International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Data Aggregation Technique for Wireless Sensor Networks based on IF algorithm

Anagha Jagtap[1], M. D. Ingle[2]

[1]ME Computer (Engineering), Jayawantrao Sawant College of Engineering, Hadapsar, Pune-28, Savitribai Phule Pune University, Pune, India

[2] Professor, Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

Abstract: ***Wireless sensor Networks (WSN) comprises of sensor nodes which have the capability to sense and communicate. The capabilities of these nodes have certain limitations such as limited computational, memory and communication resources. These networks have huge application in military, disaster management and security. Due to limited resources it is very essential to curtail the amount of data transmission. One of the novel techniques in wireless sensor networks is data aggregation. This algorithm mainly focuses on enhancing the network lifetime by gathering and aggregating data in an energy efficient manner. The purpose of this survey is to present a critical overview of different data aggregating algorithm in wireless sensor network. Also discussed the advantages and limitations of various data aggregating algorithm and compared them. In wireless sensor network data aggregation is highly vulnerable to node compromising attacks. This paper focuses on different approaches used for the purpose of secure data aggregation and it's a variety of energy-efficient uses in wireless sensor network. Proposed work mainly concentrated on attacks on both cluster member as well as aggregator.***

Keywords: Wireless Sensor Networks, Data Aggregation, Trust, collusion attacks.

1. Introduction

Wireless sensor networks are usually comprises of thousands of low-cost, low-powered sensing devices with limited computational, memory and communication resources. WSN is called as a special class of ad hoc wireless network. Wireless sensor network contains several thousand of sensor nodes distributed in a target detecting environment within its neighbourhood, collects the data and computes it.

Sensor nodes are made up of simple processor, application specific sensors, wireless transceiver and low battery. Data aggregation is used due to limited amount of power in sensor nodes and to reduce transmission overhead. A variety of schemes for data aggregation are provided.

Data aggregation is a process in which data is been merged from multiple sensors at intermediate nodes and transmitting aggregated data to the base station. Data aggregation involves collection of critical data and makes data available to the base station in an energy efficient manner with minimum latency. Basically data aggregation protocols can be classified into two types based on the topology. They are tree based data aggregation protocols and cluster based data aggregation protocols. Group of nodes form a cluster. The grouping of these nodes into clusters is called clustering. In case of cluster based data aggregation protocols cluster head or aggregator performs data aggregation and in case of tree based data aggregation protocols the intermediate parent nodes near to the sink perform data aggregation.

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. Data aggregation is a commonly used technique in wireless sensor networks. The security issues, data confidentiality and integrity, in data aggregation become very important when the sensor network is deployed in an aggressive environment. Data aggregation is a phenomenon of aggregating the sensor data based on aggregation approaches.

2. Related Work

Y. Zhou, T. Lei, and T. Zhou [2] author proposed a reputation algorithm based on correlation to solve the ranking problem. As correlation is a efficiently describe the similarity between two vectors, we choose correlation coefficient to represent user's reputation and use iterative method to obtain the result step by step. Correlation based ranking algorithm has a good efficiency to avoid the spammers attack. The proposed algorithm has higher robustness to spammers attack.

K. Hoffman, D. Zage, and C. Nita-Rotaru [3] introduced an "Iterative Trust and Reputation Management Scheme" (ITRM). The proposed ITRM is a robust mechanism to evaluate the quality of the service. Proposed algorithm can be applied to centralized schemes where a central authority collects the reports and forms the reputations of the service providers as well as report trustworthiness of the consumers. Proposed work is a bipartite graph based motivated by the iterative decoding of low-density parity-check codes. In this paper author compare of ITRM with previous known reputation management techniques which provide better result in terms of both robustness and efficiency.

R.-H. Li, J. X. Yu, X. Huang, and H. Cheng Fung [4], in case of bipartite rating networks two types of entities are present called users and the objects, where users give ratings

to objects. Main challenge in bipartite rating networks is how to rank the objects based on user's ratings. Problem with the existing algorithms either cannot robust to the spammers attack or not guarantee convergence. Author proposed six new reputation-based ranking algorithms. Measurement of user's reputation is performed by the aggregated difference between the user's rating and the corresponding object's ranking. Proposed algorithms evaluated with three real datasets and the results confirm that these algorithms are effective, efficient, and robust.

H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, [5] to guarantee trustworthiness of sensor data in the presence of adversaries is challenging issue in wireless sensor network. Author developed novel and efficient a game theoretic defense strategy to protect sensor nodes from adversaries and to guarantee a trustworthiness for sensor data. They modeled the attack-defense interaction as a Stackelberg competition and provided two alternate utility and cost measures for the game. Proposed approach solution provides an effective and efficient way of assuring sensor data trustworthiness and protecting sensor networks from various malicious attacks. Author derives the Nash equilibrium condition that is sufficient for recommend trustworthiness of sensor data.

David Wagner [6], this paper shows how the spatial correlation can be exploited on the Medium Access Control (MAC) layer. Due to the spatial correlation between sensors nodes cause to undergo observed events, which may not be necessary for every sensor node to transmit its data. Paper proposed Spatial Correlation-Based Collaborative Medium Access Control in Wireless Sensor Networks which has two components: Event MAC (E-MAC) and Network MAC (N-MAC). E-MAC filters out the correlation in sensor records while N-MAC prioritizes the transmission of route-thru packets. CC-MAC provides high performance in terms packet drop rate, energy and latency. This paper considers only one type of phenomenon sensed by the sensor nodes. The quality of service requirement of various types of sensor information needs to be improved.

S. Ganeriwal, L. K. Balzano, and M. B. Srivastava [7], cryptography cannot prevent malicious or non-malicious insertion of data from internal adversaries or faulty nodes thus author proposed a framework, RFSN, for developing a community of trustworthy sensor nodes. By maintaining resource constraint author developed lightweight modular architecture of RFSN. For reputation representation, updates, integration and trust evolution author developed a beta reputation system for sensor networks (BRSN) that uses a Bayesian formulation under RFSN. By using RFSN achieves high integrity sensor networking systems. For counting all types of misbehavior resulting from malicious and faulty nodes in the system, RFSN provides a scalable, diverse and a generalized approach.

X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee [8], paper proposed technique called SensorRank by exploring Markov Chain in the network. The accuracy of query results in wireless sensor networks may be greatly affected when faulty readings are presented. A correlation network is developed to facilitate derivation of SensorRank for sensor nodes in the network. TrustVoting algorithm is developed to determine faulty readings in case of SensorRank.

3. Proposed Work

Existing system mainly concentrated on collusion attacks of cluster member in wireless sensor network. As data is outsourced through cluster member to aggregator to base station, if in case attack occurs on aggregator then existing system is fail. In proposed work, we consider attacks on both cluster member as well as aggregator.

4. Architectural View

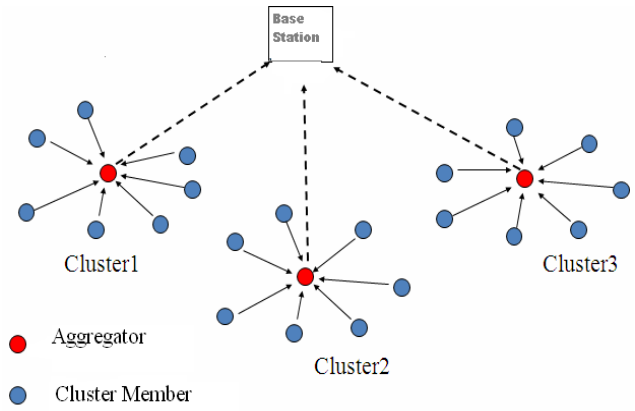

Figure 1: System Architecture

Sr.no	*Paper*	*Technique*	*Advantage*	*Disadvantage*
1	Robust Reputation-Based Ranking on Bipartite Rating Networks [4]	Author proposed six new reputation-based ranking algorithms. Measurement of user's reputation is performed by the aggregated difference between the user's rating and the corresponding object's ranking.	Complexity of proposed algorithms are linear with respect to the size of the graph, therefore they can be scalable to large datasets. These algorithms are effective, efficient, and robust.	Results confirm the effectiveness, efficiency, and robustness of proposed algorithms for only three datasets.
2	A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks [5]	Author developed novel and efficient a game theoretic defense strategy to protect sensor nodes from adversaries and to guarantee a trustworthiness for sensor data.	Proposed solution provides an effective and efficient way of assuring sensor data trustworthiness.	Defense model needs to be extend to the other scenarios
3	Spatial Correlation-Based Collaborative Medium Access Control in Wireless Sensor Networks [6]	Paper proposed Spatial Correlation-Based Collaborative Medium Access Control in Wireless Sensor Networks which has two components: Event MAC (E-MAC) and Network MAC (N-MAC).	CC-MAC provides high performance in terms packet drop rate, energy and latency	This paper considers only one type of phenomenon sensed by the sensor nodes. The qualities of service requirements of various types of sensor information need to be improved.
4.	Reputation-based Framework for High Integrity Sensor Networks[7]	Paper proposed a framework, RFSN, for developing a community of trustworthy sensor nodes	By using RFSN achieves high integrity sensor networking systems. RFSN provides a scalable, diverse and a generalized approach.	Maintain reputation only about neighboring nodes.
5.	Using Sensor Ranks for In-Network Detection of Faulty Readings in Wireless Sensor Networks [8]	Paper proposed technique called Sensor Rank by exploring Markov Chain in the network	Accuracy is improved and trust is increases.	Correlation factor consider only linear results.

5. Conclusion

This paper presented an all-inclusive survey of data aggregation algorithms in wireless sensor networks. All of them focus on optimizing important performance measures such as energy consumption, network lifetime, data latency and data accuracy. The main features, the advantages and disadvantages of each data aggregation algorithm are described. In proposed work, secure and robust data aggregation is perform in presence of collusion attacks which are available in wireless sensor network.
In proposed work, we consider attacks on both cluster member as well as aggregator.

References

[1] Mohsen Rezvani, Student Member, IEEE, Aleksandar Ignjatovic, Elisa Bertino, Fellow, IEEE, and Sanjay Jha, Senior Member, IEEE, " Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks ", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 1, JANUARY/FEBRUARY 2015.
[2] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.
[3] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.
[4] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.
[5] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A gametheoretic approach for high-assurance of data trustworthiness in sensor networks," in Proc. IEEE 28th Int. Conf. Data Eng., Apr. 2012, pp. 1192–1203
[6] M. C. Vuran and I. F. Akyildiz, "Spatial correlation-based collaborative medium access control in wireless sensor networks," IEEE/ ACM Trans. Netw., vol. 14, no. 2, pp. 316–329, Apr. 2006.
[7] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based framework for high integrity sensor networks," ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.
[8] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using SensorRanks for in-network detection of faulty readings in wireless sensor networks," in Proc. 6th ACM Int. Workshop Data Eng. Wireless Mobile Access, 2007, pp. 1–8..
[9] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw, vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
[10] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,

Author Profile

Ms. Anagha M. Jagtap, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune

University, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from Trinity college of engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. Her area of interest is network security, WSN.

Prof. M.D Ingle, received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad-402103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security and WSN.