ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

AN EFFECTIVE AND SECURE DATA AGGREGATION TECHNIQUE BY USING CERTIFICATE AUTHORITY FOR WSN

J. Beno Ranjana[1], C. Gopala Krishnan[2]

[1]PG Student, [2]Assistant Professor

Email id: benoranjana8@gmail.com

[1,2] Department of CSE, Francis Xavier Engineering College

Abstract: Data aggregation in WSN is usually done by some simple method such as averaging. These methods are vulnerable to certain attacks. Sophisticated data aggregation algorithm would make the sensor nodes less vulnerable thereby achieving the trust of data and reputation. Secure data aggregation protocol holds great promise for this purpose. To overcome the security issues in WSN, we introduce an improved Secure Data Aggregation Protocol. This technique makes them not only collusion robust but, more accurate and also achieves faster convergence. Trust and reputation have a significant role in supporting the operations of a wide range of distributed systems, from wireless sensor network to social network. We assume that the stochastic components of sensor errors are independent random variables with a Gaussian distribution. If error distribution of sensors is either known or estimated, our algorithms can be adapted to other distributions to achieve an optimal performance. A sensor node only accepts data items aggregated by authorized users. In order to ensure security, each step of the existing data aggregation protocol runs should be identified and then protected. The opinion request is sent from the source node to the remaining nodes in order to find the trust node. The primary challenge of providing security functions in WSNs is due to the limited capabilities of sensor nodes in terms of computation, energy and storage.

Key words: Wireless Sensor Network (WSN), Aggregation, Certificate Authority, Threshold Value, Security.

I. INTRODUCTION

The wireless sensor network is defined as the highly distributed networks of small, lightweight wireless node, deployed in large numbers to trust the environment or system by the measurement of physical parameters such as temperature, pressure or relative humidity. In the WSN, the data from the sensor nodes are collected by means of data aggregation. Sensory information is collected by the nodes. WSN consists of a base station and the number of nodes. The aggregator node is used to aggregate the data from multiple sensor nodes and then the data is forwarded to the base station.

There is several security challenges can be faced during the aggregation of data. Due to this wireless aggregation, eavesdropping and packet injection are occurred. Providing security in the sensor network is more difficult than MANET.

In order to achieve security in WSN, they perform various cryptographic operations like encryption, decryption and authentication and so on. For any cryptographic operation they must use any of the key like symmetric key or asymmetric key. If symmetric key is used then it is very difficult to design for security purpose. If asymmetric key is used then it is too expensive. For applying any of the encryption scheme then it has extra bits, memory required, delay occurred and so on.

In the existing system, various algorithms are used to achieve the security during data aggregation. Many algorithms focus only on the specific attacks or problems. The iterative filtering algorithm is only concentrate on collusion attack.

The secure data aggregation protocol is widely used to overcome the faults that mainly occurred on the existing system. In the existing system, the raw data is transferred to the base station. Therefore more amount of energy is utilized. To provide the energy constrained mechanism, then the transfer of the unwanted data must be prevented. This is achieved by Secure Data Aggregation Protocol (SDAP). Here the hierarchical structure is formed as a tree. The root is the base station. The nodes other than the root are aggregators. The aggregators are not the child nodes. The group is formed with the aggregators. All the necessary processing is done within the group. Now, all the groups transfer the processed data to the base station. From the received data, the groups with malicious nodes are identified.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

The security to the data is provided using the cryptographic keys. The aggregation is performed through hop-by-hop. This performs efficiency at each node to detect the malicious node. The difficulty arises by using per-hop aggregation, since it does not verify the correctness of the data.

The major challenge in SDAP under the tree topology is that [15], a high level trust is needed for the aggregator's node. Therefore, to provide a better approximation and accuracy, divide and conquer method is adopted. Logical groups are formed to reduce the threat to the number of nodes. To provide the security to the groups, a commit and attest technique is used. In this technique, when a group is committed to aggregate, it cannot be denied.

To validate the groups, the bi-variate-multiple outlier detection algorithm is used. The validation is processed based on the attestation from the group.

Security in Wireless sensor Network

During the transmission of data the wireless sensor network must need the security. This security is also needed for every data as well as the nodes for which transferring the data.The security is needed while transmitting the data for wireless communication. The following information discuss that why security is needed.

- Providing security in WSN is more difficult because of limited number of resources.
- Security is needed at the design time to ensure the operation safety, secrecy of the sensitive data and privacy for people in the sensor environment.

Wireless sensor network could not deploy the hostile and uncontrolled environment.

II. RELATED WORKS

In [2] Chan H., Perrig A., and Song D. discussed secure hierarchical in-network aggregation in sensor networks. The first algorithm for provably secure hierarchical in-network data aggregation. The algorithm is guaranteed to detect any manipulation of the aggregate by the adversary beyond what is achievable through direct injection of data values at compromised nodes. In other words, the adversary can never gain any advantage from misrepresenting intermediate aggregation computations. The algorithm incurs only O(Dlog2 n) node congestion, supports arbitrary tree-based aggregator topologies and retains its resistance against aggregation manipulation in the presence of arbitrary numbers of malicious nodes. The main algorithm is based on performing the SUM aggregation securely by first forcing the adversary to commit to its choice of intermediate aggregation results, and then having the sensor nodes independently verify that their contributions to the aggregate are correctly incorporated. They show how to reduce secure MEDIAN, COUNT, and AVERAGE to this primitive.

In [4] Ho J.-W., Wright M., and Das S. introduce fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing. Due to unattended nature of wireless sensor network, an adversary can physically capture and compromise sensor nodes and then mount a variety of attacks with the compromised nodes. To minimize the damage incurred by the compromised nodes, the system should detect and revoke them as soon as possible. However, they require each sensor node to be attested periodically, thus incurring substantial overhead. To mitigate the limitations of the existing schemes, they propose a zone-based node compromise detection and revocation scheme in wireless sensor networks. The main idea behind this scheme is to use sequential hypothesis testing to detect suspect regions in which compromised nodes are likely placed. In these suspect regions, the network operator performs software attestation against sensor nodes, leading to the detection and revocation of the compromised nodes. Through quantitative analysis and simulation experiments, they show that the proposed scheme detects the compromised nodes with a small number of samples while reducing false positive and negative rates, even if a substantial fraction of the nodes in the zone are compromised. Additionally, the detection problem using a game theoretic analysis, derive the optimal strategies for the attacker and the defender, and show that the attacker's gain from node compromise is greatly limited by the defender when both the attacker and the defender follow their optimal strategies.

In [10] Roy S., Conti M., Setia S., and Jajodia S. discussed a secure data aggregation with a large sensor network, in-network data aggregation significantly reduces the amount of communication and energy consumption. Recently, the research community has proposed a robust aggregation framework called synopsis diffusion which combines multipath routing schemes with duplicate-insensitive algorithms to accurately

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

compute aggregates in spite of message losses resulting from node and transmission failures. However, this aggregation framework does not address the problem of false sub aggregate values contributed by compromised nodes resulting in large errors in the aggregate computed at the base station, which is the root node in the aggregation hierarchy. This is an important problem since sensor networks are highly vulnerable to node compromises due to the unattended nature of sensor nodes and the lack of tamper-resistant hardware. In the paper, they should make the synopsis diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. In particular, they present a novel lightweight verification algorithm by which the base station can determine if the computed aggregate (predicate Count or Sum) includes any false contribution. Thorough theoretical analysis and extensive simulation study show that the algorithm outperforms other existing approaches. Irrespective of the network size, the per-node communication overhead in the algorithm is O (1).

In [13] Tang L.-A., Yu X., Kim S., Han J., Hung C.-C., and Peng W.-C. introduce trustworthiness analysis of sensor networks Cyber-Physical System (CPS) which integrates physical devices with cyber components to form a situation-integrated analytical system that responds intelligently to dynamic changes of the real-world scenarios. One key issue in CPS research is trustworthiness analysis of the observed data. Due to technology limitations and environmental influences, the CPS data are inherently noisy that may trigger many false alarms. It is highly desirable to sift meaningful information from a large volume of noisy data. In the paper, they propose a method called Tru-Alarm which finds out trustworthy alarms and increases the feasibility of CPS. Tru-Alarm estimates the locations of objects causing alarms, constructs an object-alarm graph and carries out trustworthiness inferences based on linked information in the graph. Extensive experiments show that Tru-Alarm filters out noises and false information efficiently and guarantees not missing any meaningful alarms.

The system performs data aggregation with security and attack handling mechanism. Iterative filtering techniques with initial approximation model are used to secure data aggregation process. Christo Ananth et al. [6] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results.

III.DATA AGGREGATION

To overcome the problem occurred in the iterative filtering algorithm new technique called Certificate Authority (CA) is introduced in each cluster. Data Aggregation is used to aggregate 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 aggregate for secure data transmission. To perform the aggregation more secure the CA is used to check each node condition whether a node is trust node or malicious node. By using the CA the node process are monitored. The data's must be transmitted from member node to cluster head and from cluster head to either cluster head or base station within a given time.

If a time exceeds or any modifications done in the data then the certificate authority checks the threshold value of that node. If the threshold value is in range then the node it trusted node and data aggregation is done through this node. If the threshold value is in out of range then the node is marked as malicious node. After marking the malicious node the data is not transferred at the particular node. Thus the data is transmitted only the trusted node and it can be aggregated more securely and efficiently. Provides more secure for all the nodes because of using the certificate authority. It increases the packet delivery ratio and also improves the performance of non-stochastic components errors such as node fault etc.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

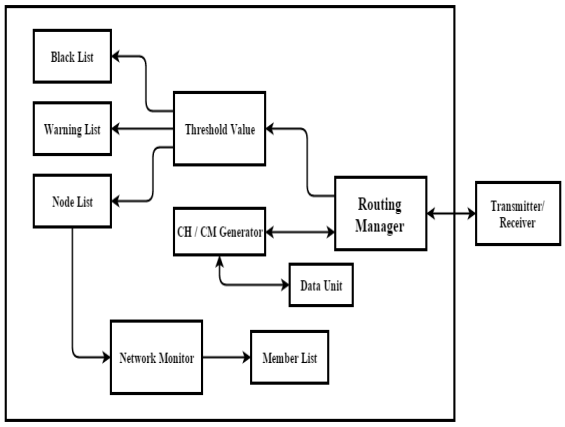

Fig 1. System Architecture

In Fig 1 describes that for every data transmission starts, the routing manager assures that the node is a trusted node or not. Based on the threshold value the node trust is decided. Every node has a specific threshold value. The threshold value is calculated based on the nodes present in the network. If the threshold value is in range then the node is moved to the Node list. If the threshold value is in out of range then the node is moved to the black list. If the threshold value of the node is not justified then it is moved to the warning list.

The trust node is present only in the node list. After the trust nodes are identified then the nodes are monitored by network monitor and add to the member list. The member list nodes are only allowed for data aggregation. The collection of data's are named as data units. The data's are collected from the cluster to the cluster head. This process is also monitored by routing manager. After complete this process the data aggregation starts securely and efficiently.

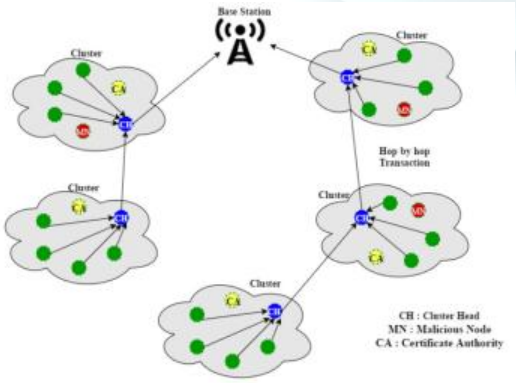

Fig 2 General Aggregation Technique

Initially, all the nodes are aggregated from the base station. The security of the data during aggregation is not ensured. By archiving this security, the certificate authority is provided by each cluster. The certificate authority checks whether the node is an authorized node or malicious node. The certificate is only provided to the authorized node. In fig 1, shows that there are several clusters. Each cluster has a specific set of nodes, cluster head and the certificate authority. The cluster head collects the data from the entire authorized node and it send to the base station. If the cluster head is far away from the base station then it transfers the nearby cluster head and again aggregated to the base station. Sometimes there is a malicious node in the cluster head. There is no communication in the malicious node. The malicious node is only identified by using the certificate authority.

A. Network Design

To create a network with number of nodes which is a wireless sensor network and also create the network with the WSN specifications i.e., each node can communicate with any other node directly which are present in the coverage area of the node. In this network, a group of nodes forming clusters. Each cluster has one leader node which is known as cluster head which will controls the entire traffic present in the cluster of the network and which is a normal nodes.

The other type of node is a certificate authority which monitors the entire traffic and finds the trusted node. The sensor nodes are usually resource constrained with respect to computation capability, memory space, power supply and bandwidth. The network users use some mobile devices to aggregate data items into the network. The network owner is responsible for generating keying materials. It can be offline and then the node is assumed to be uncompromisable.

B. Certificate Authority

This is a node which takes care of all other nodes present in the network by managing the traffic. It is going to check whether the reply's sending by the nodes are appropriate or not in regular intervals, whenever any new node enter in to the network it will check whether the node is hacking node or not by the reply it sending and inform to all other nodes about the new node for the secure data transmission.

If any node is not responding properly then the certificate authority checks the threshold

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

value for that node. If the threshold value is in out of range then it mark the node is malicious node. The data transmission is not done through this node. If the threshold value is in range then the node is a trust node. The data transmission is done through this node. If the threshold value is not justified then the node is moved in to the warning list until the threshold value is justified. The certificate authority work properly and secure efficiently.

C. Monitoring the Traffic

Certificate Authority is used to handle the security process which is important node in the network. It is going to take care of the entire network i.e., it monitors all the nodes and checks which are giving good response based on that it will allow other nodes to communicate with each other. Networks users are assigned aggregation privileges by the trusted authority in a public key infrastructure on behalf of the network owner. However, the network owner may, for various reasons, impersonate network users to aggregate data items.

The compromised entities are regarded as insiders because they are members of the network until they are identified. The adversary controls these entities to attack the network in arbitrary ways. For instance, they could be instructed to aggregate false or harmful data, launch attacks such as Sybil attacks or Denial of Service attacks and be non-cooperative with other nodes.

Data gathered by the individual nodes ultimately routed to the base station. A rate monitoring attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. Thus the node nearer to the base station is monitored continuously and transmits the data after finding that the node is a trust node.

D. Route Discovery Process

Whenever a node want to communicate with other node it have to find the route for forwarding the data. In this route if any new node is entered means there is a chance of that may be a hacking node. So, avoid that hacking nodes for secure data transmission. For this nodes are maintaining a list known as true list, in this nodes are going to store about the other nodes for finding the secure route. In external attacks, the adversary has no control of any sensor node in the network. The communication channel may also be jammed by the adversary, but this can only last for a certain period of time after which the adversary will be detected and removed. Route discovery must be initiated when a source node wants to find a route to a new destination or when the lifetime of an existing route to a destination has expired.

Create trust list

Nodes are going to create a list known as true list. In this they are going to store about the node information's which given proper response to the certificate authority. The utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pin point the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths and replaying signals.

Check trust list

Whenever a node want to send the data it will send route request to other nodes. The node which received the route request packet will checks whether that node is present in the true list or not if presented means it will forward to other nodes and it will repeats until it reaches destination. Route trust is computed by every node for each route in its routing table. It is a measure of the reliability with which a packet can reach the destination, if forwarded by the node on that particular route. For every transmission starts before it check the route whether it is a trust list or hacking list. If it is a trust list then the data aggregation is done securely

IV RESULTS

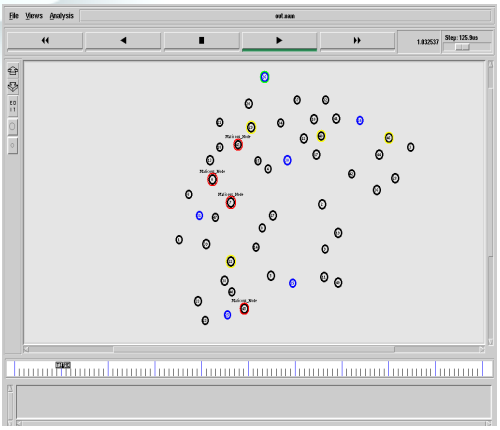

Fig 3.Placing the nodes in the network

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

Fig 3, represents the node placement in the network. The nodes are grouped into the cluster format. Each cluster has own certificate authority. The node 26 denotes the base station in the network. The cluster heads are 31, 30, 24, 25 and 35. The malicious nodes present in the network are 0,7,43 and 45. The certificate authority nodes are 22, 29,46 and 48 which finds the secure node and provide the certificate for only secure node. The malicious nodes are not involved during data transmission.

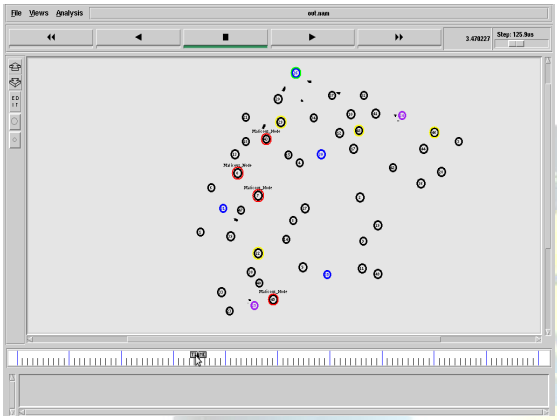

Fig 4 Data Aggregation

Fig 4 represents that data aggregation in wireless sensor network. The data's are gathered by the cluster head from cluster member. The collected data are transmitted from cluster head to cluster head or directly from cluster head to the base station. The data's will not pass through the malicious node. Each cluster has a specific certificate authority. The secure node is identified only by the certificate authority. The certificate authority checks whether the node is the trust node or not and finally the data aggregation is performed.

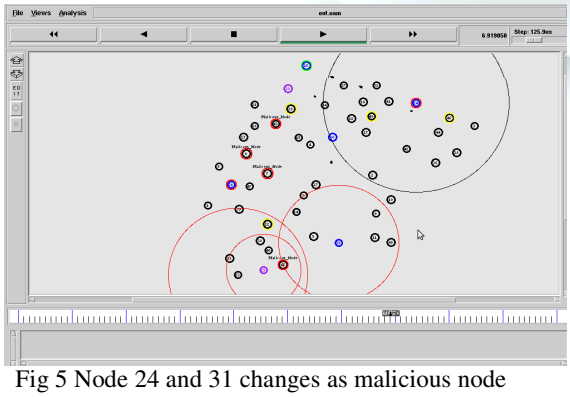

Fig 5 Node 24 and 31 changes as malicious node

Fig 5 represents the node 31 and 24 are change as malicious node. The node 31 and 24 considered as a cluster head during process both the node changed into malicious node. The data's will not transmit through the malicious node even though it is a cluster head. All the nodes present in the cluster should select the new cluster head. The new cluster head collects the data's from cluster member and transmit it to the base station.

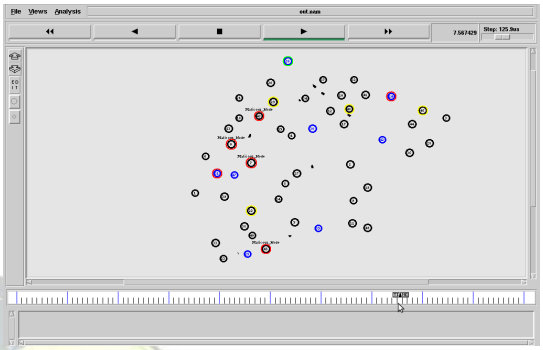

Fig 6 Choose different path after finding malicious node

Fig 6 represents choosing different path after finding the malicious node. If the Cluster Head or Cluster Member is changed into malicious node then the data's cannot be transmitted through that malicious node which may be a Cluster Head or a Cluster Member. Thus the Cluster Member should transmit the data's to another Cluster Head which is not a malicious node present in the network. They select different path for the data transmission to the Base Station.

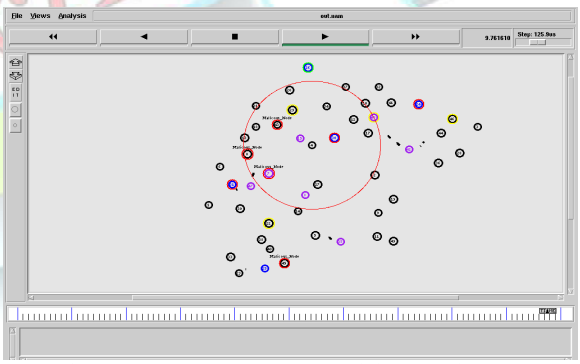

Fig 7 Node 30 changes as malicious node

Fig 7 represents the node 30 changed into a malicious node. During transmission the Cluster Head 30 is changed into malicious node. Now the data's should not be transmitted through that malicious Cluster Head. Thus another Cluster Head is chosen by the Cluster Member and the data transmission get proceed. This prevents the passage of the data's through the malicious node and secures the data's.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

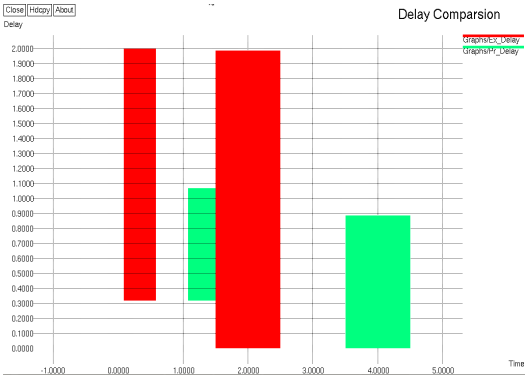

Fig 8Compared with existing delay comparison

Fig 8 represents the comparison of delay with the existing system. Time is plotted along x-axis and delay is plotted along y-axis. The delay gets reduced when compared with the existing system. The data's are transmitted in secure manner even though the delay gets decreased.

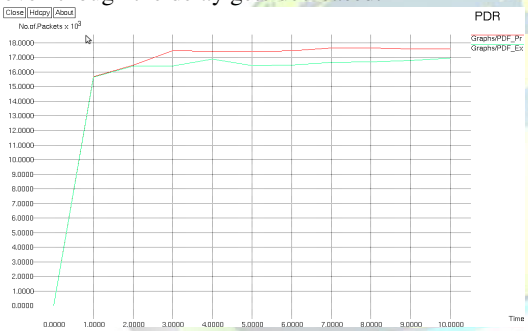

Fig 9 Compared with existing packet delivery ratio

Fig 9 represents the comparison of packet delivery ratio with the existing system. The number of packets involved in delivery is plotted along y-axis and time is plotted along x-axis. The packet delivery ratio gets increased when compared with the existing system. The increased packet delivery ratio will not cause traffic in the network.

V. CONCLUSION AND FUTURE WORK

The proposed trust management scheme that enhances the security of WSN. By using the proposed method Secure routing path can be established in malicious environments. The results of WSN routing scenario positively support the effectiveness and performance of the scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages. The security requirements of wireless sensor networks required to strengthen attack-resistant data aggregation protocols. An algorithm can enable the base station to securely compute predicate count or sum even in the presence of such an attack. The certificate authority computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. The nodes are secured by the proposed method.

In future work, the opinion request is send to the neighbour's node because the source node finds the malicious node. In the presence of malicious nodes, the requirement may lead to serious security problem such nodes may disrupt the routing process. A malicious node can attract all packets by using forged Route Reply packet. The source node broadcasts a Route Request packet to all the nodes present in the network. When destination receives the Request, it can know each intermediary node's address among the route.

REFERENCE

[1] 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.

[2] 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.

[3] Chou C. T., Ignatovic A., and Hu W. (2013), 'Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults', IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1525–1534.

[4] 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.

[5] 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.

[6] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju,S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[7] Lim H.-S., Moon Y.-S., and Bertino E. (2010), 'Provenance-based trustworthiness assessment in sensor networks', in Proc. 7th Int. Workshop Data Manage. Sensor Netw., pp. 2–7.

[8] Ozdemir S. and am H. C¸ (2010), 'Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks', IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749.

[9] 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.

[10] 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.

[11] Shi H.-L., Hou K. M., ying Zhou H., and Liu X. (2011), 'Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN', in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., pp. 1–4.

[12] Sun Y., Luo H., and Das S. K. (2012), 'A trust-based framework for faulttolerant data aggregation in wireless multimedia sensor networks', IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 785–797.

[13]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.

[14] Vuran M. C. and Akyildiz I. F. (2006), 'Spatial correlation-based collaborative medium access control in wireless sensor networks', IEEE/ ACM Trans. Netw., vol. 14, no. 2, pp. 316–329.

[15] 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.