Energy Efficient Secure Data Aggregation in Wireless Sensor Network

Shilparani[1] Yogita Patil[2]
[1,2]Appa Institute of Engineering and Technology, Kalaburgi, Karnataka, India

Abstract— Wireless Sensor Network (WSN) comprises of an expansive number of asset compelled sensor nodes. These sensor0nodes impart over wireless medium to play out an assortment of data handling usefulness. Because of constrained assets the measure of information transmission in network ought to be lessened. Information aggregation is new strategy for the above reason. Aggregation of information from various sensor nodes done at the accumulating node is normally proficient by straightforward techniques, for example, averaging. However such aggregation is known to be very presented to node bargaining attacks. The current iterative sifting system, which is altogether stronger against impact attacks. Distinguishing traded off aggregator is the one the settling issue to address this security issue. So an approach is utilized as cutting advanced0encryption0standard (AES) for mystery key encryption. These keys are utilized to give security in information aggregation and at first sender produce mystery key which is utilized to encode or decode whatever information is being sent to nodes. Encoded key is shared between the0intermediate0node can checks the key from the aggregated information sent by the Cluster Head, subsequent to confirming the keys the base station can get the amassed information. The outcome demonstrates proposed plot is secure and productive for solid information transmission.

Key words: Energy Efficient, Secure Data Aggregation, Wireless Sensor Network

I. INTRODUCTION

WSN is one of the biggest developing sorts of networks today. WSN regularly comprises of a substantial number of minimal effort sensor nodes that have entirely constrained detecting, calculation, and communication abilities. Wireless networks are confronting many sorts of security related attacks, for example, false information infusion, information forgery and eavesdropping. Because of asset confined sensor nodes, it is critical to limit the measure of information transmission with the goal that the normal sensor lifetime and the general data transfer capacity usage are made strides. Information aggregation is the strategy of a bridging and joining sensor information keeping in mind the end goal to lessen the measure of information transmission in the network. As WSNs are typically sent in remote and unfriendly situations to transmit touchy data, sensor nodes are inclined to node trade off attacks and security issues, for example, information secrecy and respectability is critical sensor network.

Information Aggregation is one of the strategies to diminish the correspondence trouble in which a sensor node named information aggregator, procedures and totals approaching information before passing it to its neighbor node. Information Aggregation is the basic method to accomplish vitality proficiency by decreasing information excess and improve the transmission capacity use. Clearly, with vitality utilization the security of WSN should likewise be contemplated, when they are sent in a shaky domain. A few security instruments can be utilized to keep the Data Aggregation process secure, for e.g., cryptography, key administration, MAC (Message Authentication Code) system. Because of a requirement for quality of observing and minimal effort of the nodes, WSNs are normally excess Information from different sensors is accumulated at an aggregator node which at that point advances to the base station .At present, because of confinements of the figuring force and vitality asset of sensor nodes, information is amassed by exceptionally basic calculations, for example, averaging. Be that as it may, such aggregation is known to be extremely presented to shortcomings, and all the more significantly, malevolent attacks. Hence information aggregation at the aggregator node must be joined by an estimation of dependability of information from singular sensor nodes. Along these lines, better, more refined calculations are required for information aggregation later on WSN.

II. LITERATURE SURVEY

The author S.Ozdemir, et.al.in [1] explained information aggregation is the way toward compressing and consolidating sensor information with a specific end goal to diminish the measure of information transmission in the network. As WSNs are generally conveyed in remote and unfriendly conditions to transmit delicate data, sensor nodes are inclined to node trade off attacks and security issues, for e.g., information classification and uprightness are critical. Henceforth, wireless sensor network conventions, e.g., information aggregation convention, must be planned on account of security. This paper gives a definite audit of secure information aggregation idea in wireless sensor networks. To give the inspiration driving secure information aggregation, to begin with, the security necessities of wireless sensor networks are introduced and the connections between information aggregation idea and these security prerequisites.

The author M.Zakirul, et.al.in [2] explained about safety protocols have been regularly used to ensure secure correspondence in networked frameworks. Such protocols might be spilled by a complex intrigue assault. Prior to an assault is made; the node is by all accounts working appropriately, speaking with others, and giving right esteems/choices. Right now, there is no efficient technique for recognizing such an assault. In this paper, writer offers CAD, a Collusion Attack Detection plot for networked frameworks. In wireless nodes more often than not have some relationship designs in correspondence measurements (e.g., radio planning, measure of bundles transmitted). At the point when there is a significant in consistency in such examples with a node, the node is said to be conspired. Computer aided design finds the connection between's framework measurements identified with correspondence equipment or programming utilizing two phase cross approval plans to distinguish collusion.

The author Y. Zhou, et.al.in [3] presents, a reputation algorithm which is based on correlation model and used in web based rating system to solve the ranking problem that can be generated by the influence of spammer attack. Writer represents user's repute by consuming correlation measurement and iterative technique to find similarity between users rating vector and objects weighted average rating vector. Proposed algorithm is more efficient and robust but still the exactness of algorithm can be improved.

The author H. Lee, et.al.in [4] presents an iterative technique for trust and reputation administration denoted as ITRM. The future calculation can be connected to concentrated plans, in which a focal specialist gathers the reports and structures the reputations of the specialist organizations and also report/rating reliability of the shoppers. The recommended iterative calculation is motivated by the iterative deciphering of low-thickness equality check codes over bipartite diagrams. The plan is hearty in sifting through the associates who give questionable evaluations. Examination of ITRM with some outstanding notoriety administration systems demonstrates the predominance of plan both as far as power against attacks and proficiency.

The author H. Cam, et.al.in [5] WSNs traded off sensor nodes can infuse false information during both information aggregation and information sending. The current false information location methods consider false information infusions amid information sending just and don't permit any change on the information by information aggregation. This paper displays adata0aggregation and0authentication protocol called0DAA, to coordinate false information recognition with information aggregation and privacy. To help information aggregation alongside false information identification, the observing nodes of each information aggregator likewise lead information aggregation and register the relating little size message validation codes for information check at their combine mates. To help secret information transmission, the sensor nodes between two successive information aggregators check the information honesty on the scrambled information as opposed to the plain information. DAA recognizes any false information infused by up to traded off nodes, and that the identified false information are not sent past the following information aggregator on the way. Notwithstanding that false information discovery and information secrecy increment the correspondence overhead, reproduction comes about demonstrate that DAA can even now decrease the measure of transmitted information by up to 60% with the assistance of information aggregation and early location of false information.

III. METHODOLOGY

The system proposes a key based approach for preventing blocking of nodes and to identity the collusion attack. In this report the information will be generated based on key value. This key will be encrypted and that will be send to the nearest node. Then the data or information value will be sent along with the same key value. To decrypt the key that will check whether the keys will be matched or not.(i) If it match then there will not be any attack.(ii) Otherwise the key will be hacked.

IV. IMPLEMENTATION

A. Modules

- Sender
- Intermediate Node
- Aggregator Node
- Base station
- Attacker
- Modules Description

B. Sender:

In this module the sender has to click on open button and select the file (txt, doc, html etc.) and the file content can view in the textarea and enter the secret key value and click on generate key button and then got to send tab the secret value is encrypted and can view in textarea and click on get file button the file content can view in textarea and sender has to select the intermediate nodes and click on transfer button the data will sent to the intermediate node.

C. Intermediate nodes:

In this module i.e. cluster node 1 form go to data tab enter the secret key value and click on generate key then go to receive tab click on aggregate button if both the secret key values are match then data is aggregated in node 1 from and if the secret key values are mismatched then data is not aggregated in cluster node1 and so on and send data to Aggregator node.

D. Aggregator Node:

In this module the data will come from the intermediate node i.e. from cluster nodes to aggregator nodes. The aggregator node takes data from each cluster nodes & sends to base station.

E. Base station:

In this module base station receives the information from the aggregator nodes. In base station we can view the file content in the textarea which the sender has sent to the base station via intermediate and aggregator nodes.

F. Attacker:

In this module the attacker wants to attack the file in the aggregator node. If the attacker has attacks to aggregator node 1 then the information will not send to the aggregator node 1 because the attacker are attacked to this aggregator node 1 and if the attacker has attacks to aggregator node 2 then the information will not send to the aggregator node 2.

V. RESULT ANALYSIS

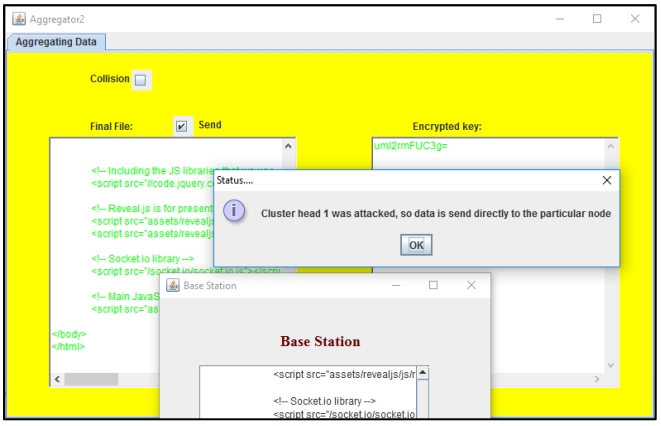

Fig. 5.1: Home Screen

This figure 5.1 shows the home screen. where we need to select the desired file which we want to send to a destination. The data will be displayed in an textbox. After words that information file is transferred to nearest node with secret key this key will be in the form encrypted key this key is checked at aggregator node if key doesn't match with enter secret key then data will not aggregate at base station this indicate attack at node.

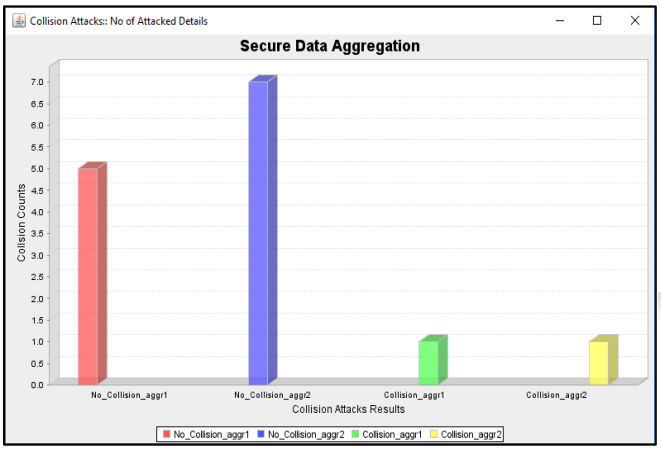

Fig. 5.2: Collision attack at aggregator nodes.

The above figure 5.2 indicates graph which gives the collision attack details with respect to collision count. Whenever attack at any one of the aggregator node has been hacked the information will be stored in the database. By using this key approach between nodes we can provide secure and efficient data transmission can be taken place.

VI. CONCLUSION

The concept of secure data aggregation with compromised aggregator node identification is performed in WSN. The data transmission from source to recipient using intermediate node The key based approach provides a way to Securing against collision Attacks. The goal of proposed work is to make sure that base station does not accept the forged aggregation information from intermediate node and also the aggregators tampering with intermediate result can be identified. From the result it is clear the data aggregation with sharing secret key provide reliable data transmission and increase security level. The result indicates proposed scheme is secure and efficient. In future work, will examine whether this methodology can defend against compromised multiple aggregators and likewise plan to implement method in a deployed sensor network.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Computer. Network, vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] Md Zakirul Alam Bhuiyan, "Collusion Attack Detection in Networked Systems" Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA

[3] Y. Zhou, T. Lei, and T. Zhou,"A robust ranking algorithm to spamming" Europhys. Lett vol. 94, p 48002, 2011

[4] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.

[5] Hasan Çam, Suat Ozdemi, "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks" Ieee/Acm Transactions On Networking, Vol. 18, No. 3, June 2010.

