RESEARCH ARTICLE OPEN ACCESS

A Secure and Efficient Particle Swarm Optimization Clustering (PSOC) Based Data Aggregation Protocol for Wireless Sensor Network (WSN)

[1]Mr. B. Karthik., [2]Dr. C. R. Sakthivel.

[1]Research Scholar, Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore, Tamilnadu.

[2]Associate Professor, Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore, Tamilnadu.

--************************----------------------------------

Abstract:

Data aggregation in Wireless sensor Network (WSN) is typically done by some easy technique like averaging. These ways are liable to sure attacks. Refined data aggregation formula would create the sensor nodes less vulnerable thereby achieving the trust of knowledge and name. Secure information aggregation protocol holds nice promise for this purpose. To beat the safety problems in WSN, Particle Swarm optimization Clustering (PSOC) based mostly secure data aggregation protocol is planned. This method makes them not solely collusion sturdy however, a lot of correct and conjointly achieves quicker convergence. Then the optimized cluster head is chosen for data aggregation by PSO. The cluster formation is reduced the ability consumption and bandwidth allocation. Trust and name have a big role in supporting the operations of a large vary of distributed systems, from wireless detector network to social network. Assume that the random elements of detector errors are independent random variables with a Gaussian distribution. If error distribution of sensors is either familiar or calculable, planned algorithms may be custom-made to alternative distributions to realize associate best performance. A sensor node solely accepts data things aggregate by licensed users. So as to make sure security, every step of the prevailing data aggregation protocol runs ought to be known then protected. The first challenge of providing security functions in wsns is that the restricted capabilities of sensor nodes in terms of computation, energy and storage.

Keywords—Wireless Sensor Network, Aggregation, PSO, clustering, Certificate Authority, Threshold Value, Security

--************************----------------------------------

I. INTRODUCTION

The wireless sensor network is outlined because the extremely distributed networks of tiny, light-weight wireless node deployed in massive numbers to trust the environment or system by the measure of physical parameters like temperature, pressure or ratio. In the WSN, the data from the sensor nodes are collected by suggests that of knowledge aggregation. Sensory data is collected by the nodes. WSN consists of a base station and also the range of nodes. The aggregator node is employed to combination the data from multiple sensor nodes then the data is forwarded to the bottom station.

There is many security challenges may be faced throughout the aggregation of data [1]. Because of this wireless aggregation, eavesdropping and packet injection are occurred. Providing security within the sensor network is tougher than the mobile adhoc network. To realize the safety in WSN, they perform varied cryptographic operations like encryption, decryption and authentication then on. For any cryptographic operation they need to use any of the key like rhombohedra key or uneven key. If symmetric key is used then it is terribly tough to style for security purpose. If uneven key is used then it is too expensive. For applying any of the cryptography theme then it has further bits, memory needed, delay occurred then on.

In the existing system, varied algorithms are accustomed succeed the safety throughout data aggregation. Several algorithms focus solely on the specific attacks or issues. The iterative filtering formula [2, 3] is merely focus on collusion attack [4]. The secure data aggregation protocol is wide accustomed overcome the faults that chiefly occurred on the prevailing system. Within the existing system, the information is transferred to the bottom station. So a lot of quantity of energy is employed. To produce the energy strained mechanism, then the transfer of the unwanted information should be prevented. This can be achieved by Secure Data Aggregation Protocol (SDAP) [5]. Here the nodes are classified as clusters and cluster head is chosen supported PSO. All the mandatory process is finished inside the cluster. Now, all the teams transfer the processed data to the base station. From the received data, the teams with malicious nodes are known. The safety to the info is provided exploitation the cryptographic keys. The aggregation is performed through hop-by-hop. This performs efficiency at every node to observe the malicious node. The problem arises by using per-hop aggregation, since it does not verify the correctness of the data.

II. RELATED WORKS

In [6] Chan H., Perrig A., and Song D. Mentioned secure hierarchical in-network aggregation in sensor networks. The primary algorithm for demonstrate secure hierarchical in-network knowledge aggregation. The algorithm is sure to cite any manipulation of the combination by the somebody on the far side what's realizable through direct injection of information values at compromised nodes. In different words, the opponent will never gain any advantage from misrepresenting intermediate aggregation computations. The algorithm incurs solely O(Dlog2 n) node congestion, supports arbitrary tree-based aggregator topologies and retains its resistance against aggregation manipulation within the presence of arbitrary numbers of malicious nodes.

In [7] Ho J.-W., Wright M., and Das S. Introduce fast zone-based node compromise detection and revocation in wireless sensor networks using serial hypothesis testing. Owing to unattended nature of wireless device network, an adversary will physically capture and compromise sensor nodes and so mount a spread of attacks with the compromised nodes. To attenuate the injury incurred by the compromised nodes, the system ought to sight and revoke them as shortly as possible. However, they need every device node to be genuine sporadically, so acquisition substantial overhead. To mitigate the constraints of the present schemes, they propose a zone-based node compromise detection and revocation theme in wireless device networks. In addition, the detection drawback employing a game hypothetical analysis [8], derive the optimum methods for the attacker and also the defender, and show that the attacker's gain from node compromise is greatly restricted by the defender once each the attacker and also the defender follow their optimum methods.

In [9] Roy S., Conti M., Setia S., and Jajodia S. Mentioned a secure data aggregation with an oversized device network, in-network data aggregation considerably reduces the quantity of communication and energy consumption. Within the paper, they must build the outline diffusion approach secure against attacks within which compromised nodes contribute false sub mixture values. Particularly, they gift a unique light-weight verification algorithm by that the base station will verify if the computed mixture (predicate Count or Sum) includes any false contribution. Thorough theoretical analysis and intensive simulation study show that the algorithm outperforms different existing approaches.

In [10] Tang L.-A., Yu X., Kim S., Han J., Hung C.-C., and Peng W.-C. Introduce trustiness analysis of device networks Cyber-Physical System (CPS) that integrates physical devices with cyber parts to create a situation-integrated analytical system that responds showing intelligence to dynamic changes of the real-world situations. One key issue in cps analysis is trustiness analysis of the determined knowledge. Owing to technology limitations and environmental influences, the cps knowledge is inherently droning which will trigger several false alarms. It is extremely fascinating to sift significant data from an oversized volume of droning knowledge. Within the paper, they propose a technique known as Tru-Alarm that finds out trustworthy alarms and will increase the practicableness of cps. Tru-Alarm estimates the locations of objects inflicting alarms, constructs Associate in Nursing object-alarm graph and carries out trustiness inferences supported coupled data within the graph. Intensive experiments show that True-Alarm filters out noises and false data expeditiously and guarantees not missing any substantive alarms.

The system performs knowledge aggregation with security and attack handling mechanism. Repetitive filtering techniques with initial approximation model square measure accustomed secure knowledge aggregation method. Owing to restricted procedure power and energy resources, aggregation of data's from multiple device nodes done at the aggregating node. Such aggregation is understood to be extremely liable to node compromising attacks. Repetitive filtering algorithms hold nice promise for such a purpose. Such algorithms at the same time mixture knowledge from multiple sources and supply trust assessment of those sources, typically in an exceedingly sort of corresponding weight factors allotted to knowledge provided by every supply. The present paper demonstrate that many existing repetitive filtering algorithms, whereas considerably a lot of sturdy against collusion attacks than the easy averaging strategies, are even so susceptive to a unique subtle collusion attack. To handle this security issue, this paper proposes Associate in Nursing improvement for repetitive filtering techniques by providing an initial approximation for such algorithms that makes them not solely collusion sturdy, however additionally a lot of correct and quicker convergence. This algorithm doesn't handle packet drop attack and not economical for centralized approach.

III. DATA AGGREGATIONS

To overcome the matter occurred within the iterative filtering algorithm new technique referred to as Certificate Authority (CA) is introduced in every cluster. knowledge Aggregation is employed to mixture data's by the cluster head finally transmit it to the base station. the base station collects all the data's from cluster head and mixture for secure data transmission. To perform the aggregation safer the CA is employed to ascertain every node condition whether or not a node is trust node or malicious node. By exploitation the CA the node method are monitored.

The data's should be transmitted from member node to cluster head and from cluster head to either cluster head or base station inside a given time. If a time exceeds or any modifications wiped out the information then the certificate authority checks the threshold value of that node. If the threshold value is in vary then the node it trustworthy node and data aggregation is finished through this node. If the threshold value is in out of vary then the node is marked as malicious node. Once marking the malicious node the information is not transferred at the actual node. So the information is transmitted solely the trustworthy node and it is collective additional securely and with efficiency. Provide safer for all the nodes due to exploitation the certificate authority. It will increase the packet delivery ratio and additionally improves the performance of non-stochastic elements errors like node fault etc.

A. Cluster head choice and cluster formation: -

The cluster head choice is predicated on the space, residual energy, position, velocity parameters. The optimized cluster head selected by exploitation PSO algorithm. Particle swarm optimization (PSO) could be a population-based random search method, shapely once the social behavior of a bird flock [11, 12]. The algorithmic rule maintains a population of particles, where every particle represents a possible answer to an optimization drawback. Within the context of PSO, a swarm refers to variety of potential solutions to the optimisation problem, wherever every potential answer is cited as a particle. The aim of the PSO is to find the particle position that ends up in the simplest analysis of a given fitness (cluster head) operate.

The clustering can be reduced the energy and bandwidth allocation. And the overall process of proposed system is explained in fig 1.

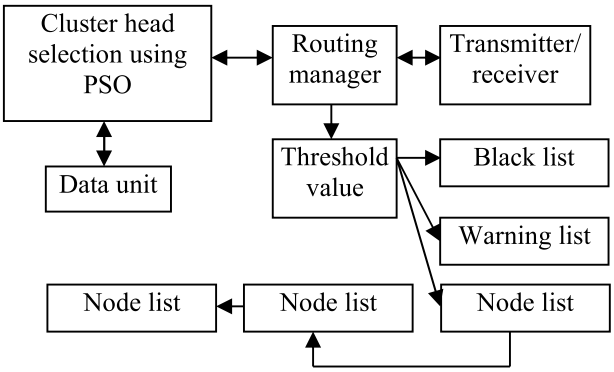

Fig 1: - System Architecture

In Fig 1 describes that for each information transmission starts, the routing manager assures that the node could be a trustworthy node or not. Supported the threshold value the node trust is set. Each node features a specific threshold value. The threshold value is calculated supported the nodes gift within the network. If the threshold value is in vary then the node is captive to the Node list. If the threshold value is in out of vary then the node is captive to the black list. If the threshold value of the node is not even then it's captive to the warning list.

The trust node is gift solely within the node list. When the trust nodes are known then the nodes are monitored by network monitor and raise the member list. The member list nodes are solely allowed for information aggregation. The collection of information’s are named as data units. The data’s are collected from the cluster to the cluster head. This method is additionally monitored by routing manager. When complete this method the information aggregation starts firmly and with efficiency.

Initially, all the nodes are aggregated from the base station. The protection of the information throughout aggregation isn't ensured. By archiving this security, the certificate authority is provided by every cluster. The certificate authority checks whether or not the node is a certified node or malicious node. The certificate is simply provided to the licensed node. In fig 1, shows that there are many clusters. Every cluster features a specific set of nodes, cluster head and therefore the certificate authority. The cluster head collects the information from the whole licensed node and it send to the bottom station. If the cluster head is way aloof from the base station then it transfers the close cluster head and once more aggregated to the base station. Generally there's a malicious node within the cluster head. There's no communication within the malicious node. The malicious node is simply known by mistreatment the certificate authority.

B. Network design

To produce a network with variety of nodes that could be a wireless sensor network and conjointly create the network with the WSN specifications i.e., every node will communicate with the other node directly that square measure in coverage space of the node. During this network, a group of nodes forming clusters. Every cluster has one leader node that is thought as cluster head which could be able to controls the whole traffic gift within the cluster of the network and that is a traditional nodes.

The other sort of node could be a certificate authority that monitors the whole traffic and finds the trustworthy node. The detector nodes are sometimes resource forced with relevancy memory house, computation capability, bandwidth and power offer. The network users use some mobile devices to aggregate data things into the network. The network owner is liable for generating keying materials. It will be offline and so the node is assumed to be uncompromisable.

C. Certificate Authority

This is a node that goes to require care of all different nodes by managing the traffic. It's getting to check whether or not the reply’s sending by the nodes are applicable or not in regular intervals, whenever any new node enter in to the network it'll check whether or not the node is hacking node or not by the reply it sending and inform to all or any different nodes regarding the new node for the secure information transmission.

If any node is not responding properly then the certificate authority checks the threshold value for that node. If the threshold value is in out of vary then it mark the node is malicious node. The data transmission isn't done through this node. If the threshold value is in vary then the node could be a trust node. The data transmission is completed through this node. If the threshold value isn't even then the node is captive in to the warning list till the threshold value is even. The certificate authority work properly and secure with efficiency.

D. Watching the Traffic

Certificate Authority is employed to handle the protection method that is vital node within the network. It's getting to pay attention of the whole network i.e., it monitors all the nodes and checks that are giving sensible response supported that it'll enable different nodes to speak with one another. Networks users are appointed aggregation privileges by the trustworthy authority in a very public key infrastructure on behalf of the network owner. However, the network owner could, for numerous reasons, impersonate network users to combination information things. The compromised entities are considered insiders as a result of they are members of the network till they are known. The someone controls these entities to attack the network in arbitrary ways that. For example, they may be taught to combination false [13] or harmful information, launch attacks like Sybil attacks or Denial of Service attacks and be non-cooperative with different nodes. Information gathered by the individual nodes ultimately routed to the base station.

E. Route Discovery Method

Whenever a node need to speak with different node it got to realize the route for forwarding the information. During this route if any new node is entered suggests that there's an opportunity of which will be a hacking node. So, avoid that hacking nodes for secure information transmission. For this nodes are maintaining an inventory called true list, during this nodes are getting to store regarding the opposite nodes for locating the secure route. In external attacks, someone has no management of any sensor node within the network. The channel may additionally be jammed by someone, however this could solely last for an explicit amount of your time when that someone are detected and removed. Route discovery should be initiated once a supply node desires to search out a route to a brand new destination or once the time period of an existing route to a destination has invalid.

F. Create trust list

Nodes are getting to produce an inventory called true list. During this they are getting to store regarding the node information's that given correct response to the certificate authority. The utility of a sensor network can trust its ability to accurately and automatically find every sensor within the network. A sensor network designed to find faults can want correct location data so as to pin purpose the situation of a fault. Unfortunately, an attacker will simply manipulate non secured location data by coverage false signal strengths and replaying signals.

G. Check trust list

Whenever a node needs to send the information it will send route request to different nodes. The node that received the route request packet can checks whether or not that node is present within the true list or not if conferred suggests that it will forward to different nodes and it will repeats till it reaches destination. Route trust is computed by each node for every route in its routing table. It is a live of the responsibleness with that a packet will reach the destination, if forwarded by the node on it specific route. For each transmission starts before it check the route whether or not it's a trust list or hacking list. If it is a trust list then the data aggregation is completed firmly certificate authority. The secure node is known solely by the certificate authority. The certificate authority checks whether or not the node is that the trust node or not and at last the information aggregation is performed.

IV. RESULTS & DISCUSSIONS

In this section, simulation experiments are presented to demonstrate the effectiveness and superiority of the proposed PSO clustering based secure data aggregation protocol algorithm in comparison with the existing algorithms such as improved iterative filtering protocol [14]. The performance is measured by network parameters such as energy consumption, throughput, message delivery ratio, network lifetime, delay.

H. Energy consumption

The average energy consumed by each node during the given simulation time and expressed in Joules (J).

I. Lifetime Evaluation

It is noted that the lifetime of the ad hoc network in PSOC based secure data aggregation protocol does not change as the node number increases.

J. Delay Evaluation

In proposed protocol, the event data routing is much easier than routing the event data to the storage node using existing routing protocol. Besides, there are many nodes located in the proposed protocol, and they just need to store the data generated by themselves locally, which can greatly decrease the average delay of data storage and retrieval.

K. Packet Delivery Ratio (PDR) Evaluation

In existing protocol some of the messages may drop due to congestion and buffer overflow at the cluster heads, this results in the drop of PDF whereas proposed protocol performed load balancing and this improves PDR.

V. CONCLUSION & FUTURE WORK

The planned cluster based trust management theme that enhances the protection of WSN. By using the planned methodology Secure routing path may be established in malicious environments. The results of WSN routing situation absolutely support the effectiveness and performance of the theme, which improves throughput and packet delivery ratio significantly, with slightly weakened average delay and overhead of messages. The protection needs of wireless sensor networks needed to strengthen attack-resistant information aggregation protocols. The certificate authority computes verity mixture by filtering out the contributions of compromised nodes within the aggregation hierarchy. The nodes are secured by the planned methodology. In future work, the opinion request is send to the neighbour's node as a result of the supply node finds the malicious node. Within the presence of malicious nodes, the need might cause serious security drawback such nodes might disrupt the routing method. A malicious node will attract all packets by using forged Route Reply packet. The supply node broadcasts a Route Request packet to any or all the nodes gift within the network. Once destination receives the Request, it will recognize every intermediator node's address among the route.

REFERENCES

[1]. Ozdemir S. and Xiao Y. (2009), 'Secure data aggregation in wireless sensor networks: A comprehensive overview', Comput. Netw., vol. 53, no. 12, pp. 2022–2037.

[2]. Ayday E., Lee H., and Fekri F. (2009), 'An iterative algorithm for trust and reputation management', Proc. IEEE Int. Conf. Symp. Inf.Theory, vol. 3, pp. 2051–2055.

[3]. 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.

[4]. Hoffman K., Zage D., and Nita-Rotaru C. (2009), 'A survey of attack and defense techniques for reputation systems', ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31.

[5]. Yang Y., Wang X., Zhu S., and S. Cao S. (2006), 'SDAP: A secure hop-byhop data aggregation protocol for sensor networks', in Proc. 7th ACM Int. Symp. Mobile Ad Hoc Netw.Comput., pp. 356–367.

[6]. Chan H., Perrig A., and Song D. (2006), 'Secure hierarchical in-network aggregation in sensor networks', in Proc. 13th ACM Conf. Comput. Commun. Security, pp. 278–287

[7]. Ho J.-W., Wright M., and Das S. (2012), 'ZoneTrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing', IEEE Trans. Dependable Secure Comput., vol. 9, no. 4, pp. 494–511.

[8]. Lim H.-S., Ghinita G., Bertino E., and Kantarcioglu M. (2012), 'A game-theoretic approach for high-assurance of data trustworthiness in sensor networks', in Proc. IEEE 28th Int. Conf. Data Eng., pp. 1192–1203.

[9]. Roy S., Conti M., Setia S., and Jajodia S. (2012), 'Secure data aggregation in wireless sensor networks', IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1040–1052.

[10]. Sharmin, S., Ahmedy, I., & Md Noor, R. (2023). An energy-efficient data aggregation clustering algorithm for wireless sensor Networks using hybrid PSO. Energies, 16(5), 2487.

[11]. Tang L.-A., Yu X., Kim S., Han J., Hung C.-C., and Peng W.-C. (2010), 'Tru-Alarm: Trustworthiness analysis of sensor networks in cyber-physical systems', in Proc. IEEE Int. Conf. Data Mining, pp. 1079–1084.

[12]. J Kennedy, RC Eberhart, "Particle Swarm Optimization", Proceedings of the IEEE International Joint Conference on Neural Networks, Vol. 4, pp 1942–1948, 1995.

[13]. Sharmin, S., Ahmedy, I., & Md Noor, R. (2023). An energy-efficient data aggregation clustering algorithm for wireless sensor Networks using hybrid PSO. Energies, 16(5), 2487.

[14]. Senthil, G. A., Raaza, A., & Kumar, N. (2022). Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network. Wireless Personal Communications, 122(3), 2603-2619.