Available online at www.sciencedirect.com

ScienceDirect

Materials Today: Proceedings 5 (2018) 388–396

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

ENERGY EFFICIENT DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

Mrs. P.Padmaja[1], Dr.G.V.Marutheswar[2]

[1]*Research scholar, VITS, Deshmukhi,telangana,India*

[2]*Professor, Dept of EEE, S.V.U.College of Engineering, Tirupati, Andhra Pradesh,India*

Abstract

To optimizing wireless sensor networks for secured data transmission both at cluster head and base station data aggregation is needed.Data aggregation is performed in every router while forwarding data. The life time of sensor network reduces because of employing energy inefficient nodes for data aggregation. Hence aggregation process in WSN should be optimized in energy efficient manner. There are some computational technics to implement aggrigation at cluster head and base station.
When sensors are deployed at differet locations in wider area, it is possible to compromising attacks by adversaries. false data injected in compromised sensors during data aggregation process which results in false decision making at the Base Station (BS). Simple average data aggregation process is suitable only in attacker free environment.So to filter the false data during data aggregation, induced by the attacker . For every round of data agg.regation need to observe the behavior of nodes.So that it easy to minimize an impact of attacker contribution at the final result.For secure data aggregation process along with trustworthiness estimation using Trust wEighted Secure Data Aggregation algorithm (TESDA). Data aggregation process is optimized by performing aggregation in energy efficient manner through clustering.
If the aggregator is compromised, then it affects entire aggregation accuracy. Hence it is necessary to propose a aggregation protocol that is resilient against compromised sensor and compromised aggregator in energy efficient and secure manner.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Keywords: CH; WSN;BS; SDAF; TESDA

1. Introduction

A network of energy-constrained sensors deploying over a region is considered, in that each sensor monitors its surrounding area and periodically generates nformation. The systematic gathering and

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

transmission of sensed data to a base station for further processing is the basic operation in such a network.Sensors have the ability to carry out in-network aggregation or fusion of data packets reroute to the base station when data gathering. In such sensor system, the lifetime is the time in which the information can be gathered from all the sensors to the base station.In data gathering, from agreed energy constraints of the sensors expanding the system lifetime is a major threat . The data aggregator node or the cluster head combine the data to the base station and the malicious attacker may attack this cluster node. The base station cannot ensure the accuracy of the aggregate data sent to it, if a cluster head is compromised. Due to the uncompromised nodes, the existing systems may send several copies of aggregate results

to the base station and the power consumption at these nodes is increased.

2. Types of Data Aggregation

Several data aggregation techniques in WSN are described briefly as follows:

- **Lossless Data Aggregation:** Lossless aggregation refers to concatenating individual data items into larger packets, thus amortizing per-packet protocol overhead. It is effective if the load on the system is not excessive.

- **Lossy Data Aggregation:** If the total communication load exceeds system capacity, then the amount of communicated data must be forcibly reduced which is called the lossy aggregation. Example of lossy aggregation is the averaging of sensor values. It can be either temporal or spatial .
- **Structured Data Aggregation:** Structure-based applications require low maintenance since the traffic pattern is unchanging and thus it is suitable for such applications. The approach changes the structure dynamically and acquires high maintenance overhead. However, this technique cannot aggregate the data efficiently.
- **Structure Free Data Aggregation:** Structure free data aggregation technique provides efficient data aggregation without explicit maintenance of a structure. Spatial convergence and the temporal convergence are the necessary conditions for aggregation during transmission.
- **Centralized Approach:** This is an address centric approach where each node sends data to a central node via the shortest possible route using a multi-hop wireless protocol.

3. PREPOSED NEW METHOD FOR DATA AGGRIGATION

3.1. Secure Data Aggregation in Wireless Sensor Network Using Trust wEighted Secure Data Aggregation algorithm (TESDA)

- Data aggregation in Wireless Sensor Network (WSN) is applied to reduce redundancy and energy consumption. In WSN, in-network data aggregation performs aggregation of data in every router while forwarding data. Employing energy inefficient nodes in data aggregation affects lifetime of sensor network. Hence aggregation process in WSN should be optimized in energy efficient manner.
- When sensors are located in hostile environment, it is vulnerable to compromising attacks by adversaries. Compromised sensors inject false data during data aggregation process which results in false decision making at the Base Station (BS). Simple average data aggregation process is suitable only in attacker free environment. It is necessary to introduce a data aggregation mechanism that filters out attackers contribution during data aggregation. Behavior of nodes need to be observed in every round of data aggregation, and it should be reflected in subsequent rounds to filter out the impact of attacker contribution at the final result.

If the aggregator is compromised, then it affects entire aggregation accuracy. Hence it is necessary to propose a aggregation protocol that is resilient against compromised sensor and compromised aggregator in energy efficient and secure manner.

3.2. IMPLEMENTATION

An optimized and secure data aggregation protocol is proposed that is resilient to false data injection attack launched by compromised sensor and aggregator. Proposed protocol with the support of energy efficient clustering, performs secure data aggregation process along with trustworthiness estimation using Trust wEighted Secure Data Aggregation algorithm (TESDA) as shown in fig 1. Data aggregation process is optimized by performing aggregation in energy efficient manner through clustering. Sensor network is divided into clusters and each energy efficient Clusterhead (CH) aggregates data collected from its cluster members and transmits to BS. Secure data aggregation is carried out in two phases.

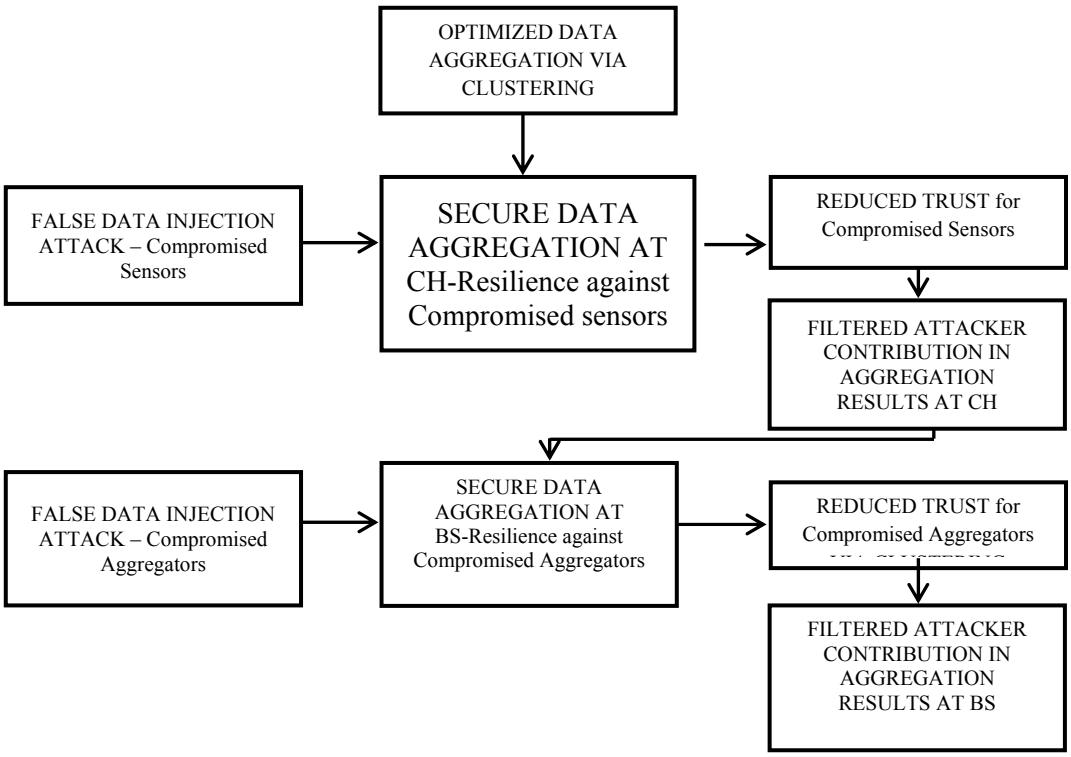

Fig. 1. Flowchart for implementing TESDA

3.3. MODULES

i. Optimized Data Aggregation via Energy Efficient Clustering.

ii. False Data Injection Attack.

iii. Secure Data Aggregation - Resilience against Compromised Sensors.

iv. Secure Data Aggregation - Resilience against Compromised Aggregator .

v. Performance Evaluation..

Modules Description are for secured data transmissionin wireless sensor networks are

3.1.1.Optimized Data Aggregation via Energy Efficient Clustering

Input: Sensors ID and Residual energy
Output: Clusterhead

Each sensor attaches its ID and residual energy in its hello message. The node that receives the hello message add the sender in its neighbor list. Each node compares the residual energy of all of its neighbors. It selects the neighbor that has high residual energy as its ClusterHead (CH). Cluster member attaches its CH ID in hello message. On receiving hello message each node checks whether the CH ID mentioned in the hello message and its own ID are same. If it so it adds the corresponding sender its its member list. CH roles are rotated in every round in order to balance the energy consumption. Clustering rounds depends on the clustering period.

3.1.2False Data Injection Attack

Input: False data through compromised sensor
Output: Falsified aggregate

Sensed result (X) of every sensor (S_i) is submitted to CH. It derives the aggregated result (A_r) by taking weighted average of collected information. Attacker compromises the sensor and alters its sensed value to very low or high to distort the aggregation result. False data from compromised sensor, reduces aggregation result as CH computes aggregation result from the reported value.

When the CH submits the falsified aggregate to the base station, it leads to false decision making.

$$\text{Aggregated result } A_r = \sum_{i=1}^{n} X_i / n \quad r=1,2..m$$

3.1.3. Secure Data Aggregation - Resilience against Compromised Sensors

Input: False data through compromised sensor, actual data from genuine sensors
Output: Reduced trust of compromised sensor, Filtered attacker contribution in aggregated result

Sensed result (X) of every sensor (S_i) is submitted to CH. It derives the aggregated result (A_r) by taking weighted average of collected information. Weight of the every sensor is assigned from the trust measurement of the sensor. Trust of every sensor is evaluated from Non Deviation Factor. If the non deviation factor is low trust becomes very low which means that its value is deviation is high. Attacker compromises the sensor and alters its sensed value to very low or high to distort the aggregation result. As the aggregator computes trust value from the deviation, compromised sensor gets very low trust. Hence contribution of the corresponding sensor is reduced in aggregated result as trust is considered as weight in computation. Final aggregated result at CH is the trust weighted summation of data reported by the cluster members of the cluster in the round.

$$\text{Average Data } (Avg_r) = \sum_{i=1}^{n} X_i \quad r=1,2..m$$

$$\text{Deviation } D_i(r) = \text{Avg}_r \sim X_i(r)$$

$$\text{Total Deviation } TD(r) = \sum_{i=1}^{n} D_i(r)$$

$$\text{Non Deviation Factor } NDF_i(r) = TD(r) \sim D_i(r)$$

$$\text{Total Non Deviation } TNDF_i(r) = \sum_{i=1}^{n} X_i$$

$$\text{Trust } T_i(r) = NDF_i(r) / TNDF_i(r)$$

$$\text{Weight } w_i(r) = T_i(r)$$

$$\text{Aggregated result } A_r = \sum_{i=1}^{n} w_i X_i \quad r=1,2..m$$

3.1.4Secure Data Aggregation - Resilience against Compromised Aggregator

Input: False data through compromised aggregator, actual data from genuine aggregators
Output: Reduced trust of compromised aggregator, Filtered attacker contribution in aggregated result

If the attacker compromises the CH, it alters the aggregated result (Z_i) before submitting it to the Base Station (BS) in order to distort the final aggregation result ($BS(A_{r)}$)) at the base station. To overcome this issue BS verifies the trustworthiness of the CH (TCH_i) through the original sensed information collected from the subset of CH nodes (k) . BS aggregates the collected data from subset of CH nodes and finds the deviation (DCH_i) between reported result by CH. If the deviation is high BS reduces the trust value of the CH as the inverse proportion of the deviation and direct proportion of the non deviation factor (NDF_CH). Hence the impact of falsified data contributed by the CH is reduced at the base station. Final aggregated result at BS is the trust weighted summation of data reported by the CHs in the round.

$$\text{BS Average Data } (BSAvg_r) = \sum_{i=1}^{k} Z_i \quad r=1,2..m$$

$$\text{Deviation } DCH_i(r) = BSAvg_r \sim Z_i(r)$$

$$\text{Total Deviation } TDCH(r) = \sum_{i=1}^{k} DCH_i(r)$$

$$\text{Non Deviation Factor } NDF\_CH_i(r) = TDCH(r) \sim DCH_i(r)$$

$$\text{Total Non Deviation } TNDF\_CH_i(r) = \sum_{i=1}^{k} NDF\_CH_i(r)$$

$$\text{Trust } TCH_i(r) = NDF\_CH_i(r) / TNDF\_CH_i(r)$$

$$\text{Weight } w_{chi}(r) = TCH_i(r)$$

$$\text{Aggregated result } BSA_r = \sum_{i=1}^{k} w_{chi} Z_i \qquad r=1,2..m$$

4. Performance Evaluation

The TESDA based proposed approach is evaluated and compared with existing approach Secure Data Aggregation in WSN using Filtering (SDAF) [1] for the following parameters using the ns-2 simulation.

- **Data Aggregation Deviation**
  It refers to the percentage of the aggregation error. It is calculated as the ratio of deviation to the

  true value sensed by the sensors.

- **Network lifetime**
  It refers to the time till half of the nodes in network remains alive.

- **Overhead**
  It refers to the total number of control packets involved for the secure data aggregation process.

- **Attacker Impact Reduction Ratio**
  It refers to the ratio of reduced trust of the compromised sensors from the actual trust of

the compromised sensors resided in the network

- **Energy Consumption**
  It refers to the total amount of energy required for data aggregation process.

5. Result

Secure data aggregation protocol, named as TESDA identifies comprised nodes over clustered WSN environment. In TESDA, the clustering mechanism separates the sensor nodes into clusters and each cluster have a CH for data aggregation. The clustering mechanism balances the energy expenditure among all the nodes in a cluster by periodically rotating the CH role within the cluster. The deviation based trust measurement mechanism measures the trust value of the nodes based on a deviation factor and it converts the trust value as a weighting factor for a succeeding round. Thus, it minimizes the impact of malicious nodes in data aggregation by estimating the current trust value of a node using a weighting factor. Besides, the TESDA protocol optimizes the data aggregation process by exploiting a deviation based trust model and extends the lifetime of the network using energy efficient clustering model. From the simulation results, the TESDA consistently outperforms the existing SDAF in terms of all performance metrics. Compared to SDAF, TESDA reduces the data aggregation deviation by and achieves a reduction in latency by 14.43% and attains reduction in energy consumption by 26.8%.

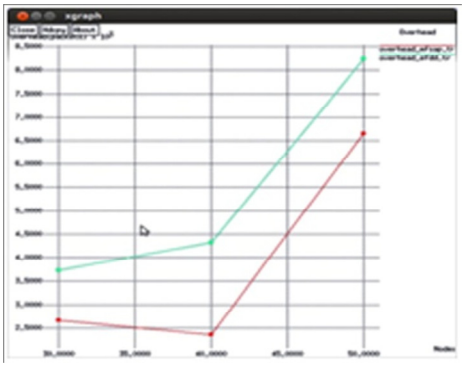

Fig.2.Attacker Impact Reduction Ratio

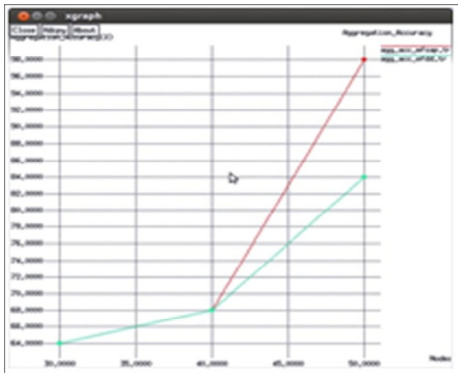

Fig.3.Data Aggregation Deviation

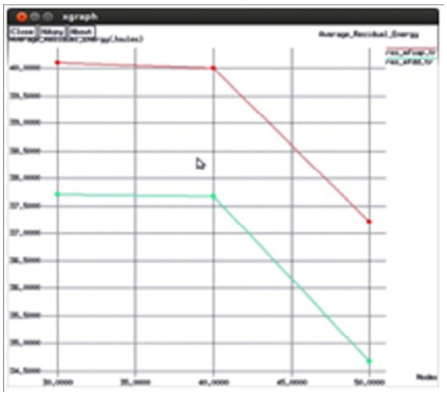

Fig.4.Network Life Time

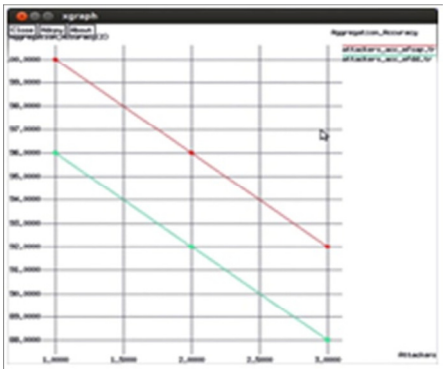

Fig.5.Energy Consumption

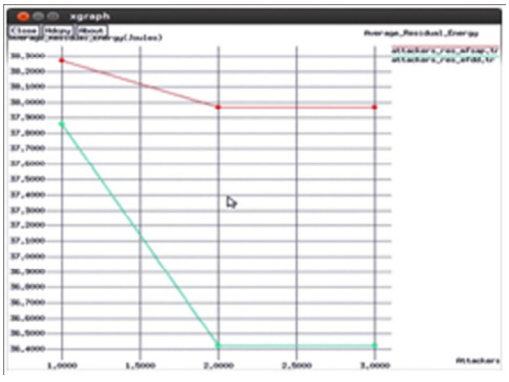

Fig.6.Over Head

6. Conclusion

After simulation using NS-2 tool, Enegy efficient data transmission is possible by using the data aggrigation technic TESDA ,compared with other technics HEF,SDAF.secured data aggregation using TESDA is more efficient.

References

[1] Roy, Sandip, et al., "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", IEEE Transactions on Information Forensics and Security, Vol.9, No.4, pp.681-694, 2014.

[2] Zhu W, Xiang, Y & Zhou, J 2011, 'Secure localization with attack detection in wireless sensor networks', International Journal of Information Security, vol. 10, no. 3, pp. 155-171.

[3] Pradeepa, K, Anne, WR & Duraisamy, S 2012,'Design and implementation issues of clustering in Wireless Sensor Networks', International Journal of Computer Applications, vol. 47, no. 11. pp. 23-28.

[4] Kavitha, T & Sridharan, D 2010 'Security vulnerabilities in Wireless Sensor Networks: A survey', Journal of Information Assurance and Security, vol. 5, pp. 31-44.

[5] Daojing He, Jiajun Bu & Chan, S 2011, 'Privacy- preserving universal authentication protocol for wireless communications', IEEE transactions on wireless communications, vol. 10, no. 2, pp. 431-436.

[6] Alcaraz, C, Lopez, J & Roman, R 2012, 'Selecting Key Management Schemes for Wireless Sensor Networks application', Journal of Computers and Security (Elsevier), vol. 31, no. 8, pp. 956-966.

[7] Azarderskhsh, R & Reyhani, A 2011, 'Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks', Eurasip Journal on Wireless Communications and Networking, Article ID: 893592, pp. 1-12.
[8] Ozdemir, Suat, and Yang Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview”, Computer Networks, Vol. 53, No. 12, pp. 2022-2037, 2009.
[9] L. Hu and D. Evans, “Secure aggregation for wireless networks”, In Proceeding of Workshop on Security and Assurance in Ad hoc Networks, 2003.
[10] S. Ozdemir, “Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism”, In Proceedings of the IEEE International Conference on Pervasive Services (ICPS), pp. 165–168, 2007