ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Secure Data Aggregation for Wireless Sensor Networks in the Presence of Collusion Attacks

Siddharth C Sawai[1], Prof. S. N. Shelke[2]

M.E, Dept. of Computer Science And Enigneering, Sinhgad Academy of Engineering, Kondhwa, Pune, Maharashtra, India [1]

Assistance Professor, Dept. of Computer Science And Engineering, Sinhgad Academy of Engineering , Kondhwa, Pune, Maharashtra, India [2]

ABSTRACT:Information accumulation assumes a significant half in remote sensing element systems (WSNs) to the extent it decreases management utilization and supports the ability of the system, significantly in topologies that square measure inclined to bottlenecks (e.g. bunch trees). To restricted machine power and vitality assets, conglomeration of knowledge from varied remote hubs done at the amassing hub is generally refined by basic techniques, as an example, averaging. but such accumulation is thought to be passing defenceless against hub mercantilism off assaults. The framework proposes a sprout separation calculations hold awing guarantee for such a reason. Such calculations at constant time total data from varied sources and provides trust analysis of those sources, a lot of usually than not in an exceedingly variety of relating weight components meted out to data gave by each supply. Moreover, the framework in addition a lot of powerful against agreement assaults than the easy averaging techniques, square measure all things thought-about susceptive to a completely unique trendy intrigue assault given. to deal with this security issue, we tend to propose procedures by giving associate degree underlying guess to such calculations that makes them intrigue powerful, additionally as a lot of precise and faster change of integrity.

KEYWORDS: Wireless Ad-hoc Networks, Robust Data Aggregation, Collusion Attacks, WSN.

I. INTRODUCTION

Wireless sensing element networks (WSNs) incorporates massive numbers of sensing element nodes to observe environmental conditions, like pressure, temperature and then on. Attributable to the prevalence of low price and organisation, WSNs area unit applied to several fields, like health care, atmosphere observance and military sensing.
Information from over one sensing element is mass at an somebody node that then forwards to the lowest station solely the mixture values. At present, thanks to obstacles of the computing strength and electricity helpful resource of nodes, information is mass by mistreatment a very simple algorithm which incorporates averaging. But, such aggregation is assumed to be terribly vulnerable to faults, and larger significantly, malicious attacks. This can't be remedied by means that of cryptologic ways, as a result of the attackers sometimes gain whole get admission to statistics hold on inside the compromised nodes. For those reason facts aggregation at the somebody node should be determined by means that of assessment of trustiness of knowledge from individual sensing element nodes. For this reason, better, a lot of progressive algorithms area unit required for statistics aggregation inside the destiny WN. Such a group of rules have to be compelled to have two options. Take into account and name systems have an oversized role in supporting operation of a good sort of distributed structures, from Wi-Fi networks and e-commerce infrastructure to social networks, with the help of presenting an assessment of trustiness of people in such disbursed systems. A trustiness analysis at any given second represents a mix of the conduct of the members the maximum amount as that moment and should be sturdy inside the presence of numerous kinds of faults and malicious behaviour. There are a unit variety of incentives for attackers to control the believe and recognition many participants during a disbursed system, and such manipulation will seriously impair the performance of this kind of machine. The most goals of malicious attackers is aggregation algorithms of settle for as true with and name structures.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

II. LITERATURE SURVEY

1. Paper Name: Fast Aggregation Scheduling in Wireless Sensor Networks. [1]
Author: HamedYousefi, MarziehMalekimajd, Majid Ashouri, and Ali Movaghar.
Description:
In this paper, to minimize time latency, we tend to focus on aggregation scheduling problem and propose an efficient distributed algorithm that generates a collision-free schedule with the least number of time slots. In contrast to others, approach named FAST mainly contributes to both tree construction, where the former studies employ Connected 2-hop Dominating Sets, and aggregation scheduling that was previously addressed through the Competitor Sets computation.
Advantages: the system minimizes time latency.
Limitation: the system requiredscheduling algorithms.

2.Paper Name: A Novel Wireless Sensor Network Frame for Urban Transportation [2]
Author: Xiaoya Hu, Liuqing Yang, and Wei Xiong.
YOP: 2015
Description:
The potential application scenarios and design requirements of WSN for urban transportation (WSN-UT) are proposed in this work. A customized network topology is designed to meet the special requirements, and WSN-UT is specifically tailored for UT applications. WSN-UT allowsuser's to achieve traffic and road infostraight from the local WSN within its wireless scopes instead of the remote ITS data center. WSN-UT can be configured according to different scenario requirements.
Advantages: wireless sensor network (WSN) technologies that are low cost, low power, and self-configuring are a key function used in this paper.

3. Paper Name: Data Aggregation and Principal Component Analysis in WSNs [3]
Author:AntoniMorell, Alejandro Correa, Marc Barceló, and José López Vicario
YOP: 2016
Description:
Our contribution is aligned with PCA and explores whether a projection basis that is not the eigenvectors basis may be valid to sustain a normalized mean squared error (NMSE) threshold in signal reconstruction and reduce the energy consumption. We derivate first the NSME achieved with the new basis and elaborate then on the Jacobi eigenvalue decomposition ideas to propose a new subspace-based data aggregation method. The proposed solution reduces transmissions among the sink and one or more data aggregation nodes (DANs) in the network.
Advantages: Base stations access the observations.
Limitation: data reduction

4. Paper Name: Secure Cluster based Data Aggregation in Wireless Sensor Networks [4]
Author: S. Siva Ranjani, Dr. S. Radhakrishna, Dr. C.Thangaraj
YOP: 2014
Description:
In this paper we tent to address the data aggregation and security issues together. In our approach, we modify our Energy efficient Cluster Based Data Aggregation (ECBDA) scheme to provide secure data transmission. Since, sensors nodes are small powered in nature, it is not viable to apply standard cryptography methods. Cluster head performs data aggregation and Bayesian fusion algorithm rule to enable security. Trust is the directional relationship between two sensor nodes. By checking the trustworthiness of a node, we can enable secure communication. Bayesian fusion algorithm rule calculates the trust probability of a sensor based on the behavior of the node.
Advantages: address the data aggregation and security issues together.
Limitation: required more time for detects the untrustworthy node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

5. Paper Name: Secure Data Aggregation in Wireless Sensor Networks [5]
Author: V. Vaidehi, R. Kayalvizhi, N. Chandra Sekar
YOP: 2015
Description:
This paper proposes a novel plan to secure the procedure of information total by giving a light-weight security plot called Combinatorial Key Distribution (CKD) instrument that expends less power and its execution is enhanced utilizing hashes of information that is sent over the system. The proposed plot minimizes the power utilization and boosts the secureness of information in the remote sensor arrange. The proposed security plan is contrasted and other existing security arrangements and the outcomes are accounted for.
Advantages: to reduce the power consumption during data gathering.
Limitation: Fair approximation of the sensor readings although a limited number of nodes are compromised.

III. PROPOSED SYSTEM

Proposes an answer for such helplessness by giving an underlying trust assess which depends on a vigorous estimation of mistakes of individual sensors. At the point when the way of blunders is stochastic, such mistakes basically speak to an estimation of the blunder parameters of hubs in remote impromptu system, for example, inclination and fluctuation. Be that as it may, such gauges likewise end up being vigorous in situations when the mistake is not stochastic but rather because of facilitated malevolent exercises. Such introductory estimation makes sprout channel calculations powerful against depicted complex arrangement assault, and, we accept, likewise more vigorous under essentially more broad conditions; for instance, it is additionally viable within the sight of an entire disappointment of a portion of the sensor hubs.

3.1 Advantages of Proposed System:

1. Proposes a fix for such vulnerability through providing a preliminary trust estimate which will depend on a strong estimation of errors of human sensors.
2. Additionally it is great at the existence of a whole failure of many of the sensor nodes.

3.2 Application of Proposed System:

Used in whether forecasting.

IV. SYSTEM ARCHITECTURE

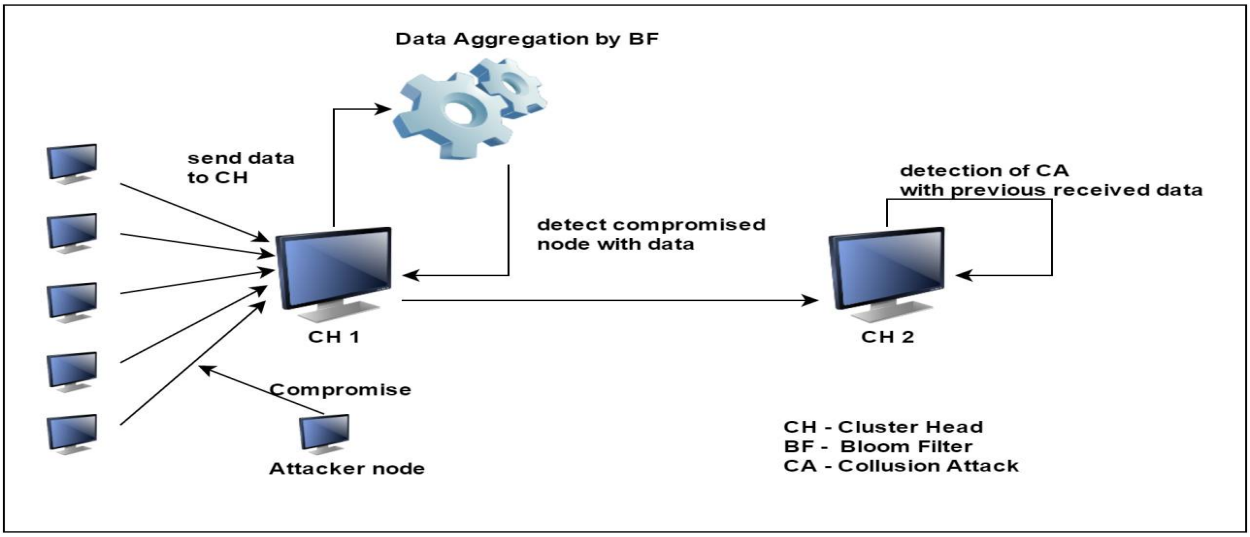

Figure 1. System Architecture of Proposed System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

V. MATHEMATICAL MODULE

Let S be the whole system,

Input:
S= {I,FileP,A,O}
Where,
I=Input to the system.
P=Processing on the Input= {Files}.
O=Output of the system.

Node= {nn,ch,an}
Where,
nn=Normal Node
ch=Cluster Head
an=Attacker Node

Process:

1. Here, nn registers and login in system.

2. nn send all data/file to cluster head.
Files= {file1, file2… file}

3. Attacker node changes the file or data.
A= {A1, A2... An}

4. Here cluster head's work get started.ch collects all data and performs aggregation. Here ch applies bloom filtering, to verify and detect compromised node. Once it detects compromised node, ch blocks the node, and forward all data from uncompromised node for further processing.

5. Another attack is collusion attack, ch further check that if there exist any colluding attack (two file contain same data), if then ch ignores the similar data.

Output: Correct data forwarded for further processing.

VI. ALGORITHM

6.1 Bloom Filter (BF):

The Filtering calculations are an attractive option for remote system since they tackle both issues information total and data dependability evaluation through the use of a solitary iterative strategy. Such dependability gauge of the sensor is dependent upon the separation with the readings of such a sensor from your gauge with the right values, got previously round of emphasis by some kind of total from the readings of most hubs. Such accumulation is commonly a weighted normal sensors whose readings fundamentally contrast from such gauge are relegated less dependability and therefore within the conglomeration procedure in our round of cycle their readings are shown a lesser weight.

Bloom Filter:
The bloom filter works on mainly two conditions false positive and false negative which specifies the received data results.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

1. Sender node

i. Capture/ sense data:
In this node will capture the data.

ii. Send:
In this data is send to CH (cluster head).

2. Aggregator/Cluster head:

In this CH can see the entire cluster nodes, there data, and status.

a. Data aggregation:

In this the CH head does data aggregation of the data received from nodes.
After performing data aggregation the CH head drops the nodes with malicious data i.e. nodes with low weight and send only the actual node data to another CH i.e. destination.

3. Hacker:

Hacker is the adversary node who compromise the node in the cluster i.e. hacker injects the false data to node.

4. Receiver:

The receiver will receive the data from sender nodes whose data is not colluded.

VII. RESULT ANALYSIS WITH GRAPH

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the accuracy, time, storage and energy cost of system. Based on this attributes we getting following analytical result for our proposed system with respect to existing system.

Expected Result:

	A	B	C
Existing	**8**	**10**	**7**
Proposed	**10**	**6**	**10**

Where,
A = Detection Accuracy.
B = Time.
C = Security.

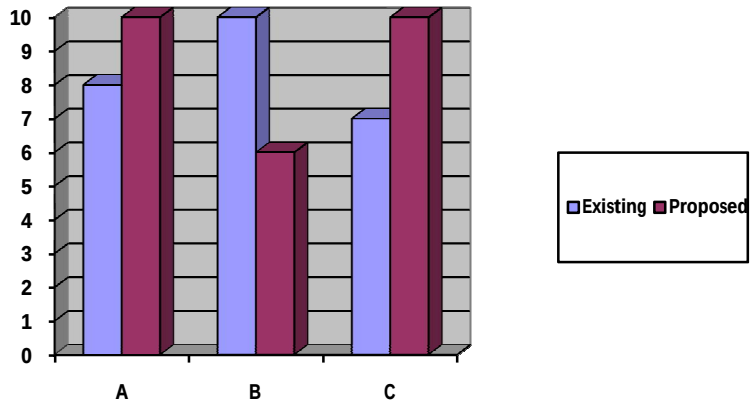

Figure 2. Exiting System vs. Proposed System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VIII. CONCLUSION

We introduced a novel collusion attack scenario against a number of existing IF algorithm rules. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging.

REFERENCES

[1] Rezvani, Mohsen, et al. "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks." IEEE Transactions on Dependable and Secure Computing 12.1 (2015): 98-110.
[2] Yousefi, Hamed, et al. "Fast aggregation scheduling in wireless sensor networks." IEEE Transactions on Wireless Communications 14.6 (2015): 3402-3414.
[3] Hu, Xiaoya, Liuqing Yang, and Wei Xiong. "A novel wireless sensor network frame for urban transportation." IEEE Internet of Things Journal 2.6 (2015): 586-595.
[4] Morell, Antoni, et al. "Data Aggregation and Principal Component Analysis in WSNs."
[5] Ranjani, S. Siva, S. Radhakrishnan, and C. Thangaraj. "Secure cluster based data aggregation in wireless sensor networks." Science Engineering and Management Research (ICSEMR), 2014 International Conference on. IEEE, 2014.
[6] Vaidehi, V., R. Kayalvizhi, and N. Chandra Sekar. "Secure data aggregation in wireless sensor networks." Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on. IEEE, 2015.
[7] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.