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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

A Review on Data Aggregation Scheme for Wireless Sensor Networks to Enhance Security from Collision Attacks

D.Basanth Kumar[1], M. Krishna Kishore[2]

PG Scholar, Dept. of CSE, Narayana Engineering College, Nellore, AP, India.[1]

Assistant Professor, Dept. of CSE, Narayana Engineering College, Nellore, AP, India.[2]

ABSTRACT: Data aggregation in WSN is usually done by easy methods like averaging, these strategies results in risk of sure attacks. To create trust knowledge and name of sensing element, nodes are going to be capable of activity additional subtle data aggregation algorithmic program, so creating without defenseless. This technique makes them not solely collision strong, however conjointly additional correct and quicker connection. According to the experiments shown that our methodology works quite well for different varieties of errors with no modifications. Still , if error dispensation of sensors is either celebrated or calculable, our algorithms are custom-made to different distributions to attain a best performance. Within the 1st stage we offer Associate in Nursing initial estimate of 2 noise parameters for sensing element nodes, bias and variance; details of the computations for estimating bias and variance of sensors. We offer Associate in Nursing initial estimate of the name vector calculated exploitation the MLE, the elaborated computation operations. Within the third stage of the proposed framework, the initial name vector provided within the second stage is employed to estimate trait of every sensing element supported the space of sensing element readings to such initial name vector. Here, Iterative filtering algorithm is applied to test the performance of LEACH, TEEN and HEF protocol.

KEYWORDS: Data Aggregation, HEF, TEEN, LEACH, WSN, iterative filtering algorithm.

I. INTRODUCTION

A wireless network consists of nodes capable of grouping information from the environment and communication with each other via wireless transceivers. The collected information are delivered to one or extra sinks, generally via multi-hop communication. The nodes unit of measurement typically expected to figure with batteries and unit of measurement typically deployed to not-easily-accessible or hostile surroundings, generally in large quantities. it'll be difficult or inconceivable to change the batteries of the nodes. As an alternative, the sink is commonly created in energy. Since the energy is that the foremost precious resource among the, economical utilization of the energy to prolong the network fundamental quantity has been the most target of plenteous of the analysis on the. The communications among that have the several-to-one property in this information from AN outsized sort of nodes tend to be centered into many sinks. Since multi-hop routing is generally needed for distant nodes from the sinks to avoid wasting energy, the nodes near a sink are going to be burdened with relaying AN outsized amount of traffic from completely different nodes. Network management is that the tactic of managing, monitoring, and dominant the behavior of a network.

Wireless sensor networks (WSNs) produce differentiated challenges for network management that make ancient network management techniques very impractical. In ancient networks the primary goals square measure minimizing latent amount and providing comprehensive information, but in detector networks the primary goal is minimizing energy use and conjointly the most suggests that for doing this will be by reducing the quantity of communication between nodes. Optimizing the operational and purposeful properties of WSNs may wish a singular declare each application draw back. Network failures square measure common events rather than exceptional ones. Thus, in WSNs, we've a bent to face live primarily committed observance and dominant node communication thus on optimize the

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

efficiency of the network, make certain the network operates thoroughly, maintain the performance of the network, and management large numbers of nodes whereas not human intervention.

What is extra, sensor nodes unit generally deployed in remote or harsh conditions so the configuration of nodes in WSNs changes dynamically. Thus, a detector network management system got to alter the network to self-forming, self-organize, and ideally to self-configure at intervals the event of failures whereas not previous data of the topology. Despite the importance of detector network management, there\'s not any existing generalized resolution for WSN management. However, most detector network applications unit of activity designed with network management in mind then no additional network management layer is needed.

II. RELATED WORKS

In [1], authors projected a replacement technique for intra cluster routing where its further energy economical than a celebrated routing protocol Multihop Router that performs multihop routing. They tested the arrangements by simulation a network with thirty nodes, whereas to justify the conception through results of the simulation that had been thought of the parameters that include: varying of packets sent into the network, energy consumed by the network, remaining energy of nodes at specific time and network amount of the network. Exploitation projection technique shows that they had hyperbolic on the network amount and varying of packet sent inside the network. In [7], author explains the Multipath Power Sensitive Routing (MPSR) Protocol for Mobile specific Networks has been given. Providing multiple ways that is helpful in specific networks as a results of once one in each of the routes is disconnected, the availability can simply use totally different on the market routes whereas not humanities the route discovery methodology over again. The simulation was done victimization the worldwide Mobile machine (GloMoSim) Library. The results of comprehensive simulation shows that the performance of MPSR protocol is on degree increasing trend as quality can increase as compared to the Dynamic offer Routing and victimization this protocol is that the end-to-end packet delay does not increase significantly. In [2] projected an energy economical and collision aware (EECA) node-disjoint multipath routing algorithmic procedure. The foremost set up of EECA is to use the printed nature of wireless communication to avoid collisions between two discovered routes whereas not any overhead. to boot, EECA restricts the route discovery flooding and adjusts node transmit power with the assistance of node position information, resulting in energy efficiency and smart performance of communication.

They planned proactive minimum latency routing algorithms: optimum PML and quick—PML. The schemes planned during this paper will offer generic routing functionalities for many of the prevailing planning schemes. Curt Schurgers initial he projected in [10], optimum routing in device networks is unworkable and projected a smart guideline that advocates a regular resource utilization, which can be unreal by the energy chart. They projected kind of wise algorithms that ar affected by this concept. There DCE (Data Combining Entities) combining theme reduces the energy, whereas there spreading approaches aim at distributing the traffic in a {very} very plenty of balanced methodology. several techniques, that swear entirely on localized metrics, are projected and evaluated. And there result shows that they\'ll increase the network amount up to an extra ninetieth on the so much aspect the gains of their initial.

III. PROPOSED WORK

Due to a desire for hardness of observance and low value of the nodes, wireless sense networks (WSNs) area unit redundant. Information from multiple sensors is collective at AN soul node that then forwards to the bottom station solely the combination values. At present, because of limitations of the computing power and energy resource of device nodes frequently, information collection is done by very simple algorithms like averaging. However, such aggregation terribly prone to faults and additional significantly, Malicious attacks [1]. It will not be given remedy by crypto logic ways, as a result of the attackers usually gain complete access to data hold on within the compromised nodes. For that reason information aggregation at the soul node needs to be in the course of an assessment of trustiness of knowledge from individual device nodes. Thus, better, additional subtle algorithms area unit required for information aggregation within the future WSN ought to have 2 preferable options.

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

- In the presence of random errors such algorithmic program ought to turn out estimates that area unit near the optimum ones in data supposed sense. Thus, as an example, if the noise gift in every device could be a mathematician severally distributed noise with a zero mean, then the estimate made by such Associate in Nursing algorithmic program ought to have a variance near the Cramer-Rao bound (CRLB) [2], i.e, it ought to be near the variance of the utmost probability computer (MLE). However, such estimation ought to be achieved while not activity to the algorithmic program the variances of the sensors, unavailable in apply.

- The formula ought to even be sturdy within the presence of non-stochastic errors, like faults and malicious attacks, and, besides aggregating data; such formula ought to additionally offer Associate in nursing assessment of the dependability and trait of the information received from the sensing element nodes.

We validate the performance of our formula by simulation on synthetically generated information's. Our simulation results defines that our sturdy aggregation technique is effective in terms of hardiness against our novel refined attack state of affairs furthermore as economical in terms of the machine value.

- Identification of a replacement refined collusion attack against IF primarily based name systems that reveals a severe vulnerability of IF algorithms.
- A completely unique methodology for estimation of sensing elements errors that is effective during a wide selection of sensor faults and not vulnerable to the represented attack.

We provide a radical empirical analysis of effectiveness and potency of our projected aggregation methodology. The results show that our methodology provides each higher accuracy and higher collusion resistance than the prevailing ways.

IV. SYSTEM STUDY

A.Existing System Cluster Head could be a node collect all the knowledge and aggregates the info. That information is forward to base station. Avoiding misconduct activities here cluster head act as associate degree critic of all the cluster members Nodes. Here nodes generated the profiles. Information from multiple sensors is collective at associate degree someone node that then forwards to the bottom station solely the mixture values. At present, as a result of limitations of the computing power and energy resource of device nodes, information is collective by very simple algorithms like averaging.

Disadvantages:

- There is no assurance for CH won't act as Malicious Node.
- Difficult generate Keys.

B. Proposed Scheme

Our proposed system has the subsequent contributions like:

1) Identification of a replacement subtle collusion attack against IF primarily based name systems that reveals a severe vulnerability of IF algorithms;

2) A completely unique methodology for estimation of devices' errors that is effective AN exceedingly in a very big selection of sensor faults and not vulnerable to the delineated attack;

3) style of an economical and strong aggregation methodology galvanized by the MLE, that utilizes Associate in Nursing estimate of the noise parameters obtained mistreatment contribution a pair of higher than;

4) Increased IF schemes ready to defend against subtle collusion attacks by providing Associate in nursing initial estimate of trustiness of sensors mistreatment inputs from contributions a pair of and three above. Here also we enhance the QOS by improving protocol of HEF. It proliferate the lifetime and packet delivery rate of network as shown in Fig.1.

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

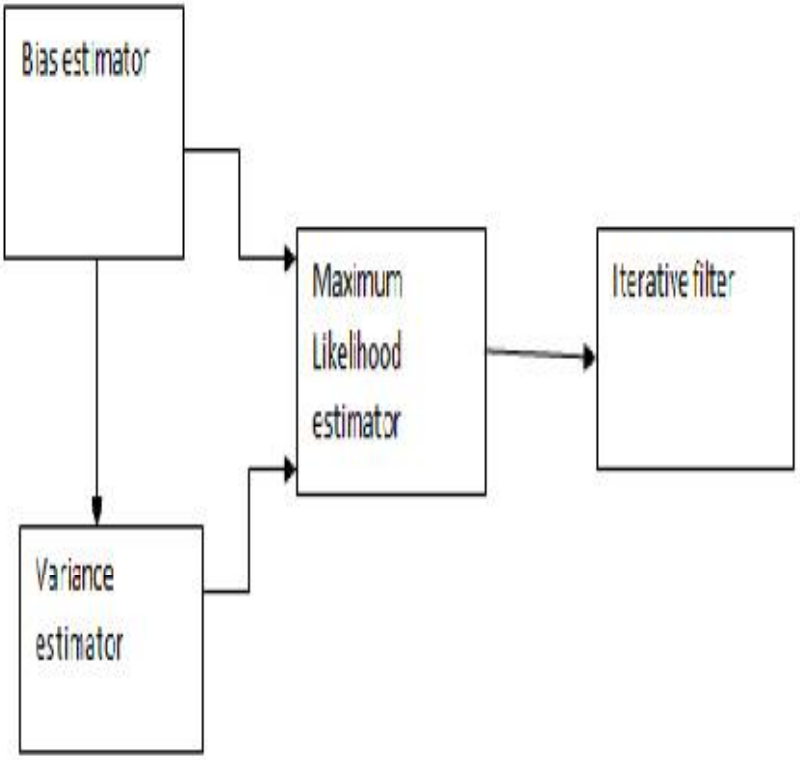

Fig.1. System Diagram.

Advantages: When CH acts as malicious node it can remove the CH also.
- High Securable
- In previous techniques CH have more work load, it reduce the work load.

C. Cluster Formation

The device nodes square measure divided into disjoint clusters, and every cluster includes a cluster head that acts as associate degree soul. Knowledge square measure sporadically collected and aggregative by the soul. Soul itself isn't compromised and concentrates on algorithms that build aggregation secure once the individual device nodes may well be compromised and may well be causation false knowledge to the soul. we have a tendency to assume that every knowledge soul has enough process power to run associate degree IF algorithmic program for knowledge aggregation. **HEF:** Without a prior data (such as network period, residue energy state, and therefore the energy consumption for clusters), it's not possible for any cluster head choice rule to get sensible results for prolonging the network period. The core plan of the HEF cluster rule is to decide on the highest-ranking energy residue sensing element as a cluster head. The HEF cluster rule is outlined as follows. Some researchers have claimed that HEF is associate degree economical cluster choice rule that prolongs network period supported simulations. However, their measurements and simulation results area unit random processes. A theoretical roof to demonstrate the optimality of HEF underneath sure conditions is provided during this paper.

D. Adversary Model

In this model, we have a tendency to produce some cluster of sensors inject any false knowledge through the compromised nodes. All the data that is within the node becomes accessible by the soul. Soul model, the assaulter node tried to vary minimum 2 sensors report. It listen the important report and it\'ll turn out to be skew report.

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

E. Robust Data Aggregation

Robust information aggregation, aggregation node aggregates all the info that area unit comes from varied sensors within the cluster. Here we want secure information aggregation, for this purpose we have a tendency to invariably analyze trait of the detector nodes. If error distribution of sensors is either glorious or calculable, our algorithms are often custom-made to alternative distributions to attain associate degree optimum performance. Our aggregation technique operates on batches of consecutive readings of sensors, continuing in many stages. Finally, we have a tendency to estimate the trait of every detector supported distance of the readings.

V. SIMULATION PARAMETER

A. Result Analysis

In our simulation all the nodes will select a base station through Cluster Head by LEACH protocol. CH will collects the data and it will send to destination. CH will always validate the data originality. This process will be done CH, it will filtering the data and compared with neighbour. If any false node detected in the network, CH will eliminate the node.

TEEN protocol implemented in IF filtering algorithm to test the simulation nam window as Shown. Here working node color will be indicate as green and remaining node will be sleep mode and that color is grey. Red color node is compromised node identified by IF algorithm. HEF protocol can be implanted on same algorithm to test the performance analysis as shown.

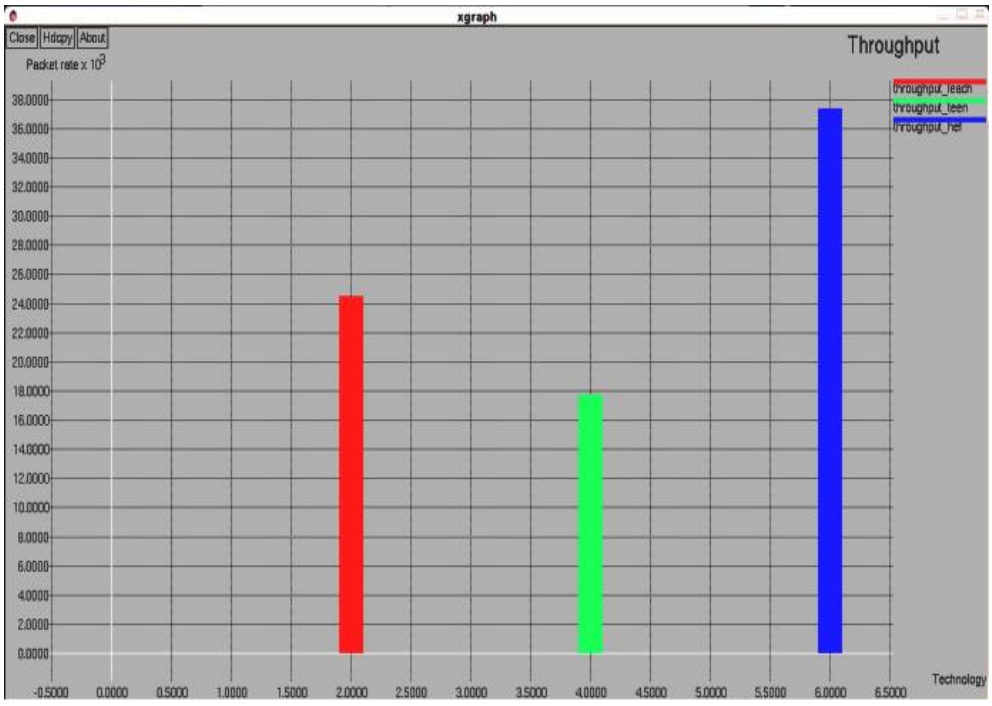

Fig1: the higher throughput rate compared to other protocols

This graph shows comparison about data rate between LEACH, TEEN and HEF protocol. Data Aggregation mechanism will reduce the workload of CH. Here HEF protocol shows the higher throughput rate compared to other protocols. From this graph our proposed system proves less delay comparing to previous one.

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

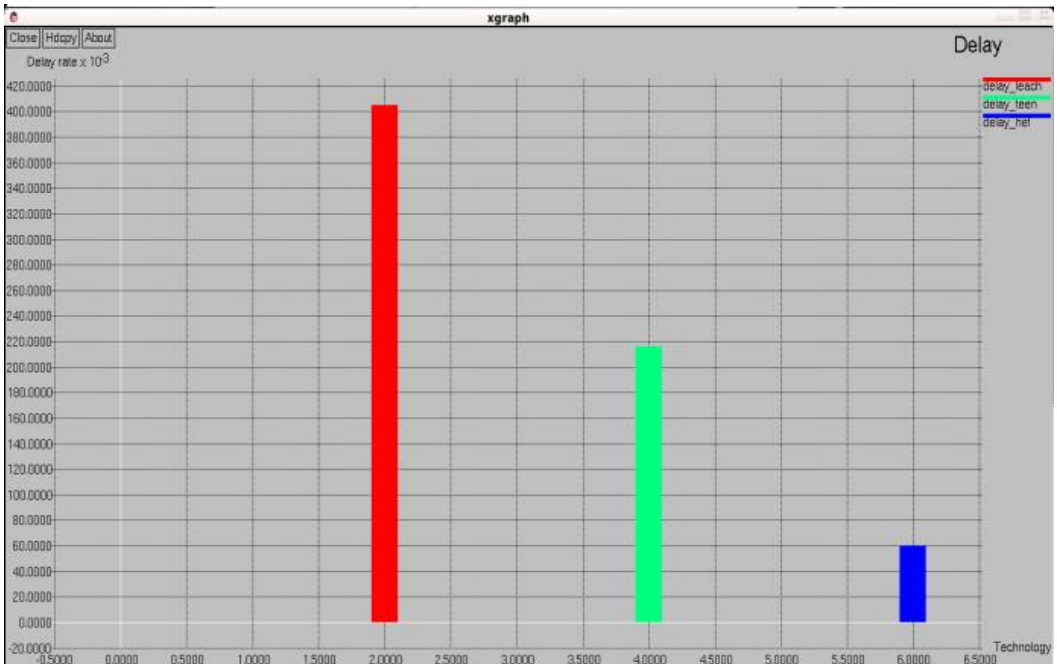

Fig1.1: the throughput rate comparation

VI. CONCLUSION

The proposed Clustering mechanism is one of the finest and proved algorithms to improve QOS in WSN. Our system is specially designed for both security and QOS. In secure data aggregation mechanism data validation by Iteration Filtering algorithm through sensors. If any false data is detected, which node send that data that node will be eliminated by a network also compression mechanism will improves the QOS of network. In future the network will be specially designed for reduce no of over heads in the network. Clustering algorithm may be changed into dual clustering algorithm.

REFERENCES

[1] 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.
[2] L. Wasserman, All of statistics : a concise course in statistical inference. New York: Springer.
[3] A. Jøsang and J. Golbeck, ―Challenges for robust trust and reputation systems,‖ in Proceedings of the 5 th International Workshop on Security and Trust Management, Saint Malo, France, 2009.
[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, ―A survey of attack and defense techniques for reputation systems,‖ ACM Comput.Surv., vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.
[5] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, ―Trust and reputation systems for wireless sensor networks,‖ in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, Eds. Troubador Publishing Ltd, 2009, pp. 105–128.
[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, ―Provenance-based trustworthiness assessment in sensor networks,‖ in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN ’10, 2010, pp. 2–7.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, ―Energy efficient and fault tolerant multicore wireless sensor network: E 2 MWSN,‖ in Wireless Communications, Networking and Mo-bile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1–4.
[8] C. de Kerchove and P. Van Dooren, ―Iterative filtering in reputation systems,‖ SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812–1834, Mar. 2010.
[9] Y. Zhou, T. Lei, and T. Zhou, ―A robust ranking algorithm to spamming,‖ CoRR, vol. abs/1012.3793, 2010.
[10] P. Laureti, L. Moret, Y.-C.Zhang, and Y.-K. Yu, ―Information filtering via Iterative Refinement,‖ EPL (Europhysics Letters), vol. 75, pp. 1006–1012, Sep. 2006.

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

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

BIOGRAPHY

D.Basanth Kumar has received his B.Tech degree in Computer Science and Engineering from Brahmas Institute of Engineering and Technology affiliated to JNTU, Anantapur in 2014 and pursuing M.Tech degree in Computer science and Engineering in Narayana College of Engineering affiliated to JNTU, Anantapur in 2014-2016.

M. Krishna Kishore has received his B.Tech in IT from PBR VITS, Kavali, J.N.T.U Ananthapur,and M.tech degree in Computer Science and Engineering from SVCET, Chittoor, J.N.T.U Ananthapur. He is dedicated to teaching field from the last 5.7 years. He has guided 9 batches U.G students.Also Ratified as an Assistant Professor from JNTUA on november 2014., At present he is working as an Assistant Professor in C.S.E Dept. in Narayana Engineering College, Nellore, Andhra Pradesh, India.