ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A Survey on Secure and Energy Efficient Data Aggregation for Wireless Sensor Networks

C.Priyadarsini[1], Dr.R.Prema[2]

Research Scholar, Department of ECS, Karpagam University, Coimbatore, Tamil Nadu, India[1]

Associate Professor, Department of ECS, Karpagam University, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) consist of a large number of sensor devices which use battery powered energy. More energy is wasted while sensing the information and transmitting the data. To save energy in WSNs data aggregation technique is used. It could cause some security problems since false may be injected during data aggregation by data aggregator. We focus on data aggregation problems in security and energy constrained in sensor networks. In this paper, we present a survey of secure data aggregation algorithms in wireless sensor networks. We compare different algorithms on the basis of performance, security and energy efficiency and propose directions for future research in the area.

KEYWORDS: Wireless Sensor Networks (WSNs), data aggregation, Security.

I. INTRODUCTION

Wireless Sensor Network consists of numerous tiny sensor devices that deployed over a geographical area and it senses environmental conditions, sensor nodes communicate among themselves and also to an external sink or a base-station. The sensors coordinate among themselves to form a network and it collects data about environment after collecting it, they process it and then send to the base station through other intermediate nodes [2,3]. Depending upon the purpose of each application, sensor node senses different kinds of data. A sensor node mostly depends on the battery power, which gets depleted fast due to the computation and communication operation. Sensing the field and uploading data are the two major tasks to consume more energy by data sink [5,7]. Energy consumption depends on the sampling rate which is relatively stable. te. On the other hand, the energy consumption on data uploading is non uniform among most of sensors. It strongly depends on the network topology and location of the destined data sink. As a result, the energy of the sensors near the base station is depleted much sooner than others sensors since these sensors need to relay much more packets from the sensors far away from the sink [7]. A major technical challenge for WSNs is the node energy constraint and its limited computing energy, which may cause a fundamental limit on the network lifetime. Therefore, innovative technique to eliminate energy inefficiencies and to shorten the lifetime of the network is highly needed [8, 9]. Due to this, to save energy WSN use data aggregation technique. Data aggregation is a technique widely used because it reduces the number of messages transmitted in the network, and therefore reduces energy consumption and improves the life of the network [10].

II. THEORETICAL BACKGROUND AND RELATED WORK

Data Aggregation Technique

Data from sensor nodes are correlated in terms of time and space, transmitting only the required and partially processed data. The required data should be efficient than sending a large amount of raw data. The duplicated messages sent to the same node and neighbouring nodes waste energy, if two nodes share the same observing region. Thus, data aggregation aggregates data progressively as it is passed through a network. The data packet size, the number of data transmissions and the number of sensor nodes involved in collecting data from WSN can reduced by using In-network data aggregation.

The main concept of the data aggregation and in-network processing approaches are to combine the data arriving from different sources at certain aggregation points. Simple processing at the aggregation points eliminates

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

redundancies. The minimize the total amount of data transmission before forwarding data to the external BS. Removing redundancies results in transmitting less number of bits, and hence reduces energy consumption and increases the sensor nodes lifetimes [11].

Data aggregation significantly reduces the amount of communication and energy consumption. Because data from sensor nodes are correlated depends on the terms of time and space, transmitting only the required and partially processed data is efficient than sending a large amount of unnecessary data. In general, sending raw data wastes energy because duplicated messages are sent to the same node and neighbouring nodes receive duplicate messages if two nodes share the same observing region. In-network aggregation, which aggregates data and it is passed through a network. In-network data, aggregation reduce data packet size, the number of data and the number of nodes involved in gathering data from a WSN. Communication between nodes the most dominating factor for consuming precious energy of wireless sensor networks i.e., transmitting and receiving messages. WSNs lifetime is enhanced by reducing unnecessary traffic. In addition, involving as many sensor nodes during data collections utilize maximum resources of every sensor node by the sink nodes. As a result, the sensor nodes closer to the sink run out of energy sooner than other nodes and the network loses its service ability, regardless of a large amount of residual energy of the other sensor nodes.

III. SECURE DATA AGGREGATION IN WSN

A. Iterative filtering algorithm [1].

Due to the limited computational power and energy resources, aggregation of data from more number of sensor nodes done at the aggregating node is usually accomplished averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in the form of corresponding weight factors assigned to data provided by each source. Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve problems such as data aggregation and data trustworthiness assessment by using a single iterative procedure [8]. Iterative Filtering algorithms provide an initial approximation of the trustworthiness of sensor nodes which makes the algorithm not only collusion robust, but also more accurate and faster converging.

B. Continuous aggregation Scheme [2]

Continuous aggregation is usually required in many sensor applications to obtain the temporal variation information of aggregates. This scheme greatly reduces the verification cost by checking only a small part of aggregation results to verify the correctness of the temporal variation patterns in a time window. A sampling-based approach is used to check the aggregation results, it also proposes a series of security mechanisms to protect the sampling process. It produces an efficient scheme to detect false temporal variation patterns in a continuous aggregation. This continuous aggregation scheme verifies the correctness of the observed temporal variation pattern in a time window by checking only a small part of aggregation results termed as representative points. It defines representative points and proposes corresponding algorithms for representative point selection. By exploiting the spatial correlation among the sensor readings in close proximity, a series of security mechanisms are also proposed to protect the sampling procedure.

C. Attack resilient computation algorithms [3]

A loss-resilient aggregation framework called synopsis diffusion, which uses duplicate insensitive algorithms on top of multipath routing schemes to accurately compute aggregate. The attack-resilient computation algorithm enables the base station to securely compute predicate count or sum even in the presence of such an attack. It computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. It uses two phases at the end of the base station to filter out the false contributions of the compromised nodes from the aggregates. It produces successful computation of the aggregates even in the presence of the attack.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

D. **Cumulative summation based detection algorithm** [4]

This algorithm proposes integration of system monitoring modules and intrusion detection modules in the context of WSNs and Extended Kalman filter (EKF) based mechanism to detect false injected data. Then it monitors the behaviour of its neighbours and using EKF to predict their future states each node aims at setting up a normal range of the neighbours future transmitted aggregated values. Using different aggregation functions (average, sum, max, and min), it present theoretical threshold and uses algorithm of combining cumulative summation and generalized likelihood ratio to increase detection sensitivity. It first proposed that IDM and SMM should work together to provide intrusion detection capabilities of WSNs. To increase detection sensitivity further applied an algorithm of combining CUSUM and GLR. It further demonstrated how the proposed IDM can together with SMM differentiate malicious and emergency events. The proposed schemes using both real periments are based on MICA2 motes and large-scale synthetic data.

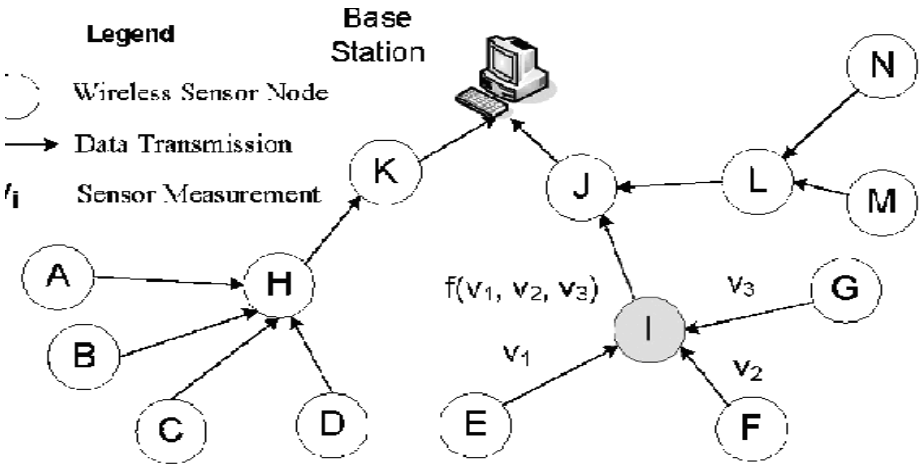

Fig 3.1(a) SENSOR NETWORK

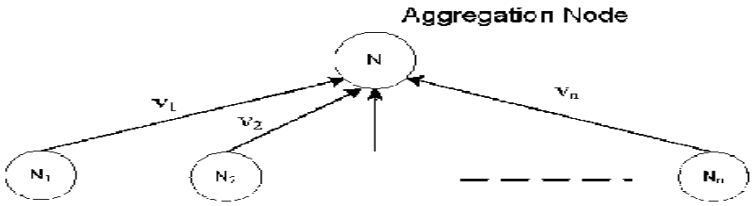

Fig 3.1(b) AGGREGATION NETWORK

E. Energy Efficient data aggregation in WSN [5]

Recovery fidelity and energy efficiency in WSNs are achieved by using a novel data aggregation scheme that exploits Compressed Sensing (CS) with arbitrary topology. It uses diffusion wavelets to find a sparse basis that characterizes the minimum-energy compressed data aggregation problem. It proves NP-completeness, and then proposes a mixed integer programming formulation along with a greedy heuristic algorithm to solve it. It designed a proper sparse basis based on

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

diffusion wavelets to achieve high-fidelity recovery for data aggregated from arbitrarily deployed WSNs. It develops the idea to allow for arbitrary network partitions and to integrate temporal correlations along with the spatial ones, which can significantly reduce energy consumption while maintaining the fidelity of data recovery. It investigated the minimum-energy CDA problem by characterizing its optimal configurations, analyzing its complexity, as well as providing both an exact solution (for small networks) and approximate solutions (for large networks).

F. Verification algorithms [6]

The synopsis diffusion which combines multipath routing schemes with duplicate-insensitive algorithms to accurately compute aggregates (e.g., predicate Count, Sum) in spite of message losses resulting from node and transmission failures. This aggregation framework does not address the problem of false sub aggregate values contributed by compromised nodes. A novel lightweight verification algorithm used in this synopsis diffusion to secure against attacks in which compromised nodes contribute false sub aggregate values. A compromised node might attempt to frustrate the aggregation process by launching several attacks. The falsified sub aggregate attack, in which a compromised node relays a false sub aggregate to the parent node with the aim of injecting error to the final value of the aggregate computed at the base station. Verification algorithm to compute aggregates, such as Count and Sum, and to enable the base station to verify if the computed aggregate is valid. Verification protocol prevent the base station from accepting a false aggregate, they do not guarantee the successful computation of the aggregate in the presence of the attack. Light weight verification algorithm enables the base station (BS) to verify whether the computed aggregate was valid.

IV. CONCLUSION

A comprehensive survey of data aggregation algorithms for wireless sensor networks has been presented.. These algorithms focus on optimization performance measures such as network data accuracy and energy consumption. Efficient routing and data aggregation are the main focused areas of data aggregation algorithms. It was focused on those algorithms that address the issues of secure data gathering and aggregation. Future work includes the enhancement of trust and reliability of the collected data from the sensor nodes. Wireless Sensor Networks are prone to many security attacks which impede the deployment and data propagation of sensor. It has been identified from the comparative study that only few studies had undergone secured routing in data aggregation. Most of the aggregation techniques consider only the energy consumption. In Future a new scheme can be proposed to identify the attacker when the false injection is very short. Finally, the discussion is brought to an end by concluding that a new technique has to be developed for secure data aggregation

REFERENCES

[1]. Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino and Sanjay Jha, "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]. Lei Yu, Jianzhong Li, Siyao Cheng, Shuguang Xiong and Haiying Shen, "Secure Continuous Aggregation in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systmes, Vol.25, No.3. March 2014.
[3]. Sankardas Roy, Mauro Conti, Sanjeev Setia and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions on Information Forensics and Security, Vol.9, No.4, April 2014.
[4]. Bo Sun, Xuemei Shan, Kui Wu and Yang Xiao, "Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks", IEEE Systems Journal,Vol.7, No.1, March 2013.
[5]. Liu Xiang,,JunLuo, "Compressed Data Aggregation: Energy-Efficient and High-Fidelity Data Collection", IEEE ACM Transactions on Networking, Vol.21, No.6, December 2013.
[6]. Sankardas Roy, Mauro Conti, Sanjeev Setia and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", IEEE Transactions on Information Forensicsand Security, vol.7, No.3, June 2012.
[7]. Miao Zhao, Ming Ma and Yuanyuan Yang, "Efficient Data Gathering with Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks", IEEE Transactions on Computers,vol.60, No.3, March 2011.
[8]. C. de Kerchove and P. Van Dooren, "Iterative filtering in reputation systems," SIAM J.Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.
[9]. Yue-Hsun Lin, Shih-Ying Chang, and Hung-Min Sun, "CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks", IEEE Transactions on Knowledge and Data Engineering, Vol.25, No.7, July 2013.
[10]. Haifeng Zheng, Shilin Xiao, Xinbing Wang, Xiaohua Tian and Mohsen Guizani, "Capacity and Delay Analysis for Data Gathering with Compressive Sensing in Wireless Sensor Networks", IEEE
Transactions on Wireless Communications, Vol.12, No.2, February 2013.
[11]. Junchao Ma, Wei Lou and Xiang-Yang Li, " Contiguous Link Scheduling for Data Aggregation in Wireless Sensor Networks",IEEE Transactions on Parallel and Distributed Systems, Vol.25, No.7, July 2014
[12]. R.Prema and R.Rangaraja " A Novel Approach for a Secured Power Aware and Energy Efficient Routing Protocol (SPAEERP) for Wireless Sensor Networks" in the European Journal of Scientific Research, Volume 101, No.2, May 2013, pp. 166-176