Jestr

Journal of Engineering Science and Technology Review 10 (2) (2017) 75- 79

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Secure Data Aggregation for Wireless Sensor Networks using Double Cluster Head Approach

A.L.Sreenivasulu* and P.Chenna Reddy

Dept of Computer Science & Engineering, JNTUA, Anantapuramu

Received 24 August 2016; Accepted 28 February 2017

Abstract

In Wireless Sensor Networks (WSNs), data aggregation is defined as the method of acquiring sensed data from neighboring nodes and merged to send data to the base station. It is required to manage the limited in-network processing and storage capacity of nodes in the aggregation process with collaborative computing and also secure communication aspects. In this paper, double cluster head based secure aggregation method (DCSDA) is proposed. The method is more suitable for the cluster based communication strategy with security as a primary requirement with privacy and authentication. The experimental evaluation shows the performance of the DCSDA approach in terms of packet drop ratio, delay and energy consumption. The results proved the effectiveness of the DCSCA approach.

Keywords: cluster, sensor node, WSN, security, Data aggregation

1. Introduction

WSNs is a group of inexpensive and autonomous sensor nodes interconnected and work together to monitor various environmental conditions such as humidity, temperature, pressure, and other climate changes. Wireless sensor nodes are randomly installed and communicate themselves through the wireless communication medium. It has few restrictions like limited energy, storage and processing capabilities and has the probability for physical damages in hostile environments. The design of sensor network may differ as per application requirement. The sensed data is shared among the multiple sensor nodes to an identified sink and follows many to one approach in the communication process.

The deployment of a large quantity of sensor nodes is complex and produces more traffic. The clustering mechanism is required to minimize the complexity in the communication process and base stations needs to be deployed in every cluster and this process is called cell splitting. Reduction of the cell size gives the flexibility to manage more traffic. A cluster incurs less communication over head in the routing process from sensor nodes with in the cluster to cluster head (CH) and from CH to base station. In the clustering approach, the sensor nodes with in the network are grouped in to the clusters based on the CH node selection. Every CH from the cluster receives and aggregates the data from the sensor nodes and forwards to the base station.

The basic advantages in this approach are primarily on limiting the long distance communication and energy optimization. A few properties of clusters include count of clusters; stability and topology of internal cluster and external inter cluster communication. The CH selection is a crucial problem and the network life time is dependent on it. In this paper, double cluster head based data aggregation method is proposed with security integrated to achieve the maximum efficiency of the network..

The organization of the paper is as follows: Section 2 explains about the Literature review about clustering and security. Section 3 deals with problem description and DCSCA approach. Section 4 explains about the simulation environment and the results evaluation of proposed method. Finally, conclusion with possible future enhancements is drawn in Section 5.

2. Literature Survey

Data aggregation is playing a crucial role in WSN research. Extensive study about the data aggregation and security with other possible aspects like energy optimization and load balancing are given in the literature. The data precision is treated as the crucial aspect in measuring the performance of data aggregation. In [1-2], the tradeoff between energy and QoS parameters in the data aggregation process was described. Data aggregation delay minimization methods studied by the authors [3-5] and energy factors affecting the data aggregation further discussed with various constraints [6-7].

The authors [8] proposed a new clustering approach for hierarchical structure to the multi-hop communication. The process is represented with a connected graph of vertices. The renowned research problem is conflict in In-network data aggregation [9-12] and data privacy protection [13-15]. Within the network, each sensor node act as a data aggregator and collects the data from the other neighboring nodes. This process hugely reduces the burden over CH nodes and Base station, but in this process every sensor node must have access to the data items that they are operating with. It may lead to fail in the privacy preserving of data from nodes. Data can be encrypted by applying the cipher

*E-mail address: intellseenu@gmail.com

text [12-15] but these methods works only by summation and average, but not considering the median or min/max procedures.

In [16-17], to allow the aggregation of data, the protocols followed the symmetric and asymmetric encryption. One of the methods [17] works on asymmetric key homomorphism to manage the data aggregation. S. Roy et al [20] proposed a synopsis diffusion approach to address the false sub-aggregate values attack. The proposed algorithm compromises the base station to compute the predicate sum securely and filters the malicious nodes from the hierarchy. Wireless sensor networks are compromised with the number of sensor nodes and those sensor nodes are constrained with computation, communication and memory. There is a need for efficient data processing to support the WSNs. Liu et al., [21] proposed a method for privacy preserving data aggregation. This method also considers the factor of reducing energy consumption. This scheme achieved high data accuracy and less overhead with effective privacy preservation. Villas et al., [22] proposed a light weight routing approach to the data aggregation in WSNs. The Data routing in network aggregation (DRINA) approach reduces the communication cost by aggregating the redundant data at intermediate nodes. The performance of the DRINA is compared with the InFRA and SFT algorithms. They claimed that the DRINA has superior performance in terms of data aggregation when compared to the InFRA and SFT. Yu Yanli et al., [23] discussed several countermeasures and different attacks of the trust method in WSNs. They summarised the challenges of trust models in WSNs and trust models are classified in to secure data and secure routing. WSN is a combination of thousands of nodes and it is very important to identify the spatially correlated and redundant data by the neighbouring nodes and this type of practices leads to the minimization of energy.

Villas et al., [24] considered the spatial correlation aware routing method (YEAST) for data aggregation in WSNs. YEAST has the special mechanism to identify the redundant data and aggregates the data at intermediate nodes and also it reduced the energy utilization of the network. In WSNs, data aggregation is the efficient mechanism to decrease the network overhead and to improve the network lifetime. But, some malicious nodes pose false values at the time of data aggregation. To address the issues, Li et al., [25] proposed the energy efficient and secure mechanism for data aggregation. The proposed mechanism identified the malicious nodes at the base station by comparing the constant value of the node with network overhead value. The proposed method considered the key based encryption method for data aggregation in WSNs. Many algorithms were proposed by the researchers to support the privacy preserving and data aggregation for WSNs. But, due to communication cost, computation capacity and memory of the sensor nodes, the algorithm doesn't completely solve the privacy preserving issue. Yoon et al., [26] proposed signature based data aggregation scheme for managing the security at the time of data aggregation in WSNs. The proposed scheme utilized the complex numbers to achieve data integrity and privacy checking in sensor nodes. The authors claimed that the proposed method achieved 50 % more communication over the existing methods. Zhou et al., [27] proposed homomorphic scheme for secure communication (SDA-HP) in WSNs. This scheme applied the symmetric encryption for the homomorphic data and secures the data privacy for WSNs.

3. Proposed Method

Few problems are identified in the literature, such as communication overhead, complexity, security and higher energy consumption. An aggregation process is defined as the process of compressing the sensed data from various autonomous nodes by applying minimum, maximum, average and other functions. The data aggregation will lead to the reduction in energy consumption. Accuracy, Completeness, Message overhead and Latency are considered as efficiency calculation parameters and they show great impact on the network lifetime.

In various data aggregation sessions, the cluster head (CH) and Co-Cluster Head (CCH) passes instructions to the sensor nodes to forward their data sets. The CCH performs the aggregation process and passes to the CH. The CH directly communicates to the base station. The total duration of the sessions for aggregation is identified based on the buffer capacity of sensor nodes and reading capability.

Double cluster head aggregation approach considers the two nodes as CH and CCH, by taking various factors into consideration like minimum distance, residual energy and nodes lifetime.

3.1 Key Management

A unique secret key K_i is shared during the deployment of the network, among the sensor nodes to communicate with the base station. Base station stores the record of secret keys shared among the sensor nodes, and there is no probability for attackers to get a secret key. However, there is a problem if any sensor node got compromised. In this process pseudo random number generation approach provides the privacy to the sensor nodes and base station [18]. In each aggregation session, the sensor nodes synchronize the random number as specified in [18].

Algorithm 1: Secure Key Generation

1. Cluster Head CH broadcasts R_{req}
2. Each sensor node floods the request to all neighbor nodes.
3. Each node compares the hop count and send R_{rep} in reverse path.
4. CH will identify the key tree and identifies the Co-Cluster Head as in algorithm 2.
5. Cluster key K_c, secret key K_s are generated for secure transmission.
6. CH unicasts the secret keys to CCH.
7. CCH identifies the nodes and unicasts the keys to its cluster slice.
8. The generation source should be taken from the base station.
9. During the update process, the CH needs to contact the BS for re retrieving of source.
10. CH will remove all entries from source

3.2 Residual Energy and Node Degree:

The Energy of a sensor node after performing one transaction is a subtraction of normal energy of node to one pair of operations. The pair can be transmission and reception of data. The residual energy R_e is given in equation 1.

$$R_e = I_e - \left(T_e + X_e\right) \quad (1)$$

Where, I is the initial energy of the node at the starting point and T and X denoted as transmission of data and reception of the data.

Node degree is calculated using the number of neighbor nodes and transmission range of nodes in a cluster. That operation can be represented

$$Node\ Degree = N\_Deg / \pi X\delta \quad (2)$$

Where δ is a communication range. The transmission range is calculated based on the antenna characteristics

$$\delta = \frac{T_{power}}{P_{porer}} G_t G_r h_t^2 h_r^2 \quad (3)$$

Where, T and R represent the transmission power and receiving power. Gain and height of the antenna from ground level is denoted with G and h with respect to transmission and receiving constraints.

Algorithm 2: Selection of Co-Cluster Head

1. As an initial step, identify the sensor nodes of the cluster by selecting the cluster head (CH)
2. Divide the cluster nodes to two sets C_i and C_j.
3. Choose the weight index value of the cluster members by considering history at T_0
4. Let choose the co-cluster head (CCH) by the CH for C_j based on index.
5. Assign CCH as a CH to the far nodes, such as C_j.
6. CH by default acts as a Head for C_i.
7. CCH aggregates the data from C_j and forwards to the CH.
8. The final aggregated data from $C_i + C_j$ is transmitted to the base station by CH.

4. Result Analysis

The simulation of the proposed DCSDA approach is carried out using the NS2 simulator. In the simulation process, 100 nodes are deployed with in the region of 1000 m X 1000 m. The time period for the simulation process is taken as 200 seconds. The traffic pattern is chosen as the constant bit rate (CBR) and each node having the transmission area of 250 meters. The performance is calculated for Delay, Packet Delivery Ratio and energy consumption. The proposed method is compared with SMART [19] by considering overhead, accuracy in aggregation and energy consumption.

Average end to end delay is calculated as the average total time required for sending the data to the destination node. Energy consumption is defined as the total average amount of energy required to send and receive and forward the packets to the destination. Average Packet Drop ratio is calculated as the total average of packet drops at the receiving nodes.

Table 1. Simulation Parameters

Simulation Area	1000m x 1000m
Node Count	100
Simulation Time	200 Sec
Traffic Type	CBR
Packet Size	512 Bytes
Transmission range	250m
Transmission energy	0.6 J
Receiving energy	0.3 J
Initial Energy	25.1 J
Antenna	Omni Directional
Number of Attackers	20

Communication overhead is greatly reduced in the proposed model while deploying more number of nodes. With double cluster heads, the aggregation process obtains better results in high density sensor network. Figure 1 shows the communication overhead scenario, the proposed method highly optimizes the communication cost at greater extent.

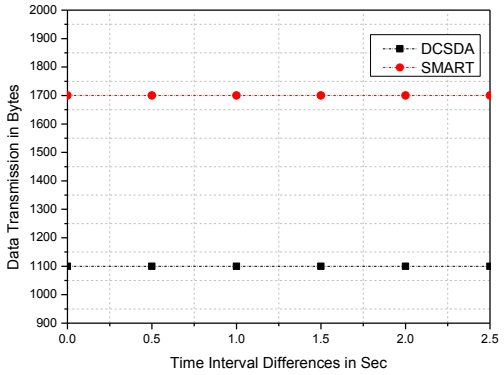

Fig. 1. Communication overhead over the various time intervals

Figure 2 depicts the packet delivery ratio with different number of nodes (i.e., from 100 to 500) with different data rates. The proposed method is more efficient and obtaining around 40 percent higher packet delivery ratio than the existing approach.

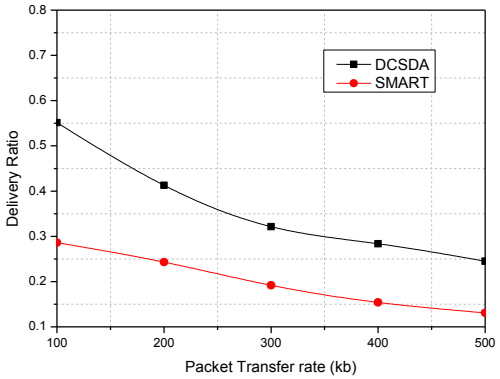

Fig. 2. Packet Transfer Rate vs. Delivery Ratio

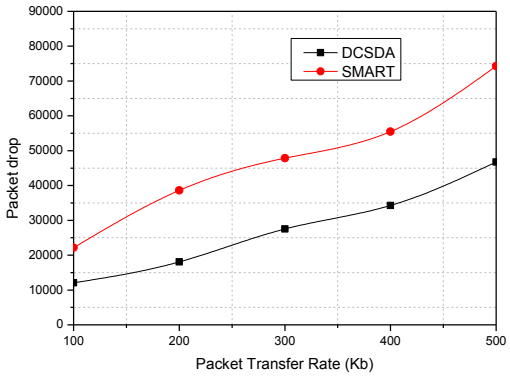

Fig. 3. Packet Transfer Rate vs. Packet Drop

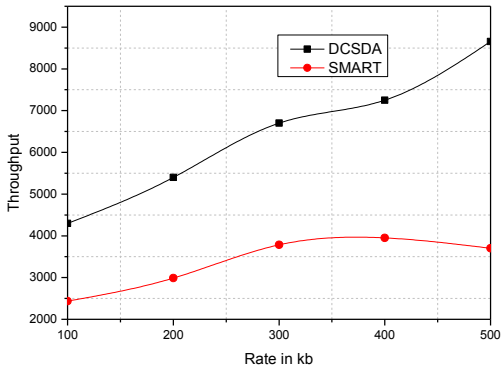

Fig. 4. Packet transfer rate Vs Throughput

Figure 3 is a comparison between packet transfer rate and drop count. The proposed method has recorded the 30% less packet drop count when compared to the existing method. Figure 4 shows the ratio between packet transfer rate and throughput. It is 40% more efficient than the SMART method.

5. Conclusion

In this paper, we present the double cluster head secure data aggregation model, which follows the structure of the cluster but it is constructed with two cluster heads main cluster head and co cluster head. This mechanism helps to reduce the overhead of the network and provides considerable security. The efficiency is calculated based on delay, delivery ratio, drop and throughput and outperforms the existing method. The proposed aggregation technique improves the lifetime of the network by making the energy optimization at sink and at individual sensor nodes.

References

1. T. Pham, E.J. Kim, M. Moh, On data aggregation quality and energy efficiency of wireless sensor network protocols-extended summary, in: IEEE First International Conference on Broadband Networks, 2004, pp. 730–732.
2. J. Zhu, S. Papavassiliou, J. Yang, Adaptive localized QoS-constrained data aggregation and processing in distributed sensor networks, IEEE Trans. Parall. Distrib. Syst. 17 (9) (2006) 923–933.
3. S. Xiao, J. Huang, L. Pan, Y. Cheng, J. Liu, On centralized and distributed algorithms for minimizing data aggregation time in duty-cycled wireless sensor networks, Wireless Netw. 20 (7) (2014) 1727–1741.
4. P. Wang, Y. He, L. Huang, Near optimal scheduling of data aggregation in wireless sensor networks, Ad Hoc Netw. 11 (4) (2013) 1287–1296.
5. H. Li, C. Wu, Q.-S. Hua, F. Lau, Latency-minimizing data aggregation in wireless sensor networks under physical interference model, Ad Hoc Netw. 12 (2014) 52–68.
6. I. Tan, Power efficient data gathering and aggregation in wireless sensor networks, ACM Sigmod Record 32 (4) (2003) 66–71.
7. R.R. Rout, S.K. Ghosh, Adaptive data aggregation and energy efficiency using network coding in a clustered wireless sensor network: an analytical approach, Comput. Commun. 40 (0) (2014) 65–75.
8. S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Anchorage, AK, 2001, pp. 1028-1037 vol.2.
9. S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," in SIGOPS Oper. Syst. Rev., vol. 36, no. SI, 2002.
10. S. Nath, P. B. Gibbons, S. Seshan, and Z. R. Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks," in ACM SenSys, 2004.
11. K.-W. Fan, S. Liu, and P. Sinha, "On the potential of structure-free data aggregation in sensor networks," in IEEE INFOCOM, 2006.
12. P. Jadia and A. Mathuria, "Efficient secure aggregation in sensor networks," in High Performance Computing, vol. 3296, 2004.
13. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks," in IEEE INFOCOM, 2007.
14. J. Girao, D. Westhoff, and M. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," in IEEE ICC, 2005.
15. C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in MobiQuitous, 2005.
16. Westhoff D, Girao J, Acharya M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution and routing adaptation. IEEE ransactions on Mobile Computing 2006; 5(10): 1417–1431.
17. Ozdemir S. Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism, In Proceedings of ICPS'07 : IEEE International Conference on Pervasive Services, Istanbul, Turkey, 2007; 165–168.
18. Seetharam D, Rhee S. An efficient pseudo random number generator for low-power sensor networks, In Proceedings of 29th Annual IEEE International Conference on Local Computer Networks, Tampa, Florida, USA, 2004; 560–562.
19. Li, H., Lin, K., & Li, K. (2011). Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Computer Communications, 34, 591–597.
20. S. Roy, M. Conti, S. Setia and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact,"

in IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681-694, April 2014.

21. Liu, Chen‐Xu, et al. "High energy‐efficient and privacy‐preserving secure data aggregation for wireless sensor networks." International Journal of Communication Systems 26.3 (2013): 380-394.
22. Villas, L. A., Boukerche, A., Ramos, H. S., de Oliveira, H. A. F., de Araujo, R. B., & Loureiro, A. A. F. (2013). DRINA: a lightweight and reliable routing approach for in-network aggregation in wireless sensor networks. IEEE Transactions on Computers, 62(4), 676-689.
23. Yu, Yanli, et al. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." Journal of Network and computer Applications 35.3 (2012): 867-880.
24. Villas, Leandro A., et al. "A spatial correlation aware algorithm to perform efficient data collection in wireless sensor networks." Ad Hoc Networks 12 (2014): 69-85.
25. Li, Hongjuan, et al. "Secure and energy-efficient data aggregation with malicious aggregator identification in wireless sensor networks." Future Generation Computer Systems 37 (2014): 108-116.
26. Yoon, Min, et al. "A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks." International Journal of Distributed Sensor Networks 2014 (2014).
27. Zhou, Qiang, Geng Yang, and Liwen He. "An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks."International Journal of Distributed Sensor Networks 2014 (2014).