Tree Based Secure Data Aggregation in WSN on Cloud

[1]Shrutika Kapadne, [2]Dhanokar Prajakta, [3]Pratiksha Doshi, [4]Tejas Ingle, [5]Prof. P.P.Jorvekar, [6]Milind Ankleshwar

[1,2,3,4]Students, [5]Professor, [6]Director of Mass Technology
Computer Engineering,
N.B.N.Sinhgad School Of Engineering, Pune,India

***Abstract*: Simple wireless sensors has restrictions on how efficiently wireless sensors can be used due to resource limitation. Latest models of communicating with wireless sensors such as Internet of Things and Sensor Cloud focus to overcome these restrictions. Sensor cloud architectures, which enable different wireless sensor networks, spread in a huge geographical area to connect together and be used by multiple users at the same time on demand basis. We will implement virtual scenario assist in creating a multiuser environment on top of resource constrained physical wireless sensors and can help in supporting multiple applications on-demand basis.**

***Index Terms*: Data Aggregation, Sensor Network Security, Synopsis Diffusion, Attack-Resilient**

I. INTRODUCTION

Wireless Sensor Networks are used to gather the information from various devices or sensor over a geographic area. So the gathered information from sensors is collected at a hub called aggregator node and the values that are aggregated must be sent to the cloud via base station. At present, because of constraints of the computing power and resource of sensor nodes, information is aggregated by simple algorithms such as averaging. Such aggregation is known to be very vulnerable to faults and all the more essentially, malicious attacks. This can't be helped by cryptographic techniques, in light of the fact that attackers generally gain complete access to data stored in the compromised nodes. Consequently information aggregated at the aggregator node must be joined by an assessment of trustworthiness of data from individual sensor nodes. Therefore, better advanced algorithms are required for data aggregation in WSN and cloud. Trust and reputation have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). In spite of the fact that sensor systems are by and large progressively conveyed in numerous application areas, assessing trustworthiness of reported information from distributed sensors has remained a challenging issue. Sensors deployed in hostile environments maybe subject to node compromising attacks by adversaries who intend to inject false data into the system. So, we propose a bandwidth-efficient
Cooperative authentication (BECAN) scheme for separating infused false information. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication method.

II. LITERATURE REVIEW

Synopsis diffusion approach secure against the above assault propelled by the traded off nodes. In specific, algorithm to empower the base station to safely compute predicate Count or Sum even in the nearness of such an assault.Theirattack-resilient computation algorithm registers thetrue aggregate by filtering out the contributions of traded off nodes in the total chain of command. Exhaustive hypotheticalanalysis and extensive simulation study which was introduce by Roy, Mauro Conti, SanjeevSetia, and SushilJajodia [1].

TaochunWang, JiZhang introduced theSCIDA, which propose a safe and concentric-circle itinerary-based data aggregation calculation (called SCIDA for short). Utilizes a safe channel to guarantee information protection and maintains a strategic distance from emotional vitality utilization caused by heavy encryption operations. SCIDA does not have to carry out encryption during data aggregation, which fundamentally diminishes energy utilization, and draws out the lifetime of the system [2].

Iterative Filtering calculations were discovered to be exceptionally usefulwhich was implemented byUma Angadi1, G.F Ali Ahammed.These calculations all the while total information from numerous sources and give a trust estimation of these sources, for the most part in a type of comparing weight factors allocated to information given by each source. Some data aggregation mechanisms and presented another confounded collision attack with its effect on remote sensor systems [3].

A Robust Data Aggregation Method (RDAM) e algorithm is to estimate a set of non-equal initial weights for the readings is proposed by AnesYessembayev and DilipSarkar .The objective of the method is to calculate smaller initial weights for the readings of the compromised sensors. Results of extensive empirical evaluation of the RDAM method against other methods demonstrated highest accuracy for both simple and collusion attacks [4].

Priyanka G.P., K.G. Bagde introduce the Secure information conglomeration by utilizing sink devices and expounded a novel bandwidth scheme efficient cooperative authentication (BECAN) plot for filtering the infused false information. By hypothetical examination and simulation evaluation, the BECAN scheme has been shown to accomplish not just high en-routing separating likelihood yet in addition high reliability quality with multi reports[5].

III. PROPOSED SYSTEM

sensor networks are typically deployed at unattended or hostile environments. Therefore, they are really hard to verify security attacks, like selective forwarding, wormholes, and Sybil attacks. For above attacks and vulnerability in WSN, the BECAN scheme may be applied to secure data aggregation by using sink node and a novel bandwidth scheme efficient cooperative authentication (BECAN) scheme for filtering the injected false data.BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi reports. BECAN scheme supported the random graph characteristics of sensor node demonstration and thus the cooperative bit-compressed authentication technique, the proposed BECAN scheme can save energy by early detecting and separating the majority of infused false information with minor additional overheads at the path of node . Also applied statistical en-routing filtering mechanism called SEF. SEF wants to verify the MACs, and uses them to produce the MACs. And also to save the bandwidth, SEF adopts the bloom filter to reduce MAC size.

Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability however additionally high reliability

-First, we tend to study the random graph characteristics of wireless device node preparation, and estimate the probability of k-neighbour's, that provides the required condition for BECAN authentication.

-Second, we tend to propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data will be early detected and filtered by the en-route device nodes. Additionally, the accompanied authentication information is bandwidth-efficient.

-Third, we tend to develop a custom simulator to demonstrate the effectiveness of the planned BECAN scheme in terms ofen-routing probability and false negative rate true reports.Therefore, it's crucial to filter the false data as accurately.

As well as security at cloud level is essential, to provide security and privacy for data onCloud we are using encryption and decryption algorithms.Encryption algorithm like DES,AES etc are used to encrypt the data stored on cloud to avoid data misuse by attackers.Decryption algorithms are used to decrypt the encrypted data.

IV. SYSTEM ARCHITETURE

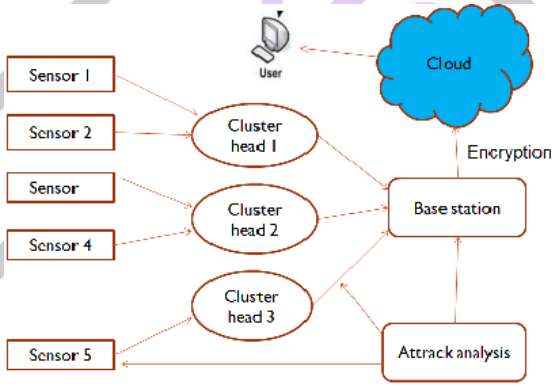

Figure-1: System Architecture

V. CONCLUSION

We presented an attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack.

Our algorithm requires less communication and computation overheads than previously known methods and can effectively preserve data privacy, check data integrity, and consuming less energy to prolong network lifetime.

REFERENCES

[1] Roy, Mauro Conti, SanjeevSetia, and SushilJajodia, Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact, IEEE transactions on information forensic and security vol:9 no:4 year 2014

[2] TaochunWang,JiZhang,YonglongLuo, KaizhongZuo, Xintao Ding, An Efficient and Secure Itinerary-based Data Aggregation Algorithm for WSNs, 2017 IEEE Trustcom/BigDataSE/ICESS

[3] Uma Angadi1, Dr. G.F Ali AhammedAnalysis of Secure Data Aggregation Technique for Wireless Sensor Network in the Presence of Adversary Environment based on IF algorithm, *International Journal of Advanced Research in Computerand Communication Engineering Vol. 5, Issue 4, April 2016*

[4] AnesYessembayevDilipSarkar Secure Data Aggregation Algorithms for Sensor Networks in the Presence of Collusion Attacks The First IEEE International Workshop on Security, Privacy and Trust for IoT, 2016

[5] Miss. Priyanka G. Padmane1, Prof. K.G. Bagde,Secure Data Aggregation in Wireless Sensor Network using BECAN *International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 10, October 2015*