Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 1, January -2017

Secure Data Aggregation Technique For Wireless Networks

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

[1]*M.E Computer Science And Engineering, Sinhgad Academy of Engineering , Kondhwa, Pune,*
[2]*Computer Science And Engineering, Assistance Prof. At Sinhgad Academy of Engineering , Kondhwa, Pune.*

Abstract —*Due to restricted procedure power resources and energy resources, aggregation of data from multiple sensing element nodes done at the aggregating node is sometimes accomplished by easy strategies like averaging. but such aggregation is thought to be extremely liable to node compromising attacks. Since WSN are typically unattended and while not tamper resistant hardware, they're extremely prone to such attacks. Thus, ascertaining trait of knowledge and name of sensing element nodes is crucial for WSN. Because the performance of terribly low power processors dramatically improves, future individual nodes are going to be capable of playing additional refined information aggregation algorithms, therefore creating WSN less vulnerable. Repetitive filtering algorithms hold nice promise for such a purpose. Such algorithms at the same time mixture information from multiple sources and supply trust assessment of those sources, typically in a very type of corresponding weight factors allotted to information provided by every supply. During this paper we tend to demonstrate that many existing repetitive filtering algorithms, whereas considerably additional strong against collusion attacks than the easy averaging strategies, are nonetheless susceptive to a unique refined collusion attack we tend to introduce. To deal with this security issue, we tend to propose AN improvement for repetitive filtering techniques by providing AN initial approximation for such algorithms that makes them not solely collusion strong, however conjointly additional correct and quicker joining.*

Keywords- *Atmospheric Scattering Model, Dark Channel Prior, Color Attenuation Prior, Mean Square Error, Structural Similarity.*

I. INTRODUCTION

Due to a want for robustness of monitoring and occasional value of the nodes, wireless sensor networks (WSNs) are generally redundant. Information from more than one sensor is aggregated at an aggregator node which then forwards to the bottom station only the mixture values. At present, because of obstacles of the computing strength and electricity useful resource of sensor nodes, data is aggregated by using extremely simple algorithms which includes averaging. But, such aggregation is thought to be very liable to faults, and greater importantly, malicious attacks [1]. This cannot be remedied by means of cryptographic strategies, because the attackers usually gain whole get admission to statistics stored within the compromised nodes. For those reason facts aggregation at the aggregator node must be observed by means of an assessment of trustworthiness of information from individual sensor nodes. For this reason, better, more state-of-the-art algorithms are needed for statistics aggregation within the destiny WSN. Such a set of rules need to have two features. Consider and reputation systems have a large role in supporting operation of a wide variety of dispensed structures, from Wi-Fi sensor networks and e-commerce infrastructure to social networks, with the aid of presenting an assessment of trustworthiness of individuals in such disbursed systems. A trustworthiness evaluation at any given second represents a combination of the conduct of the members as much as that moment and must be robust within the presence of diverse varieties of faults and malicious behavior. There are a number of incentives for attackers to manipulate the agree with and recognition scores of participants in a disbursed system, and such manipulation can seriously impair the performance of this sort of machine [3]. The main goal of malicious attackers is aggregation algorithms of accept as true with and reputation structures [4].

II. LITERATURE SURVEY

1. Fast Aggregation Scheduling in Wireless Sensor Networks
Author: **Hamed Yousefi, Marzieh Malekimajd, Majid Ashouri, and Ali Movaghar.**
YOP: 2015
Description:
Data aggregation is a key, yet time-consuming functionality introduced to conserve energy in wireless sensor networks (WSNs). In this paper, to minimize time latency, we 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, our 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. We prove that the latency of FAST under the protocol interference model is upper-bounded by $12R+\Delta-2$, where R is the network radius and Δ is the maximum node degree in the communication graph of the original network. Both the

theoretical analysis and simulation results show that FAST outperforms the state-of-the-art aggregation scheduling algorithms.

2.A Novel Wireless Sensor Network Frame for Urban Transportation
Author: Xiaoya Hu, Liuqing Yang, and Wei Xiong.
YOP: 2015
Description:
The rapid progress in the research and development of electronics, sensing, signal processing, and communication networks has significantly advanced the state of applications of intelligent transportation systems (ITSs). However, efficient and low-cost methods for gathering information in large-scale roads are lacking. Consequently, wireless sensor network (WSN) technologies that are low cost, low power, and self-configuring are a key function in ITS. The potential application scenarios and design requirements ofWSN 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 enables users to obtain traffic and road information directly from the local WSN within its wireless scope instead of the remote ITS data center. WSN-UT can be configured according to different scenario requirements. A three-level subsystem and a configuration and service subsystem constitute the WSN-UT network frame, and the service/interface and protocol algorithms for every subsystem level are designed for WSN-UT.

3. Data Aggregation and Principal Component Analysis in WSNs
Author: **Antoni Morell, Alejandro Correa, Marc Barceló, and José López Vicario**
YOP: 2016
Description:
Data aggregation plays an important role in wireless sensor networks (WSNs) as far as it reduces power consumption and boosts the scalability of the network, especially in topologies that are prone to bottlenecks (e.g. cluster-trees). Existing works in the literature use clustering approaches, principal component analysis (PCA) and/or compressed sensing (CS) strategies. 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. In our simulations, we consider without loss of generality a single cluster network and results show that the new technique succeeds in satisfying the NMSE requirement and gets close in terms of energy consumption to the best possible solution employing subspace representations. Additionally, the proposed method alleviates the computational load with respect to an eigenvector-based strategy (by a factor of six in our simulations).

4. Secure Cluster based Data Aggregation in Wireless Sensor Networks
Author: **S. Siva Ranjani, Dr. S. Radhakrishna, Dr. C.Thangaraj**
YOP: 2014
Description:
Data aggregation is the best technique for energy conservation in Wireless Sensor Networks (WSN). Because of the open deployment, sensors are vulnerable for security threats. In this paper we address the data aggregation and security issues together. In our approach, we modify our Energy efficient Cluster Based Data Aggregation (ECBDA)[1] scheme to provide secure data transmission. Since, sensors nodes are low powered in nature, it is not viable to apply standard cryptography methods. Cluster head performs data aggregation and Bayesian fusion algorithm 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 calculates the trust probability of a sensor based on the behavior of the node. The simulation results show that our approach effectively detects the untrustworthy nodes with minimum energy consumption.

5. Secure Data Aggregation in Wireless Sensor Networks
Author: **V. Vaidehi, R. Kayalvizhi, N. Chandra Sekar**
YOP: 2015
Description:
Data aggregation is a widely used technique in wireless sensor networks to reduce the power consumed in WSN. In a bid to reduce the power consumption during data gathering, cluster heads are elected to gather data from every node in the WSN. There are various challenges that are involved in the process of data aggregation like checking of duplication of data after encryption, overhead due to encryption etc. The security issues, data confidentiality and integrity in data aggregation become vital when the sensor network is deployed in a hostile environment (eg, battle field). This paper

proposes a novel scheme to secure the process of data aggregation by providing a light-weight security scheme called Combinatorial Key Distribution (CKD) mechanism that consumes less power and its performance is improved using hashes of data that is sent across the network. The proposed scheme minimizes the power usage and maximizes the secureness of data in the wireless sensor network. The proposed security scheme is compared with other existing security solutions and the results are reported.

III. PROPOSED SYSTEM

Proposes Associate in Wagner for such vulnerability by providing an initial trust estimate that is predicated on a sturdy estimation of errors of individual sensors. once the character of errors is random, such errors basically represent AN approximation of the error parameters of sensing element nodes in WSN like bias and variance. However, such estimates additionally convince be sturdy in cases once the error isn't random however because of coordinated malicious activities. Such initial estimation makes IF algorithms sturdy against represented subtle collusion attack, and, we believe, additionally additional sturdy underneath considerably additional general circumstances; as an example, it's additionally effective within the presence of an entire failure of a number of the sensing element nodes.

IV. SYSTEM ARCHITECTURE

The abstract model planned by Wagner in [6] is taken into account for sensing element configuration. Fig. one shows assumption for network model in WSN. The sensing element nodes area unit divided into seperate clusters, and every cluster features a cluster head that acts as associate someone. information area unit sporadically collected and aggregate by the someone. Authors in [7] assume that the someone itself isn't compromised and consider algo-rithms that build aggregation secure once the individual sensing element nodes may well be compromised and may well be causation false information to the someone. It conjointly assume that every information ag-gregator has enough machine power to run associate appropriate rule for information aggregation.

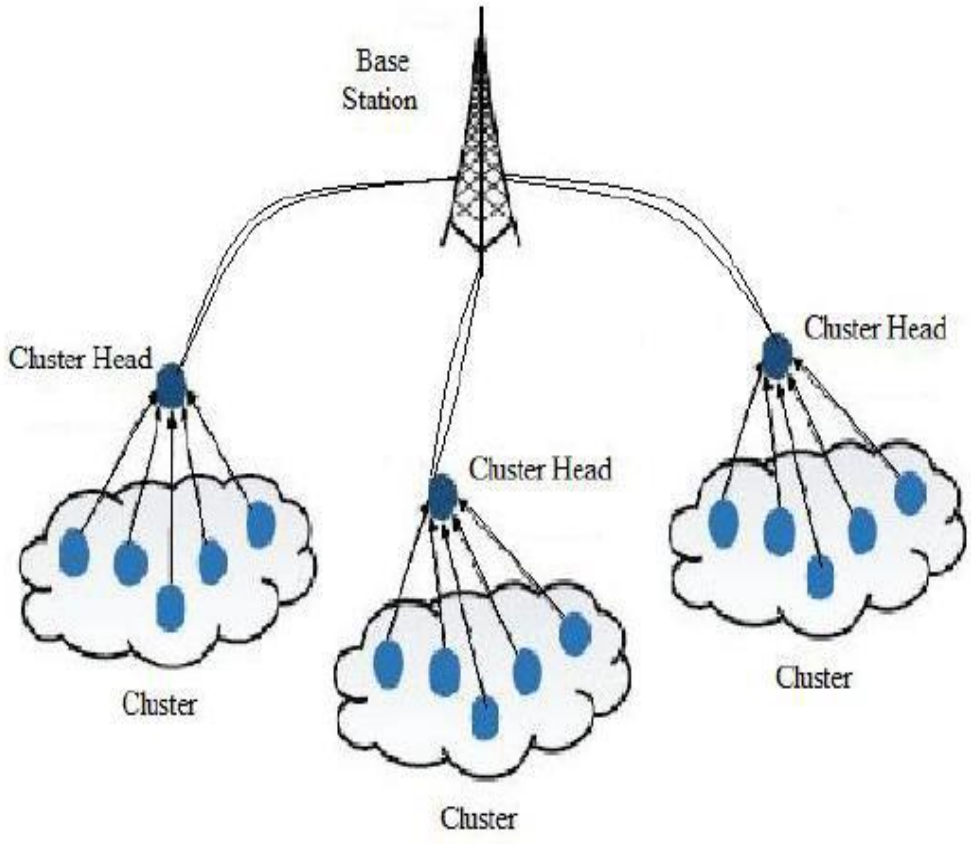

Fig. 1 Network model of wirelss sensor network

The past researchers [9] [8] develops the attack models by considering the fact that they cannot rely on cryptographic methods forpreventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. The

authors in, considers Byzantine attack model, where the ad-versary can compromise a set of sensor nodes and insert any false data through the compromised nodes.
Following are some assumptions made in this project:

a. Sensors are deployed in a hostile unattended environment with some physically compromised nodes.
b. When a sensor node is compromised, all the information which is inside the node becomes accessible by the adversary. System cannot depend on cryptographic methods for preventing the attacks because the adversary may extract cryptographic keys from the compromised nodes.
c. Through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of changing the aggregate values.
d. All compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack.
e. The adversary has enough knowledge about the aggregation algorithm and its parameters. The base station and aggregator nodes cannot be compromised by adversary node.

IV.MODULES

There are two clusters on two different pcs each cluster is having cluster head who is having highest weight among all the nodes in the cluster.

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).

Aggregator/Cluster head:
In this CH can see the entire cluster nodes, there data, and status.
a.Data aggregation:
In this CH can see the entire cluster nodes, there data, and status. Status column shows the whether particular node has been compromised or not.
In this the CH head does data aggregation of the data received from nodes.After performing data aggregation the CH head drops the nodes and send only the actual node data to another PC. (ie. PC1 to PC2).

Hacker:

- Hacker will be on pc3.
- Hacker is the adversary node who compromise the node in the cluster i.e. hacker injects the false data to node.
- Hacker login to system to compromise the node in the cluster i.e. hacker injects the false data to node.
- The hacker will perform the false data injection attack as mentioned inscenario2 and scenario3.

Receiver:

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

Collusion attack detection at receiver node:

When pc2 receives the pc1 data pc2 will sends the collusion attack notification to pc1.Collusion attack means when pc1 sends the same data to pc2 again and again. i.e. pc1 sends data to pc2 which is already present at pc2.

IV. CONCLUSION

We introduced a unique collusion attack situation against variety of existing IF algorithms. Moreover, we have a tendency to projected Associate in Nursing improvement for the IF algorithms by providing Associate initial approximation of the trait of sensing element nodes that makes the algorithms not solely collusion sturdy, however additionally a lot of correct and quicker convergence.

REFERENCES

[1]. Fast Aggregation Scheduling in Wireless Sensor Network Author: HamedYousefi, MarziehMalekimajd, MajidAshouri, and Ali Movaghar.YOP: 2015

[2]. A Novel Wireless Sensor Network Frame for Urban TransportationAuthor: Xiaoya Hu, Liuqing Yang, and Wei Xiong.YOP: 2015

[3]. Data Aggregation and Principal Component Analysis in WSNsAuthor:AntoniMorell, Alejandro Correa, Marc Barceló, and José López Vicario YOP:2016

[4]. Secure Cluster based Data Aggregation in Wireless Sensor Network Author: S. Siva Ranjani, Dr. S. Radhakrishna, Dr. C.ThangarajYOP: 2014

[5]. Secure Data Aggregation in Wireless Sensor NetworksAuthor: V. Vaidehi, R. Kayalvizhi, N. Chandra SekarYOP:2015

[6]. D. Wagner, "Resilient aggregation in sensor networks," in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 78–87.

[7]. Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: a secure hopby-hop data aggregation protocol for sensor networks," in MobiHoc, 2006, pp. 356–367.

[8]. E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," in Proceedings of the 2009 IEEE international conference on Symposium on Information, 2009.

[9]. Mohsen Rezvani, AleksandarIgnjatovic, Elisa Bertino, and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks" , IEEE Transactions on Dependa-ble and Secure Computing (TDSC) ,2014.

