International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 04 | April -2019 ISSN: 1847-9790 || p-ISSN: 2395-0126

Implementation of Secure Data Aggregation in WSN

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

[1]*Student & NBN SSOE,PUNE*
[1]*Student & NBN SSOE, PUNE*
[2]*Student & NBN SSOE, PUNE*
[3]*Student & NBN SSOE, PUNE*
[4]*Student & NBN SSOE, PUNE*
[5] *Professor & NBN SSOE, PUNE*

Abstract - *Simple wireless sensors has confinements on how effectively remote sensors can be utilized because of asset constraint. Most recent models of communication with remote sensors, for example, Internet of Things and Sensor Cloud center to defeat these limitation. Sensor cloud structures, which empower distinctive wireless sensor systems, spread in an immense land zone to interface together and be utilized by various clients in the meantime on interest premise. We will actualize virtual situation help with making a multiuser environment over asset constrained physical remote sensors and can help in supporting numerous applications on-request premise.*

Key Words **:***Data Aggregation, Sensor Network Security, Synopsis Diffusion, Attack-Resilient*

1.INTRODUCTION

Wireless Sensor Networks are utilized to accumulate the data from different gadgets or sensor over a geographic territory. So the assembled data from sensors is collected at a center point called aggregator hub and the qualities that are collected must be sent to the cloud by means of base station. At present, because of limitation of the computing power and resource of sensor nodes, data is collected by straightforward calculations, for example, averaging. Such total is known to be truly helpless against shortcomings and even more basically, malicious attacks. This would not benefit from outside intervention by cryptographic procedures, in light of the way that attackers mostly got complete access to information put away in the compromised nodes. Subsequently data totaled at the aggregator hub must be joined by an appraisal of reliability of information from individual sensor hubs. Along these lines, better advance algorithms are required for information aggregation on cloud by WSN. Trust and reputation have been as of late proposed as a compelling security measures for Wireless Sensor Networks (WSNs). Despite the way that sensor frameworks are all things considered logically passed on in various application regions, evaluating reliability of announced data from different sensors has remained a testing issue. Sensors sent in unfriendly conditions perhaps subject to hub compromising attack by enemies who plan to infuse false information into the framework.

2. LITERATURE REVIEW

1. Abstract dispersion approach secure against the strike pushed by the exchanged off hubs. In explicit, algorithm to enable the base station to securely process predicate Count or Sum even in the proximity of such an assault.Thei rattack-flexible calculation registers the true total by sifting through the commitments of exchanged off hubs in the complete levels of leadership. Thorough hypothetical analysis and broad reproduction consider which was present by Roy, Mauro Conti, SanjeevSetia, and SushilJajodia [1].

2. Taochun Wang, Ji Zhang presented the SCIDA, which propose a concentric-circle itinerary-based based information accumulation computation (called SCIDA for short). Uses a sheltered channel to ensure data insurance and keeps up a vital separation from passionate imperativeness use brought about by overwhelming encryption activities. SCIDA does not need to do encryption amid information collection, which in a general sense lessens vitality use, and draws out the lifetime of the framework [2].

3. AES algorithm was intended to have obstruction against every single known attacks, speed and code smallness on a wide scope of stages and design simplicity. AES 128-piece keys has more grounded protection from a exhaustive key search. It is a substitution permutation network. Each round in AES encryption incorporates four distinctive round changes: Substitute Bytes, Shift Rows, Mix Columns and Add Round Key[3].

4. Nandini. S. Patil and Prof. P. R. Patil explain The point of the proposed work is to think about the

execution of TAG as far as energy effectiveness in correlation with and without data aggregation in remote sensor systems and to survey the appropriateness of the protocol in a situation where resources are restricted[4].

5. Correspondence misfortunes coming about because of hub and transmission fail, which are basic in WSNs, can antagonistically influence tree-based accumulation approaches. To address this issue, Mrs.Saba Sultana and Mr.Kanike utilize multi-way routing methods for sending sub-totals. For duplicate insensitive totals, for example, Min and Max, this methodology gives an issue tolerant arrangement. Unfortunately, for duplicate sensitive totals.,such as Count and Sum, multi-way routing prompts double counting of sensor readings[5].

3. DISADVANTAGES OF EXISTING SYSTEM

i. A sensor hub has limitation as far as calculation ability and energy reserves.
ii. Technique is restrictively costly as far as communication overhead.
iii. The likelihood of node compromise presents more difficulties in light of the fact that a large portion of the current in-network aggregation algorithms have no arrangements for security.
iv. A compromised node may endeavor to upset the aggregation procedure by propelling a few attacks, for example eavesdropping, jamming, message dropping, active and passive attack, and so on.

4. PROPOSED SYSTEM

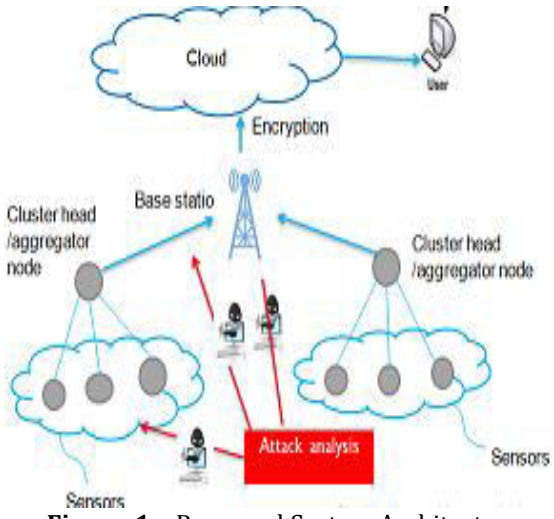

Figure-1: Proposed System Architecture

In a small area location such as a house, office or in a classroom, there is a small network called a Local Area Network (LAN). Our project aims to transfer a file peer-to-peer from one computer to another computer using JAVA application in the same LAN and at the time of attack detection and after attack analysis by using multipath routing and shortest path we can transfer data to base station (destination). For shortest path here we can use dijkshtra algorithm .By using this application ,we can provides the necessary authentication for file transferring in the network transmission. By implementing the Server-Client technology, we can use a File Transfer Protocol mechanism and through socket programming, the end user is able to send and receive the encrypted and decrypted file in the LAN. An additional aim of this project is to transfer a file between computers securely in LANs. Elements of security are needed in this project because securing the files is an important task, which ensures files are not captured or altered by anyone on the same network. Whenever you transmit files over a network, there is a good chance your data will be encrypted by encryption technique. In this project, an AES algorithm is used to encrypt the file that needs to transfer to another computer. The encrypted file is then sent to a receiver computer and will need to be decrypted before the user can open the file. The file is expected to be transferred securely and without being modified because it is fast. In addition after successful file transfer we can store data on cloud to give access to authenticate user as well as security at cloud level is important, to supply security and privacy for information/data which store on Cloud we tend to use Encryption algorithmic program like AES etc are used to encrypt the data stored on cloud to avoid data misuse by attackers .Decryption algorithm are used to decrypt file into user readable format.

5. MODULES

1. Setting up Network Model
2. Data aggregation
3. Falsifying the local value
4. Attacks analysis
5. Performance Analysis
6. Cloud Storage

5.1 Description of modules :

5.1.1. Setting up Network Model:

Our first module is fixing the network model. we have a tendency to consider a large-scale, same sensor network consisting of resource-constrained sensing element nodes. Analogous to previous distributed detection approaches; we have a tendency to assume that associate degree identity-

based public-key cryptography facility is offered within the sensor network.

5.1.2. Data aggregation:

Data aggregation is taken as one of the essential spread data processing measures to save lots of the energy and also the fundamental plan is to collect the data from totally different sources, redirect it with the removal of the redundancy and thereby reducing the quantity of transmissions and additionally saves energy.

5.1.3. Falsifying the local value:

A compromised node will falsify its own sensor node reading with the goal of influencing the aggregate worth value. We have a tendency to assume that if a node is compromised; all the data it holds are going to be compromised. We consider that all malicious nodes can be under control of single attacker. We have a tendency to use a Becan scheme, can save energy by early detecting and filtering the majority of injected false data by supporting graph characteristics of sensor node demonstration and co-operative bit compressed authentication technique. However, we assume that the attacker does not launch *dos* attacks, e.g., the multi-hop flooding attacks with the goal of making the whole system *unavailable*.

5.1.*4.* Attacks analysis:

BS ought not to receive authentication messages from all of the nodes. so algorithmic rule decision the attack-resilient computation algorithmic rule that is in 2 phases. The first section, the Base station received authentication data from the nodes. The second section, the Base station demands a lot of authentication data from only a set of nodes.

At the last of the second section, the Base station will separate out the false contributions of the compromised nodes from the collection to minimize the communication overhead.

5.1.5. Performance Analysis

In the proposed model, we use the following parameter to evaluate its performance:

- Number of (Unique) MACs
- Average Nodes Sent bits

5.1.6. Cloud storage:

In our propose system ,Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote cloud storage based on internet. Our computer and the database create connection between them by using internet. On the surface, cloud storage so it store number of files & ,compressed data on cloud storage and also give access to user anytime ,anywhere.

6. ALGORITHM

Our model use algorithms are as follows:

1. Advanced Encryption Standard Algorithm
2. Dijkstra's Algorithm

6.1 Description of algorithms:

1. Advanced Encryption Standard Algorithm(AES):

- AES is that the short form of Advanced Encryption Standard. It's radically symmetrical block cipher which might encrypt and decrypt information.
- Encryption part converts (data) Plain text into cipher text form while decryption part converts cipher text into plain text (text form of data).
- AES is implemented in each hardware and software package to protect digital information in numerous forms like data, voice, video etc. from attacks or eavesdropping. It is fast, compact and has a very simple mathematical structure that might build AES encryption and decryption processes faster than others algorithm

Advantages of AES Algorithm:

I. It uses higher length key sizes such as 128, 192 and 256 bits for encryption. So it is makes AES robust due to which it is prevent from hacking.
II. It is used in several of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
III. By using no one can hack your personal information.

2. Dijkstra's Algorithm:

- DIJKSTRA algorithm can be used to compute shortest paths from a single node to all other nodes, so it's used in many routing protocols.
- Routers are based on dijkstra algorithm, Dijkstra's is used for computing shortest path between two nodes in a efficient time.
- Time Complexity of Dijkstra's Algorithm: O(E log V)

Advantages of Dijkstra's Algorithm:

I. To find locations of Map which refers to vertices of graph.
II. Distance between the locations refers to edges.

III. It is used in IP routing to find Open shortest Path First.

7. METHODOLOGIES:

In this paper, methods and tools have been utilized is the most recent procedures, for example, Data NetBeans application to build up a file transfer system by using JAVA socket programming socket gives the correspondence component between two PCs utilizing Transmission Control Protocol (TCP). TCP is an connection-oriented protocol. To impart over the TCP protocol, an association should initially be built up between the pair of socket. While one of the socket accepts the connection request (server), the connection is asked by another socket (client).attempts to connect the socket to a server the customer program create that socket for communication. When two sockets have been associated, they can be utilized to transmit information in possibly one or the two ways.

Cloud computing is the conveyance of various services through the web. Data storage, servers, databases, networking, and software like these applications and resources are provided by the cloud computing. As opposed to keeping documents on an exclusive hard drive or local storage, cloud-based capacity makes it conceivable to spare them to a remote database. Up to an electronic device approaches the web, it approaches the information and the software projects to run it.

AES is symmetric encryption utilize a similar key for utilizing an encoding and decoding, so both the sender and the beneficiary must know and utilize a similar secret key. Symmetric encryption necessitates that the secret key be known by the send party those are encoding the information and the receiving party those are decoding the information. AES-128 indicate to bit key lengths that are deemed adequate to secure grouped data up to the "secret" level with "Top Secret" data. by repeating the same steps several times AES encrypt the data. AES algorithm is changed to make it reasonable for document transfer situations. AES coordinates with frameworks that have been created at the SEND button to begin encryption procedure. The decoding procedure happens when cipher text changes over to plaintext toward the finish of transmission when the document is gotten by the receiver.

8. ADVANTAGES OF PROPOSED SYSTEM

I. We build the synopsis diffusion method secure against the falsified sub-aggregate attack.
II. Those algorithms we are use our model are outperforms alternative existing approaches in many metrics, like the communication overhead. We tend to declare that the communication overhead of our algorithm may be higher if the belief concerning compromised nodes being uniformly distributed doesn't hold.
III. Our model is more secure by this parameter confidentiality, integrity, authenticity.
IV. According to Confidentiality Sensor data/readings cannot be disclosed to attackers.
V. In Integrity parameter, If an adversary modifies a Data message, the receiver Should be able to detect this Tampering.
VI. Due to Authenticity parameter Ensures that data messages come from the intended Sender.
VII. Our model provides security and scalable environment to data which store on cloud by using encryption and decryption method.
VIII. Our model provide result by consider this metrics are high data transmission efficiency, and less energy to Prolong network lifetime.

9. RESULT ANALYSIS:

In our application at the time of result analysis ,we consider two parameter which are as follows:

1. Data loss or not during file transfer at the time of attack.
2. Time require to transfer file with attack or without attack.

The sender and receiver are connected in the same network to establish a connection. Then, as an example for the analysis, the “pppp.txt” file of size 45 byte was chosen by the sender from the “Documents” folder. The file has been successfully transferred securely to destination without losing data means the size of file remain same which was 45 byte and in very less time means 35 millisecond.

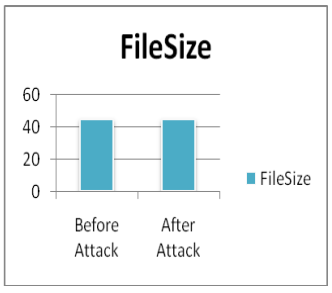

Fig1: data loss

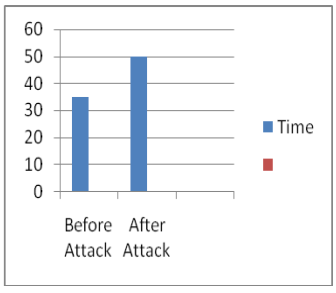

Fig: time required

But at situation of attack happen for result analysis ,we again chosen file pppp.txt file which is 45 byte from document folder then by giving IP of attacker node (node 4),we successfully send the file to destination that time .the attack happen at node 4 then transmission paused for little time after this moments transmitting status goes to safe

state by using multipath routing and shortest path, file has been again send to destination. so at the time of attack happened ,it take more time(50 millisecond) to transfer file because it take time to chooses another and shortest path additionally after attack also file size remain same which was 45 byte so we consider data cannot loss at the time of attack in process of file transmission and also transmission take more time to chosen another and shortest path at the time of attack as compare to transmission of file without attack to destination.

Due to this our application generate result that file can be securely and successfully transfer to destination at the time of attack also.

10. CONCLUSIONS

In this paper, we have mentioned the protection vulnerabilities of data aggregation proto-cols for sensing element networks. We tend to additionally confer a survey of secure and resilient aggregation protocols for each single aggregator. We present associate degree of attack-resilient computation algorithm which might guarantee the computation of the aggregator even within the presence of the attack. Our algorithm needs less communication and computation overheads than antecedently noted ways and may effectively preserve information privacy, check information integrity, and overwhelming less energy to prolong network period of time. Our model is designed for sensor networks, over cloud, it can also be adopted in wireless network and the future work is designed model in mobile networks. Where the goal is to provide access control in collaborative and data aggregation scenario.

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] Nor Surayati Mohamad Usop, Ahmad Faisal Abidin, Fauziah Ab. Wahab , Securing File Transferring System by Implementing AES Algorithm, World Applied Sciences Journal 35 (New Advancement of Research & Development in Computer Science): 122-132, 2017

[4] Nandini. S. Patil, Prof. P. R. Patil, Data Aggregation in Wireless Sensor Network, 2010 IEEE International Conference on Computational Intelligence and Computing Research

[5] Mrs.Saba Sultana, Mr.Kanike Srinivasulu , Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact, International Journal & Magazine of Engineering, Technology, Management and Research A Peer Reviewed Open Access .