p591-597.

[11] Maraiya, K., Kant, K. and Gupta, N. (2011). Wireless Sensor Network: A Review on Data Aggregation. IJSER, 2(4), p1-6.

[12] Nath, S., Yu, H. and Chan, H. (2009). Secure Outsourced Aggregation via One-way Chains. *ACM*, p1-14.

[13] Ozdemir, S. and Xiao, Y. (2011). Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. *Computer Networks*. 55, p1735–1746.

[14] Ozdemir, S. and Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. *Computer Networks*. 23, p2022–2037.

[15] Sriramoju Ajay, B. (2017). Intelligent mobile app for finding path and tracking post packets using android platform. International Journal of Research in Science & Engineering, 3(2), 9.

[16] Sriramoju Ajay, B. (2017). Investigation of Feasible Tourist Destinations using Android Mobile App. International Journal of Research in Science & Engineering, 3(2), 9.

[17] Babu, Sriramoju Ajay, and Namavaram Vijay. Image Tag Ranking for Efficient Matching and Retrieval. (2016).

[18] Babu, Sriramoju Ajay, and Namavaram Vijay. Design and Implementation of a Framework for Image Search Reranking. (2016).

[19] Babu, Sriramoju Ajay and Babu, S Shoban. International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020.

[20] Babu, Sriramoju Ajay. Particle swarm optimization algorithm for routing network. (2017).

[21] Babu, Sriramoju Ajay. Modification affine ciphers algorithm for cryptography password. (2017).

[22] Babu, Sriramoju Ajay. Perceptual-Based Quality Metrics for Image and Video Services. (2015).

[23] Sriramoju, Ajay Babu. Analysis on Image Compression Using Bit-Plane Separation Method. (2014).

[24] Babu, Sriramoju Ajay. Objective Quality Metric Design for Wireless Image and Video Communication. (2014).

[25] Ajay Babu Sriramoju, Dr. S. Shoban Babu. Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays for Image Processing. (2013).

[26] Sriramoju, Ajay Babu. Image Processing: Lossy Compression by Color Quantization and Gct Modeling. (2012).

[27] Sriramoju, Ajay Babu. Analysis on Lossless Image Compression in Image Processing. (2011).

[28] Padmavathi, Dr. G. and Shanmugapriya, Mrs. D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *(IJCSIS) International Journal of Computer Science and Information Security*. 4 (1), p1-9.

[29] Rani, G. R. and Srilakshmi, K. (2014). Secure Data Aggregation in Wireless Sensor Networks. IJETCSE, 9 (1), p1-4.

[30] Roy, S., Conti, M., Setia, S. and Jajodia S. (2012). Secure Data Aggregation in Wireless Sensor Networks. *IEEE* transactions on information forensics and security. 7 (3), p1-13.

[31] Sang, Y., Shen, H., Inoguchi, Y., Tan, Y. and Xiong, N. (2006). Secure Data Aggregation in Wireless Sensor Networks: A Survey. IEEE Confernece, p1-7.

[19] Shu, T., Liu, S. and Krunz, M. (2010). Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. *IEEE*, p1-5.

[32] Sicari, S., Grieco, L., Boggia, G. and Porisini, A. (2012). DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. *The Journal of Systems and Software*. 85, p152–166.

[33] Yu, H. (2011). Secure and highly-available aggregation queries in large-scale sensor networks via set sampling. *Springer.* 23, p373–394.