International Journal of Scientific Research in Computer Science and Engineering **Review Paper**
Vol.4, Issue.3, pp.26-29, June (2016) **E-ISSN:**2320-7639

An Efficient Approach for Secure Data Aggregation Method in Wireless Sensor Networks with the impact of Collusion Attacks

U. Korupolu[1*], S. Kartik[2], G.K. Chakravarthi[3]

[1]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam - India
[1]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam - India

Corresponding Author: korupoluuma@gmail.com

Available online at www.isroset.org

Received: 10 May 2016, Revised: 25 May 2016, Accepted: 18 Jun 2016, Published: 30 Jun 2016

Abstract— The basic component in wireless sensor networks (WSNs) is represented by the nodes. The sensor node consumes energy during sensing, processing and transmission. The aggregation of data from multiple sensor nodes which is done at the aggregating node is to be performed by simple method such as averaging. In Wireless sensor network power and energy resources are limited. In this paper the monitoring system and READA technique will be used. The number of sensor nodes can detect simultaneously a single target of interest. Redundant and correlated data are collected. If every node sends data to the base station, energy will be wasted and due to that the network energy will be consume quickly. Redundancy Elimination for Accurate Data Aggregation (READA) uses a grouping and compression mechanism to remove duplicate data in the aggregated set of data to be sent to the base station without losing large accuracy of the final aggregated data. In wireless sensor network, security and energy efficiency issues are found.

Keywords- Wireless Sensor Networks; Network Lifetime; Collision attack; Data Aggregation techniques

I. INTRODUCTION

Wireless sensor networks are mainly redundant they are composed of nodes with the capacity of sensing, communication and computation. It is necessary to define the capability of computing due to limitations of the energy resource and computing power in sensor nodes, data is aggregated significantly by simple technique such as averaging and transporting special functions of sensor measured to the sink node. Network aggregation plays a very important role in enlarging such capacity for wireless sensing network. The aggregation technique is to be used to aggregate the sensor data completely. This approach enhances the network lifetime by associating and aggregating the data in and for robustness of monitoring and minimum cost of the nodes, wireless sensor networks are usually redundant very adequate manner. The paper is organized as follows. Various strategies and techniques that are available for the lifetime maximization are been given. It also described about the advantages and the disadvantages related with all these solutions.

Lastly it proposes a new system using READA algorithm for scrutinize the network lifetime. A data aggregation framework on WSN's is presented and a survey on various energy-efficient mechanism for data aggregation.

II. RELATED WORK

Data packets can be across particular organizational, information domains or security in order to be the results delivered and handled. These calls for a systematic organizational design way technique which include means to secure data transfer or receive. The various facts of secure information exchange are already being tackled by many researches. Data aggregation is done by using the following techniques.

A. Iterative Filtering Reputation Systems

This algorithm is used to reduce the energy consumption in an efficient manner. So that, It resolves the problem of the data aggregation. The literature on the iterative filtering has been increased rapidly per day. The aggregation algorithm is used to detect and avoid from various attacks.

B. Concealed Data Aggregation Technique

Concealed Data Aggregation places more strength on passive attacks. These are considered if adversaries can eavesdrop the communications on the air. After CDA, to attain higher security levels thriving research has been suggested. If sensors within the similar cluster encrypt their sensing data with a same secret key, by arranging only one sensor an adversary may decrypt the aggregated cipher text. Addition homomorphism public-key encryption suggested a data aggregation scheme. It looks like more secure since every sensor stores only the public key protecting secure aggregation is a challenging task.

C. EPSDA Protocol

To prevent the replay attack by concluding data freshness during aggregation using ESPDA protocol, this performs the aggregation on encrypted data and reduced number of transmissions; this increases the accuracy certainly of the aggregated result.

D. Scaling Laws and Block coding and Parallel scheme

Scaling laws of the aggregation capacity for wireless sensing network. The significant advantage of researching scaling laws is to overview the qualitative and architectural properties of the system without getting bogged down by too whole details. The potential scaling laws of a network are directly intend by the adopted network models, including delivery models, scaling models and transmission models, a part from the pattern of traffic sessions.

E. Energy efficient routing protocol and EERDAT:

For WSN's EERDAT technique is dependable and energy efficient. This approach is based on cluster formation technique. To decrease the energy consumption can be adequately measures the lost data in nodes in cluster. By using a coordinate node reliable communication can be given. The above literature analysis shows pros and cons of various protocols and methodologies. They will transmit the data to the base station. This paper uses a new data aggregation strategy called “READA”.

F. Collusion attack scenario:

Most of the IF algorithms involve simple assumptions about the initial values of weights for the sensors. In case of our opponent model, an attacker is able to mislead the aggregation system from side to side cautious range of report data standards. Consider that ten sensors report the values of temperature which are aggregated using the IF algorithm planned in with the reciprocal discriminated function. » In scenario 1, all sensors are dependable and the result of the IF algorithm is nearer to the actual value. » In scenario 2, an suggested method compromises two sensor nodes, and bothers the readings of these values such average of all sensor readings is skewed towards a lesser value. As these two sensor nodes report a lower value, lower weights are hand over to them by IF algorithm, because their values are far from the values of other sensors. Particularly, the algorithm is robust against the false data injection in this scenario because the compromised nodes individually falsify the readings without any knowledge about the aggregation algorithm. The algorithm hand over very low weights to these two sensor nodes and therefore their contributions decrease. In scenario 3, in order to propel a collusion attack an adversary employs three compromised nodes. It listens to the reports of sensors in the network and guides the two compromised sensor nodes to report values far from the true value of the measured quantity. It then guides the skewed value of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings.

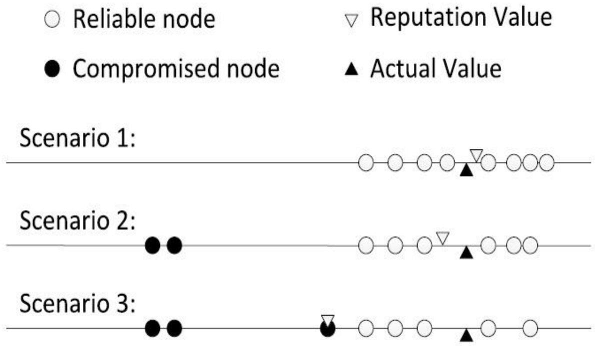

Figure 1. Collusion attack scenario against IF algorithm

III. PROPLEM DEFINITION

In wireless sensor networking (WSN), instantly upon the environment the sensed nodes are created, which transfer the collected data to the base station.

1. When the data in the wireless sensor network are reciprocal, multiple number of nodes available, report almost similar readings to the base station.

2. When millions of redundant data are transmitted a very huge amount of energy is wasted.

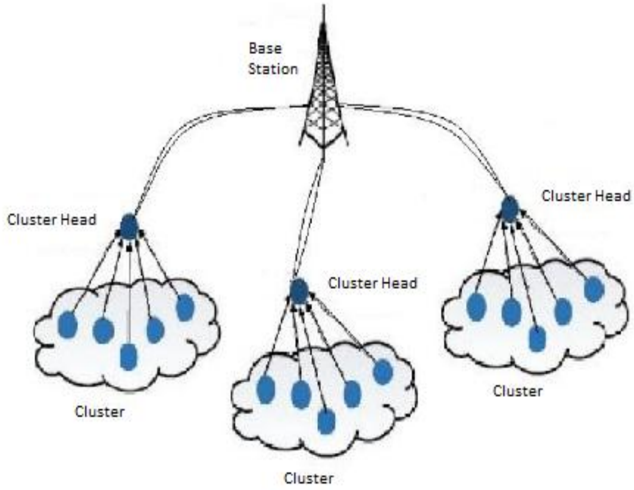

Figure 2. Network Model for WSN

The figure 2 shows that supposition for network model in wireless sensor network. The sensor nodes used in clusters and every cluster has a cluster head these acts as an aggregator. Data are systematically collected and generated by the aggregator. Thus, we provide a through empirical evaluation of the effectiveness and efficiency of our suggested aggregation using this method. The result shows that our methodology provides both better accuracy and higher collusion protection than the previous methods.

IV. Proposed System

Working READA technique Network lifetime of WSN's is increase by following way: For the suggested aggregation technique, the nodes will be organized in clusters and one of them is work contribute cluster head. Then after that each cluster head is connect to the base station in aggregation technique. They will send the data to the base station. In this paper we use a new data aggregation technique called "Redundancy Elimination for Accurate Data Aggregation". (READA).

A. Data Aggregation

Aggregation technique will be performed by a few ways that is monitoring system and event detection. In READA approach aggregation will be manipulated by two ways that is monitoring system and event detection. First of all the observing system is used to search the sensor nodes. In this way two approaches will be used that is one of the compression and another grouping. For prediction data grouping approach is to be used. Sensor nodes with the identical profile and having a conveniently "small" scale factor are grouped to form new sensor nodes. By this way the number of nodes can be reduced in linear time. The elevator is making from grouping expression. It first selects the elevator rather of transferring a single data that transmit the group of compressed data. Event detection approach continuously monitoring the nodes and report an unused node.

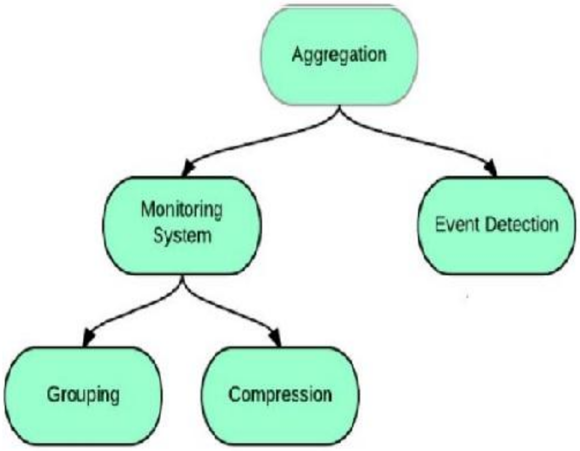

Figure 3. Working Principle of Data Aggregation

The working principal of WSN's approach suggested architectural model illustrated below figure 4 that starts working together choosing and selecting of nodes and divided into clusters. These clusters can satisfy the intended parameter conditions and requirements. The parameters like RSSI, MRIC, bandwidth, TTL, battery consumption are addicted verify the amount of nodes that will be entertained in a cluster. There after a cluster head [CH] is selected among nodes exist within the every cluster. Cluster head are going to be responsible for administration of all different nodes within the several clusters and grouping the data from the nodes within the cluster and information transferring to the neighbouring cluster head for large amount of information updating and exchange.

The currently appeared nodes will be assigned as cluster head if the global cost of arrived node is reduced, else other cluster nodes are going to be give convenience to global and participate cost is once more calculated. There after the data aggregation approach is presumed as the collection of data and numerous problems defines from the user end are checked and sends into minimum level schemes by a query processor. Data are aggregate and collected is stored at a storage location to the database server. Lastly at last the data is aggregated by data cube approach and each and every one the grouped data are going to be transfer to the base station.

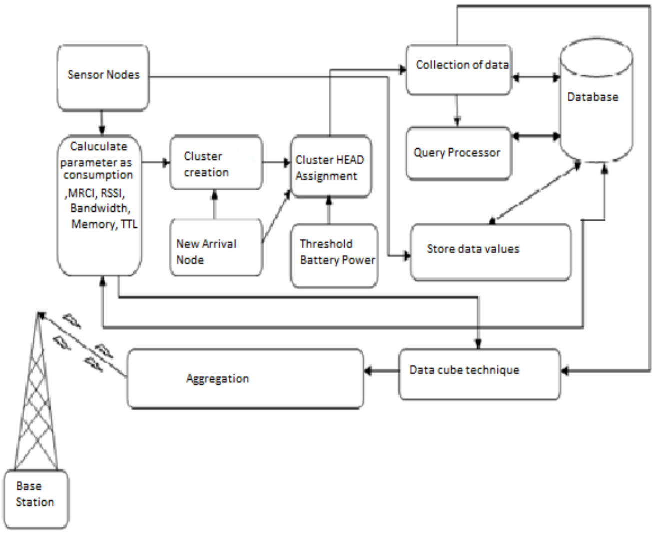

Figure 4. Architecture of Data Collection and aggregation for WSN

V. Conclusion

This paper describes about various techniques and strategies used for lifetime maximization of WSN. Thus considering those factors a new technique READA is to be introduced. READA is used for large Data Aggregation Techniques of Wireless Sensor Network Increasing Network Lifetime and sensor networks lifetime maximization scheme for reducing the power and increasing the lifetime. To produce a compromised but accurate aggregate data the grouping and compression technique is to be used.

REFERENCES

[1]. P. saini, M. Sharma, *"Impact of Multimedia Traffic on Routing Protocols in MANET"*, IJSR in Network Security and Communication, Vol.3, Issue.3, pp.1-5, 2015,

[2]. L. Pal, P. Sharma, N. Kaurav, S.L. Mewada, "*Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.5, pp.1-4,2013.

[3]. R. Nathiya, S.G. Santhi, "*Energy Efficient Routing with Mobile Collector in Wireless Sensor Networks (WSNs)*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.2, pp.36-43, 2014.

[4]. H. Singh, *"Randomly Generated Algorithms and Dynamic Connections*", International Journal of Scientific Research in Network Security and Communication, Vol.2, Issue.1, pp.1-4, 2014.

[5]. O. Hiteshreddy, P. Singh, S. Chahuan, "*A Review on Cluster Based Data Aggregation Protocols in Wireless Sensor Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.8, pp.37-45, 2015.

[6]. D. Tamrakar, S. Bhattacharya, S. Jain, *"A Scheme to Eliminate Redundant Rebroadcast and Reduce Transmission Delay Using Binary Exponential Algorithm in Ad-Hoc Wireless Networks"*, International Journal of Scientific Research in Network Security and Communication, Vol.2, Issue.2, 1-5, 2014.

[7]. Md.A. Mushtaque, "*Comparative Analysis on Different parameters of Encryption Algorithms for Information Security*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.4, pp.76-82, 2014.

[8]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, *"Electron spectroscopy studies on magneto-optical media and plastic substrate interface,"* IEEE Translation Journal on Magnetics in Japan, Vol. 2, Issue.8, pp.740–741, 1987.

[9]. R. Sharma, Heena Das, S.N. Das, "*WSN for Computerized Irrigation System in Tea Gardens*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.2, pp.26-30, 2016.