ISSN (online) : 2277-5390
ISSN (Print): 2277 - 5382

Secure aggregation against Collusion Attacks and compromised aggregator

[*1]Mohanraj Govindaraj, [2]Saritha Karthik

[*1,2]*Lecturer, International Graduate Studies College, Brunei Darussalam*
[*1]mohanrajvlb@gmail.com, [2]sarithaviswam1980@gmail.com

Abstract

Objective: To provide Secure Aggregation against Collusion attacks and Malicious or compromised aggregator.
Statistical Analysis: Wireless Sensor Network incorporate aggregation of data from multiple sensor nodes performed at the aggregator node or the cluster head due to limited computational power and energy. This aggregation technique is vulnerable to attacks of compromised nodes. Thus a secure Data Aggregation for Collusion Attacks (SACA) was proposed earlier that improved the previously stated IF algorithms by providing initial approximation of trustworthiness of the sensor nodes. This made the algorithm to be more accurate and faster.
Findings: The problem in this approach is that these improvisations were made with the assumption that the aggregator is not compromised. So in case if the aggregator node is compromised this method stands pointless in determining the security. Thus a new framework called Secure aggregation against Collusion Attacks and compromised aggregator (SACACA) is proposed to ensure that the Secure Date Aggregation scheme also fetch protection over the compromised aggregator node. The proposed work initializes with an aggregator node, that estimates the error and noise of the other sensor nodes in the cluster, and then calculates the reputation vector of each node and provides the information of trustworthiness of each node to the enhanced IF algorithm. The aggregator sends the aggregated information to the base station directly or to the aggregator of another cluster's aggregator and then reaches to the base station. This procedure is repeated by the replacement of the aggregator by a node in the cluster as the next aggregator node once in a time period. Thus the path of the aggregated information to the base station may vary according to the selection of the aggregator in each cluster. The Variance of each aggregator is calculated in the Base Station. The Calculated values are compared to a threshold value that determines whether the aggregator node is compromised or not. In order to find the variance value the enhanced IFs algorithm is utilized.
Improvements: Thus the proposed method improves the effectiveness of the enhanced IF algorithm over the compromised aggregator nodes. The change of aggregator in the network also saves a significant amount of computational power and energy.

***Keywords*:** Wireless Sensor Networks, Secure Data Aggregation, Collusion attacks, compromised aggregator.

1. Introduction

Security is one of the important topics in WSNs. Common security protocols cannot be applied directly to the sensor networks because they have limited hardware resources in terms of memory, computing, energy, capabilities and communications range. Distributed deployment nature of WSNs poses challenge to the security of node cooperation. It might be vulnerable to several types of attacks namely Black hole, Spoofing, Rushing, Wormhole, Modification, No-cooperation, etc. Data in WSN is transferred over a number of nodes and any malicious node in the path leads to a dangerous situation.

To address this safety issue and to detect compromised nodes, research on security in WSNs has advanced, showing cryptography mechanisms, intrusion detection systems, and efficient routing protocols. Unfortunately, these security models face with several security issues: computation-intensive techniques like public-key cryptography are not expected to be used in wireless sensor networks. The intruder detection system can detect the malicious node, however, this latter is very expensive for WSNs and there is no guarantee in detecting a malicious node and the IDS package generates additional overhead as well as more false alarms are triggered. The Dynamic Source Protocol (DSP) does not have any built-in functionality to calculate an alternate path if the path has a malicious node so cannot detect the malicious node.

Trust and reputation monitoring (TRM) system has recently been suggested as an effective security mechanism to improve reliability and to mitigate attacks within networked environments, it is an innovative solution for

ISSN (online) : 2277-5390
ISSN (Print): 2277 - 5382

maintaining a minimum security level that have been proposed for a variety of applications, among them are the selection of good peers in a peer-to-peer network. The choice of transaction partners for online auctioning such as E-bay, and the detection of misbehaving nodes in mobile ad-hoc network. It has recently been suggested as an effective security mechanism to improve reliability and to mitigate attacks within WSNs. While many secure schemes focus on preventing attackers from entering the network through secure key management, trust management takes a further step to guard the whole network even if malicious nodes have gained access to it and to identify malicious, selfish and compromised nodes which have been authenticated.

Aggregation involves data from multiple sensors to be aggregated at an aggregator node and then it forwards to the aggregated values to the base station. Due to limitations of the computation power and the energy resource of sensor nodes, data is aggregated but it is known to be very vulnerable to faults and malicious attacks. It is very serious problem because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation performed at the aggregator node should possess the trustworthiness information of individual sensor nodes. Thus efficient and powerful algorithms are needed for data aggregation in the future WSN.

2. Related Works

[1] Proposed a technique for dynamic secure end-to-end data aggregation along with privacy protection, known as DyDAP. The proposed approach was designed initially from a UML model with the most important building blocks of a privacy-aware WSN that included aggregation policies. It also introduced an aggregation algorithm with discrete-time control loop to dynamically handle in-network data fusion for reducing the communication load. DyDAP avoided network congestion, improves WSN estimation accuracy and also guarantees anonymity and data integrity. However it needs an extra work of decryption before any aggregation process.

[2] Proposed a new protocol which provided the control integrity for aggregation in wireless sensor networks. The proposed protocol was based on a two-hop verification mechanism of data integrity and was essentially different from existing solutions. The solution was named as called as Secure and Efficient Data Aggregation protocol for wireless sensor Networks (SEDAN), in which each node verified the integrity of its two-hop neighbors' data, and the aggregation of the immediate neighbors. This made the elimination of useless transmission of bogus data, and hence saving sensors' energy resources. It does not require referring to the base station for verifying and detecting faulty aggregated readings, thus providing a totally distributed scheme to guarantee data integrity. But it requires extra transmissions in order to co ordinate incorrect aggregations.

[3] Proposed a zone-based node compromise detection and revocation scheme for sensor networks using the Sequential Probability Ratio Test (SPRT). Robustness of the SPRT was also enhanced with biased sampling. The proposed scheme achieved robust untrustworthy zone detection capability even if a majority of nodes in each zone are compromised. The work also proposed countermeasures against the attacks of disruption of the proposed scheme. The modeled interaction between the defender and the adversary as a repeated game with complete information was proposed and found a Nash Equilibrium. The results showed that the scheme quickly detected untrustworthy zones with a small number of zone-trust reports. However, the change in sampling strategy affects the average number of samples.

[4] Proposed energy efficient multipath data transfer scheme that addressed the troubles caused by false data injection attack. It was done by early detection and filtering of injected false data. The multipath data transfer technique prevented the direct access of event information using a compromised en-route node. The proposed work focused to achieve reliable data delivery against compromise of the data. Initially two node-disjoint paths are used for key sharing and data sharing, then false event reports was filtered within few hops. And if a path was found to be attacked, it can be replaced using an alternate path. However, this causes more communication overhead.

[5] Proposed a trust system that was persistent against routing attacks and even trust system attacks. Each node can choose the shortest secure path as possible. The proposed technique does not need any time synchronization and location information of the node. The sink can determine trust values of the nodes by receiving control information of the node. It has a high accuracy because of comprehensive view of the sink and therefore the malicious node can't create different trust values in nodes through conflicting behavior attack.

[6] We proposed a lightweight and dependable trust system (LDTS) for WSNs, with clustering algorithms. A lightweight trust decision-making scheme was proposed based on the role of the node in the clustered WSNs that was suitable for such WSNs because it facilitates energy-saving. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. LDTS had greatly improvised the

system efficiency while reducing the effect of malicious nodes in case of the cancellation of feedback between nodes. A dependability-enhanced trust evaluating approach was adopted for co-operations between Cluster Heads (CH), LDTS detected and also prevented malicious, selfish, and faulty CHs. But the storage overhead increases as the number of Cluster Members increase.

[7] Discussed about a new type of false data injection attacks known as collaborative false data injection, and proposed two filtering schemes namely the geographical information based false data filtering scheme (GFFS) that used the absolute positions of the sensors, and the neighbor information based false data filtering scheme (NFFS) that used relative positions of the sensors when the exact positions were not obtained. Initially a new false data injection model called collaborative false data injection was developed to point out that existing data filtering techniques can't defend such attacks. In case of GFFS, each node distributed it's the location information to the forwarding node. The data report of each node carries the MACs and locations of t detecting nodes to sense the event. The forwarding node verifies the correctness of both the MACs and locations and the legitimacy of the t locations. Results prove that when there are totally ten nodes compromised in a 400 nodes network, the detection probability of collaborative false data injection attacks is higher than 97% in GFFS and NFFS, but is less than 7% in traditional false data filtering approaches such as SEF. But the extra fields in GFFS cause more energy consumption in reports transmitting, computation and reception.

[8] Discussed about the attacks faced by an aggregation framework called synopsis diffusion that used duplicate insensitive algorithms on top of multipath routing schemes for accurate computation of aggregates. This aggregation framework never addresses the problem of false sub aggregate values contributed by the compromised nodes and this attack causes large errors in the aggregates computed at the root node in the aggregation hierarchy. In oreder to make this synopsis diffusion approach secure against the above attack an algorithm to enable the base station for secure computation of predicate count or sum even in the presence of such an attack. The proposed attack-resilient computation algorithm computed the true aggregate by filtering out the compromised node's contributions. But it incurs high computation cost.

[9] Proposed a secure, energy-efficient data aggregation scheme to detect the malicious nodes with a constant per node communication overhead. In the proposed approach, all aggregation results are signed with the private keys of the aggregators such that they are not altered by others. The nodes on each link additionally use their pair wise shared key for the communication to secure. Then each node receives the aggregation results from its parent and its siblings, and also verifies the aggregation result of the parent node. Analysis proved that the proposed approach was better on energy consumption and communication overhead, but the performance of the nodes can be disturbed by Byzantine attacks to the child nodes.

[10] Proposed a proactive defense model for wireless sensor networks. It was used to emphasize that the node has a limited ability to learn the evolution of rationality from different attack strategies of the attacker. The proposed work dynamically adjusts their strategies to achieve the most effective defense. While the proposed approach the cost has been greatly saved and also the life cycle of the nodes has been extended. The whole wireless sensor network can be implemented in an effective way by employing the proposed model. But the model has high computational complexity.

[11] Discussed about the problems faced by the Iterative filtering (IF) algorithms that estimate the aggregate value of the readings and the trustworthiness of the nodes. However, it represented a difficulty in applications involving streaming data. Hence this paper proposed a STRIF (Streaming IF) to extend IF algorithms to data streaming which is done by a novel method for updating the sensor variances. STRIF can process data streams much more efficiently than the batch algorithms with accuracy of the data aggregation close to that of the batch IF algorithm. But whenever there is a change in the sensor variance, the cumulative error increases.

[12] Proposed a novel secure data aggregation protocol for WSNs. Proposed scheme employed the Stateful Public Key Encryption (StPKE) with some previous techniques to provide an efficient end-to-end security. The proposed solution does not impose any bound on the aggregation function's nature such as Maximum, Minimum, or Average. The proposed scheme was implemented on TelosB as well as MicaZ sensor network platforms. It measured the execution time of various cryptographic functions of the proposed scheme. It achieved a high security level with a low overhead in large-scale scenario. But it incurs more energy consumption.

[13] Focused on suddenly spoiled nodes in the network that may incur intelligent attacks against a trust-establishment mechanism. Hence proposed a reliable generic trust model named TMR (a Trust Model based on Risk evaluation). Proposed scheme was a reliable scheme as it combined the risk assessment with the reputation evaluation for deriving trustworthiness. The proposed work contributed for the first modeling of the risk as the

opinion of short-term trustworthiness combined with traditional reputation evaluation to derive the trustworthiness in WSNs. But it does not perform well in newcomer attack in mobile network.

[14] Proposed a novel algorithm for the identification of the malicious data injections. The proposed algorithm that characterized the relationships between the sensors' reported values. It also built measurement estimates which are resistant to several compromised sensors even when they collude in the attack. A methodology for applying this algorithm in different application contexts was also proposed and evaluated its results on three different datasets from distinct WSN deployments. This leads us to identify different trade-offs in the design of such algorithms and how they are influenced by the application context. But the detection rate becomes low as threshold reduces.

Proposed novel WSN framework-based investigations performs on peer trust and linguistic fuzzy trust model (LFTM) which was used for trust and reputation models. Reports of Accuracy, path length, and energy consumption of sensor node are evaluated for their current and average scenarios. It also emphasized the evaluation over the satisfaction for LFTM model in the deployed WSN framework. The sensor augmentation performance for the proposed framework was evaluated via analytic bounds and numerical simulations. The evaluated results exhibited the eminence of the proposed sensor augmentation-based realization over past trust and reputation model investigations. However, it does not satisfy for all types of distribution strategies.

3. Methodology

Consider a WSN with n number of sensors. Sensors are denoted as Si, where i = 1 to n. The sensor network model is same as that of the model proposed in [15]. The nodes are formed as disjoint clusters, with each cluster there is a cluster head called the aggregator. The data from the sensor nodes are periodically collected and aggregated by the aggregator. This framework assumes that the aggregator is not compromised and concentrates on effectively improving the IF algorithm to be efficient over collusion attacks with compromised sensor nodes that sends false information to the aggregator.

Initially Bias and Variance of the sensor nodes are estimated and the Maximum Likelihood estimation of the variance is also done to obtain the reputation vector of the sensor nodes. The previously proposed IF algorithm [16] is enhanced by providing the trustworthiness information of the sensor nodes of the network as an initial reputation to the algorithm to make it effective by reducing the number of iterations in the algorithm. But when the aggregator node is compromised, the enhanced IF algorithm proves to be ineffective. Thus in order to make this algorithm perform well in case of aggregator node compromise, a new approach is proposed.

The proposed work initializes with an aggregator node, that estimates the error and noise of the other sensor nodes in the cluster, and then calculates the reputation vector of each node and provides the information of trustworthiness of each node to the enhanced IF algorithm. The aggregator sends the aggregated information to the base station directly or to the aggregator of another cluster's aggregator and then reaches to the base station. This procedure is repeated by the replacement of the aggregator by a node in the cluster as the next aggregator node once in a time period. Thus the path of the aggregated information to the base station may vary according to the selection of the aggregator in each cluster. So in order to find the compromised aggregator in the cluster enhanced IF algorithm is utilized. The result of reveals whether the aggregator node is compromised or not by determining its reputation vector.

3.1. Malicious aggregator node detection

A cluster with an aggregator node, estimates the error and noise of the other sensor nodes in the cluster, and then calculates the reputation vector of each node and provides the information of trustworthiness of each node to the enhanced IF algorithm. The aggregator sends the aggregated information to the base station directly or to the aggregator of another cluster's aggregator and then reaches to the base station. This procedure is repeated by the replacement of the aggregator by a node in the cluster as the next aggregator node once in a time period. Thus the path of the aggregated information to the base station may vary according to the selection of the aggregator in each cluster. So in order to find the compromised aggregator in the cluster enhanced IF algorithm is utilized.

Consider a number of clusters in the network [17], each with a cluster head called aggregator. The aggregator aggregates the data from the sensor nodes and sends it directly to the base station or it sends it to the aggregator of the nearby cluster and then to the base station. Consider the number of clusters as n, and the number of nodes in each cluster is m. Thus an aggregator in a cluster is denoted as A_{ai}. The A_{11} is the aggregator of the cluster 1.

The aggregator for each cluster varies once in a time period, ie it is replaced by its sensor nodes that are located at the boundaries of the cluster. Thus the route of the aggregated information may vary according to the selection of

the aggregator in each cluster. Thus the Base station receives the aggregated information through a variety of aggregator routes. Thus the aggregators reputation vectors, error and variance are calculated and initialized in the enhanced IF algorithm to make it faster and accurate.

The Base Station or any other aggregator receives the information through different order of the aggregators. Then the Mean and Variance value is calculated for each aggregator of the network considering the enhanced IF algorithm. The Variance values of all the aggregators are determined and checked whether it lies below the threshold or not. Thus while analyzing the information of the all the aggregator in the base station, it is inferred whether any aggregator deviates in its value of variance. If it exceeds the threshold value, then the aggregator is detected as a compromised one in the network.

3.2. Enhanced IF Algorithm

3.2.1.Bias Estimation for the sensor node

The aggregator's function in the cluster is to receive the data from each sensor node, aggregates it and then sends it to the base station. The enhanced IF algorithm [16] for sensor nodes is explained below,

Let r_t denotes the true value of the signal at time t. Each sensor reading $\mathrm{x_s^t}$ can be written as $x_s^t = r_t + e_s^t$.The main idea is that, since we have no access to the true value $\mathrm{r_t}$ the system cannot obtain the value of the error e_s^t . However, we can obtain the values of the differences of such errors.

$$\delta(i,j) = \bar{e}_i - \bar{e}_j \approx \mathrm{b_i} - \mathrm{b_j} \qquad (1)$$

Let $\delta = \{\delta(i,j) : 1 \le i,j \le n\}$; this matrix is an estimator for mutual difference of sensor bias. In order to obtain the sensor bias from this matrix, the minimization problem is solved and a Lagrangian multiplier is introduced,

$$F(\vec{b}) = \sum_{i=1}^{n}\sum_{j=1}^{i-1}\left(\frac{b_i - b_j}{\delta(i,j)} - 1\right)^2 + \lambda\sum_{i=1}^{n} b_i \qquad (2)$$

By setting the gradient of $F(\vec{b})$ to zero, the bias values of the sensor node is obtained.

3.2.2. Variance Estimation for the sensor node

A similar method is used to estimate variance of the sensor noise using the estimated bias from previous section. Given the bias vector b = [b1; b2; _ _ _; bn] and sensor readings of the sensor as $\mathrm{x_s^t}$, the system can define matrices $\hat{\mathrm{x}}_\mathrm{s}^\mathrm{t}$ and β = {β(i, j)}as follows

$$\hat{\mathrm{x}}_\mathrm{s}^\mathrm{t} = \mathrm{x_s^t} - \mathrm{b_s} \qquad (3)$$

We assume that the sensor noise is generated by independent random variables

$$\beta(i,j) = \frac{1}{m-1}\sum_{t=1}^{m}(e_i^t - b_i)^2 + \frac{1}{m-1}\sum_{t=1}^{m}(e_i^t - b_j)^2 \qquad (4)$$

The above formula shows that the variance of sensor noise can be calculated by computing the matrixβ. The estimation of variances of sensors is obtained from the matrix β = {β(i, j)} by solving,

$$\text{Minimise } \sum_{i=1}^{n}\sum_{j=1}^{i-1}\left(\frac{v_i - v_j}{\beta(i,j)} - 1\right)^2 \qquad (5)$$

$$\text{Subject to } \sum_{i=1}^{n} v_i = \frac{n}{m(n-1)}\sum_{i=1}^{n}\sum_{t=1}^{m}(\hat{x}_i^t - \bar{x}^t)^2 \qquad (6)$$

It uses a Lagrangian multiplier λ and by solving the minimization problem, obtains this equation,

$$\sum_{\substack{i=1\\ i\neq k}}^{n}\frac{1}{\beta(i,k)^2}\, v_i + \sum_{\substack{i=1\\ i\neq k}}^{n}\frac{1}{\beta(i,k)^2}\, v_k + \frac{\lambda}{2} = \sum_{i=1}^{n}\frac{1}{\beta(i,k)} \qquad (7)$$

$$\sum_{i=1}^{n} v_i = \frac{n}{m(n-1)}\sum_{\mathrm{i=1}}^{\mathrm{n}}\sum_{\mathrm{t=1}}^{\mathrm{m}}(\hat{\mathrm{x}}_\mathrm{i}^\mathrm{t} - \bar{\mathrm{x}}^\mathrm{t})^2 \qquad (8)$$

For all k= 1,,,,n.

This provides the possible variance by subtracting the bias estimates from sensor readings. The above mentioned procedure of calculating bias and variance for sensor nodes is extended to aggregator node. The framework only calculates the Mean and Variance of the sensor values from the aggregator and determines the compromised aggregator. The variance of the aggregator is obtained by the subtracting the mean value of the each sensor nodes from aggregator from the value of a sensor node from each aggregator. The procedure for the calculation of the Variance and detecting the compromised aggregator is explained below using an algorithm,

Algorithm for Secure aggregation against Collusion Attacks and compromised aggregator (SACACA):

1. Aggregator for each cluster is denoted as A_{ai} for ath cluster, and ith node.
2. Consider the aggregator A_{11} sends aggregated information of the first cluster to the aggregator of the nearby second cluster $A_{21.}$
3. Then it transfers it to the nearby third aggregator A_{32} or to the base station directly.
4. Thus the sequence followed is A_{11} to A_{21} to A_{32} then to the Base station say.
5. Then once in a time period the aggregator may change in each cluster.
6. Let the next sequences be A_{11} to A_{21} to A_{32} then to the Base station say.
7. Next one is A_{11} to A_{22} to A_{31} then to the Base station.
8. Thus the base station receives the aggregated data through various aggregator sequences.
9. The Mean and Variation values of each aggregator is calculated as,
10. Consider an aggregator performing in each cluster sending values to the nearby aggregator or to the base station directly. The aggregator gets values from each sensor node in the cluster, let the mean values of each sensor from the aggregator is calculated as,

$$\overline{S_{iat}} = \frac{1}{t}\sum_{a=1}^{n}\sum_{t=1}^{m} x_t(S_{ia}) \quad (9)$$

Where S_{ia} is the value from each sensor, where i denote the node in the cluster and a denotes the Cluster. Then, the value from the same sensor node from each aggregator is calculated as

$$S_{iat} = \frac{1}{t}\sum_{a,t=1}^{m} x_t(S_{ia}) \quad (10)$$

The Variance of each aggregator is calculated as,

Variance of the Aggregator, $\mathrm{Var(Aa)} = \overline{S_{iat}} - S_{iat}$ (11)

11. The base station receives the variance values of all the aggregator nodes. It checks whether the variance values lie below a threshold value T determined for reputed aggregator.

$$\text{If } \mathrm{Var(Aa)} > T \quad (12)$$

Then the corresponding node is compromised.

12. If the variance values that lie below the threshold value, then the node is genuine. If the value exceeds the threshold then it is known that the aggregator node is compromised.
13. Thus the compromised aggregator is detected in the WSN thus saving the computational power and energy as there is a change in the aggregator node in the cluster once in a while.

Thus the compromised aggregator is detected in the network using the enhanced IF algorithm that calculates the variance for the sensor nodes. These calculations are extended for the aggregator nodes. Hence the proposed framework detects the compromised aggregator nodes in the network.

4. Results and Discussion

The proposed Secure aggregation against Collusion Attacks and compromised aggregator (SACACA) method is compared with the existing Secure aggregation against Collusion Attacks (SACA) on the basis of two IF algorithms namely Robust Aggregator & Reciprocal and Robust Aggregator & Affline. The parameters that are used for the comparison of the two algorithms consist of 1. RMSE error with no of colluders and standard deviation & 2. RMSE error with no of aggregator and standard deviation. Thus the results are evaluated and compared below to prove the efficiency of the proposed SACACA method.

ISSN (online) : 2277-5390
ISSN (Print): 2277 - 5382

The result provides the comparison of the accuracy of SACA and SACACA method with two approaches Robust Aggregate + Reciprocal and Robust Aggregate + Affline.

4.1. RMS Error with No. of Colluders and standard deviation

Figure 1. Comparison Result on RMS error with No. of Colluders and Standard Deviation for Robust Aggregate + Affline

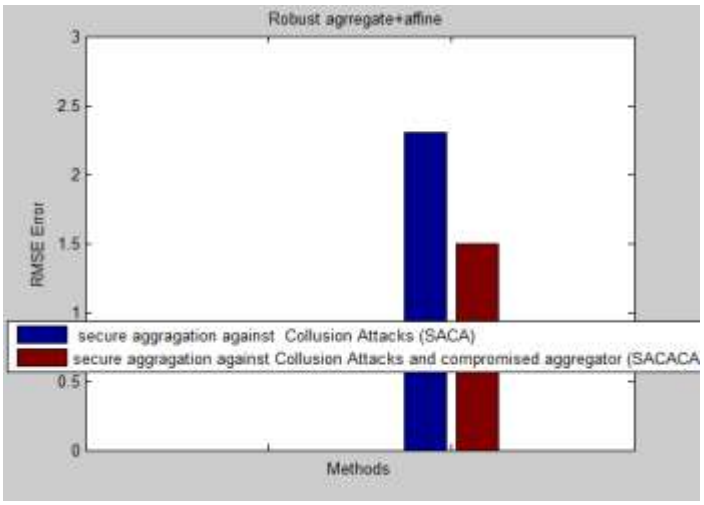


Figure 2. Comparison Result on RMS error with No. of Colluders and Standard Deviation for Robust Aggregate + Reciprocal

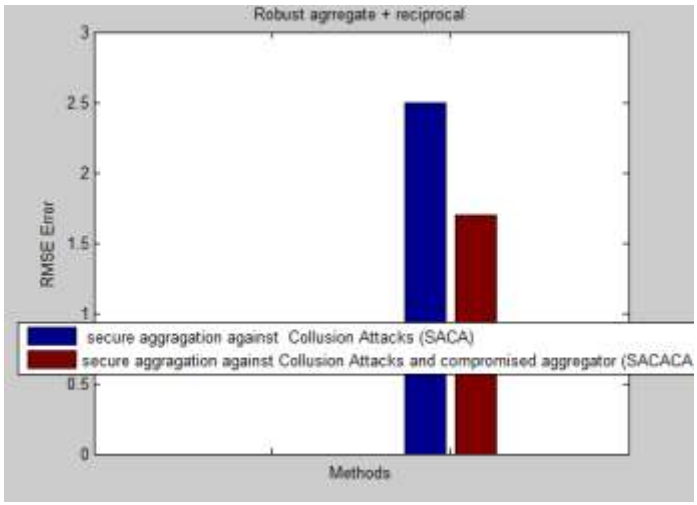
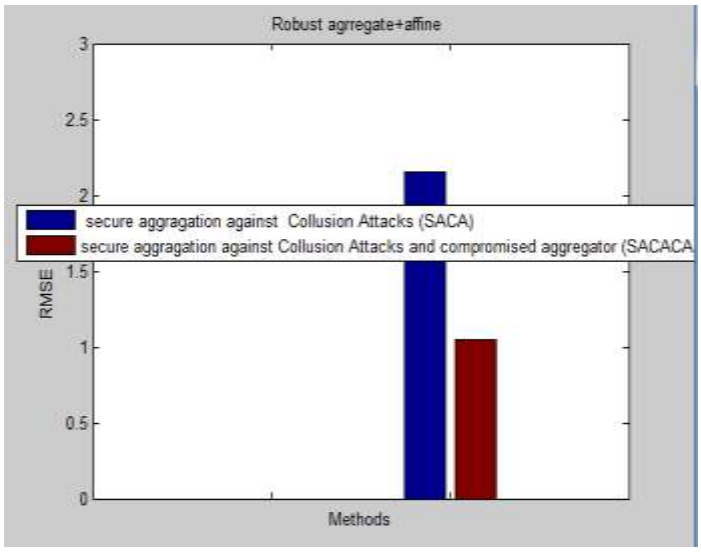


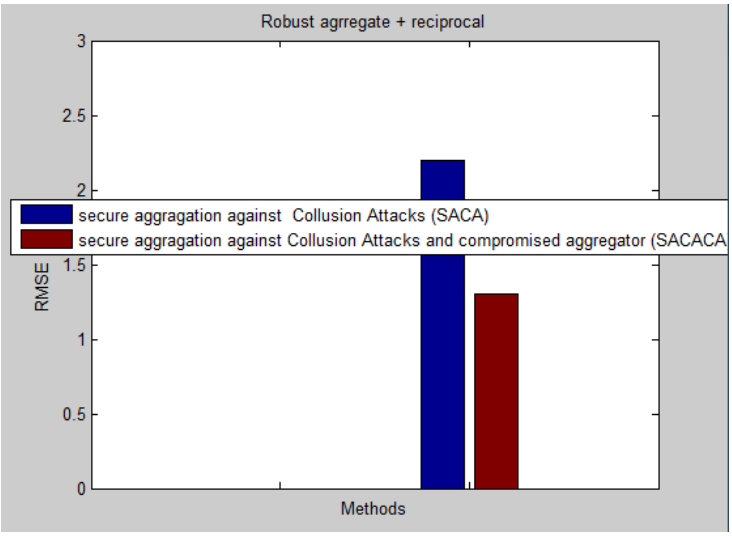
Figure 3. Comparison Result on RMS error with No. of Aggregators and Standard Deviation for Robust Aggregate + Affline



ISSN (online) : 2277-5390
ISSN (Print): 2277 - 5382

4.2. RMS Error with no. of Aggregators and standard deviation

Figure 4. Comparison Result on RMS error with No. of Aggregators and Standard Deviation for Robust Aggregate + Reciprocal



From Figure 1 and 2, it is inferred that the proposed method shows low RMS error and hence the detection accuracy of the proposed SACACA is high when compared to the Existing SACA method. From Figure 3 and 4, it is also clear that the proposed system shows low value of the RMS Error and hence proves their effectiveness in accuracy on the detection of the compromised Aggregator nodes.

5. Conclusion

Secure aggregation against Collusion Attacks and Compromised aggregator (SACACA) is proposed. The proposed work concentrates on the detection of the malicious aggregator. The enhanced IF algorithm is implemented on the set of aggregators to calculate the variance values of each aggregator. Thus the proposed work presents an energy efficient framework that detects the compromised aggregator in the network. As the aggregator of the cluster changes once in a while, it proves that it saves a significant amount of energy and power of computation and also helps in the detection of the compromised aggregator simultaneously.

6. References

1. Sabrina Sicaria, Luigi Alfredo Griecob, Gennaro Boggiab, Alberto Coen-Porisinia. DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. *Journal of Systems and Software*. 2012; 85(1), 152-166.
2. Miloud Bagaaa, Yacine Challalb, Abdelraouf Ouadjaouta, Noureddine Laslaa, Nadjib Badachea. Efficient data aggregation with in-network integrity control for WSN. *Journal of Parallel and Distributed Computing*.2010; 72(10), 1157-1170.
3. Ho, Jun-Won, Matthew Wright, Sajal K. Das. ZoneTrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing. *Dependable and Secure Computing, IEEE Transactions*. 2012; 9(4), 494-511.
4. Jeba, S.V. Annlin, B. Paramasivan. Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks. *Computers & Electrical Engineering*. 2013; 39(6), 1867-1879.
5. Hajibabaei, Fatemeh, Mohammad Hossein Yaghmaee Moghaddam. Proposing a centralized trust management system to detect compromised node in WSN. *Computer and Knowledge Engineering (ICCKE)*, 2013 3th International eConference on. IEEE, 2013.
6. Li, Xiaoyong, Feng Zhou, Junping Du. LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. *Information Forensics and Security, IEEE Transactions*.2013; 8(6), 924-935.
7. Wang, Jianxin, et al. Defending collaborative false data injection attacks in wireless sensor networks. *Information Sciences*. 2014; 254, 39-53.

8. Roy Sandip, M. Conti, S. Setia. S. Jajodia. Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. *Information Forensics and Security, IEEE Transactions*. 2014; 9(4), 681-694.
9. Hongjuan Lia, Keqiu Lia, Wenyu Qub, Ivan Stojmenovicc. Secure and energy-efficient data aggregation with malicious aggregator identification in wireless sensor networks. *Future Generation Computer Systems*.2014; 37, 108-116.
10. Zhide Chen, Cheng Qiao, Yihui Qiu, Li Xu, Wei Wu. Dynamics stability in wireless sensor networks active defense model. *Journal of Computer and System Sciences*.2014; 80(8), 1534-1548.
11. M. Rezvani, A. Ignjatovic, E. Bertino, S. Jha. A trust assessment framework for streaming data in WSNs using iterative filtering. Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on. IEEE, 2015.
12. Boudia, Omar Rafik Merad, Sidi Mohammed Senouci, Mohammed Feham. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. Ad Hoc Networks.2015; 32, 98-113.
13. Labraoui, Nabila. A reliable trust management scheme in wireless sensor networks. Programming and Systems (ISPS), 2015 12th International Symposium on. IEEE, 2015.
14. 14.Illiano, P. Vittorio, Emil C. Lupu. Detecting malicious data injections in event detection wireless sensor networks. Network and Service Management, IEEE Transactions.2015; 12(3), 496-510.
15. Wagner, David. Resilient aggregation in sensor networks. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, ACM, 2004.
16. M. Rezvani, A. Ignjatovic, E. Bertino, S. Jha. Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. Dependable and Secure Computing, IEEE Transactions on 12.1 (2015): 98-110.
17. J. Jasmine jose, B. Prasath. An Enhanced Wormhole Detection Approach for Hop by Hop Message Authentication, *Indian Journal of Innovations and Developments*. 2014; 3(4), 74-79.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

***Citation**:*

Mohanraj Govindaraj, Saritha Karthik. Secure aggregation against Collusion Attacks and compromised aggregator. *Indian Journal of Innovations and Developments.* 2015; 4 (8), December.