Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 4, Pages 28-33, May 2017

Design of a Dynamic Clustering With Secured Hashing Technique in Wireless Sensor Network

P.K.Poonguzhali[1] and Dr.N.Anandha Moorthy[2]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Coimbatore, India.*
[2]*Professor and Head, Department of Electrical and Electronics Engineering, Hindusthan College of Engineering and Technology, Coimbatore, India.*

Article Received: 29 April 2017 *Article Accepted: 09 May 2017* *Article Published: 12 May 2017*

ABSTRACT

Clustering in the WSN to keep the traffic local sensor nodes would send only to nearby cluster-head within a fixed radius, independent of the network size. Clustering is an appropriate strategy to efficiently organize the network. Moreover, public safety or military networks are structured through a hierarchical organization via operational groups. This organization has an impact on both the mobility of nodes which move in groups, and the data flow since the traffic is mainly intra-group. In this work we propose a novel distributed clustering algorithm suited to such networks, called Dynamic Clustering with Operational Groups. We focus on data aggregation problems in energy constrained mobile networks. A new hash based authentication scheme DCSHT for wireless sensor networks which reduces the computational overhead of sensor nodes is implemented with strong unique message authentication code (MAC) for a particular message. SHA-1 hash function modified with the help of regularly distributed pseudo random function which provide collision resistant requirement for hash functions and the pre-shared secret key obtained from ECDH secret key exchange algorithm. A secure keyed one-way hash functions are provided to improve security in military networks. The simulation results proves the new technique provides secured data aggregation with minimum energy consumption. Performance of the r the proposed DCSHT is analyzed for various parameters packet delivery ratio Time delay A key authority manages this functionality. Keys are updated for every session. Data are authenticated using this key and transmitted between wireless devices. Received data are verified by corresponding cluster heads. The main features is to track the target and distribute the information (target location, distance) to all the nodes with the help of cluster head.

Keywords: Cluster, Data aggregation, Energy efficient and Hash function.

1. INTRODUCTION

Sensor networks are composed of small, battery operated sensors, whose main function is to collect and forward the required data to the base stations. WSN's facilitate monitoring and controlling of physical activities from the surveillance areas with better accuracy. WSN's have applications in a variety of fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. A wireless sensor network (WSN) is an ad-hoc network composed of small sensor nodes deployed in large numbers to sense the physical world. In wireless sensor network most of the energy is consumed during transmission and it is further increased with the distance, as energy consumption is directly proportional to the square of the distance among the nodes.

WSN has various characteristics like Ad Hoc deployment, Dynamic network topology, Energy Constrained operation, Shared bandwidth, large scale of deployment. Despite of these characteristics routing in WSN is more challenging. Firstly, Resources are greatly constrained in terms of power supply, processing capability and transmission bandwidth. Secondly, it is difficult to design a global addressing scheme as Internet Protocol (IP). Furthermore, IP cannot be applied to WSNs, since address updating in a large-scale or dynamic WSN can result in heavy overhead. Thirdly, due to the limited resources, it is hard for routing to cope with unpredictable and frequent topology changes, especially in a mobile environment. Fourthly, data collection by many sensor nodes usually results in a high probability of data redundancy, which must be considered by routing protocols. Fifthly, applications of WSNs require the only communication scheme of many-to-one, i.e., from multiple sources to one particular sink, rather than multicast or peer to peer.

Selecting the optimum sensors and wireless communications link requires knowledge of the application and problem identification. Wireless sensor network (WSN) applications are the fast growing technology trend but security and privacy is still largely ignored, since they are hard to achieve given the limited computation and energy resources available at sensor node level. However, secure communication is a requirement for many WSN applications to ensure integrity and authenticity of transmitting data. In many cases it is sufficient to secure data transfer between the sensor nodes.

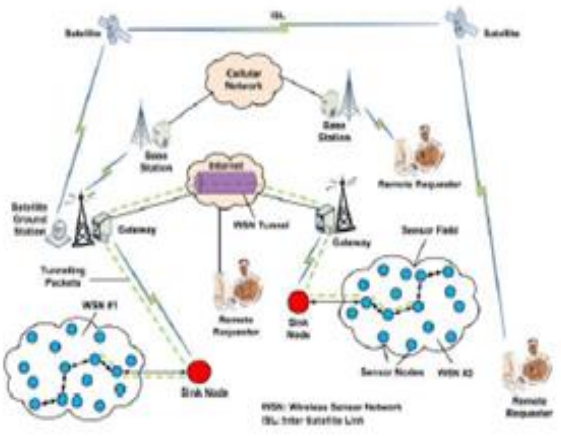

Fig. 1. Articulation of Wireless Sensor Network

Wireless sensor network (WSN) applications are the fast growing technology trend but security and privacy is still largely ignored, since they are hard to achieve given the limited computation and energy resources available at sensor node level. However, secure communication is a requirement for many WSN applications to ensure integrity and authenticity of transmitting data. In many cases it is sufficient to secure data transfer between the sensor nodes. Many WSN applications such as health-care monitoring systems or military domains needs strong and lightweight authentication schemes to secure data from unprivileged users. The authenticity and integrity of messages received by base station greatly influence final tracking results

2. LITERATURE REVIEW

Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collision attacks due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks [1]. However such aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor node is crucial for WSN.As the performance of very low power processors dramatically improves, future aggregation algorithms, thus making WSN less vulnerable. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which make them not only collusion robust, but also more accurate and faster converging.

In Efficient Computation of Robust Average of Compressive Sensor Data in Wireless Sensor Networks in the Presence of Sensor Faults [4] has been introduced. Wireless sensor networks (WSNs) enable the collection of physical measurements over a large geographic area. It is often the case that we are interested in computing and tracking the spatial-average of the sensor measurements over a region of the WSN. Unfortunately, the standard average operation is not robust because it is highly susceptible to sensor faults and heterogeneous measurements noise. A computational efficient method to compute a weighted average (which we will call robust average) of sensor measurements, which appropriately takes sensor faults and sensor noise into consideration

A Trust- Based Framework for Fault-Tolerant Data Aggregation in wireless Multimedia Sensor Networks" was done by Y.Sun,H.Luo and S.K.Das [17] have been introduced for wireless multimedia sensor networks(WMSNs) deployed in noisy and unattended environments, it is necessary to establish a comprehensive framework that protects the accuracy of the gathered multimedia information. In this paper, we jointly consider data aggregation, information trust, and fault tolerance to enhance the correctness and trustworthiness of collected information.

In the research paper, *"**ZoneTrust: Fast zone-based Node Compromised Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing",*** was done by J.W.Ho, M.Wright and S.Das [10] have been introduced. Due to the unattended nature of wireless sensor networks, 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. Researchers have recently proposed a variety of node compromise detection schemes in wireless ad hoc and sensor networks Reputation-based trust management schemes identify malicious nodes but do not revoke them due to the risk of false positives. Similarly, software-attestation schemes detect the subverted software modules of compromised nodes. However, they require each sensor node to be attested periodically, thus incurring substantial overhead.

In Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks", by Suat Ozdemir and Hasan Cam [14]. In wireless sensor networks, compromised sensor nodes can inject false data during data aggregation. However, in this research work a data detection with data authentication protocol, called DAA, is implemented to integrate false data detection with data aggregation and confidentiality. Performance analysis shows that DAA detects any false data injected by up to compromised nodes, and that the detected false data are not forwarded beyond the next data aggregator on the path. Despite that false data detection and data confidentiality increase the communication overhead, simulation results show that DAA can still reduce the amount of transmitted data by up to 60% with the help of data aggregation and early detection of false data.

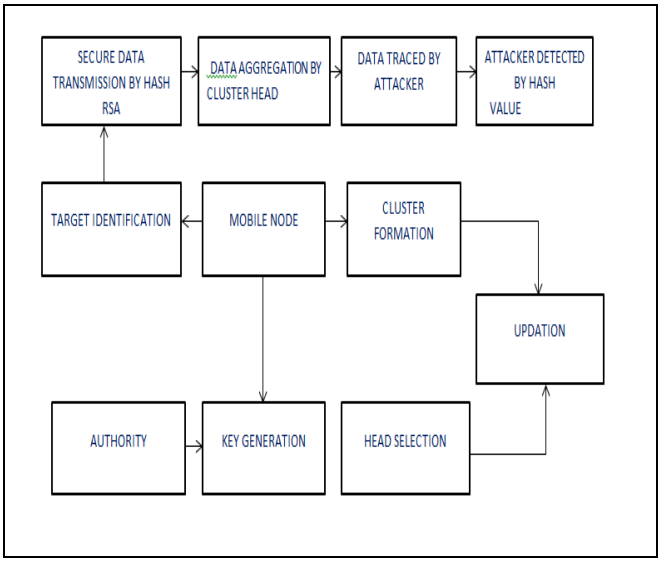

Fig. 2a. Evaluation of Dynamic Clustering with Hashing Technique

3. PERFORMANCE EVALUATION OF DYNAMIC CLUSTERING WITH HASHING TECHNIQUE

Cluster node collects the information from the nodes about the target location and distance. Hashing technique used to eliminate the altered data .It provides the secure data transmission. By using this technique, data is send to the cluster node without packet loss. It minimizes the energy consumption and provide the secure path.

Initially start the process and select the cluster head by energy efficiency. Location of other nodes is shared. If the attacker is traced, it is detected by hash value. Key manager node provides the key value to the cluster head. Once the data is transmitted, key is updated. The required data is not available in the mobile node means it will get the data by using updated transmission .Target location and distance is identified by the node and it is transmitted to the cluster head. Then, the cluster head transmit the information to other neighbouring cluster head.

The main objective of the dynamic clustering is using the data aggregation algorithm for secure data transmission. The cluster head collect the data from other nodes and aggregate the data, then transmits to the neighbouring cluster head. Hashing technique is used for key distribution to the nodes .It is used to identify the altered data and discard it. The nodes identify the target location and distance, then transmit to the cluster head under hashing technique. The cluster head collects and aggregates the data.

The nodes in MANET can act as hosts and routers for sending packets to each other .The network topology keeps changing quickly and randomly, whereas the terminal connectivity changes according to the time. Cluster-based Private Data Aggregation (CPDA) scheme could aggregate data without revealing any private information and consume fewer resources than others. Simulation results show that using the proposed algorithms, efficient data aggregation privacy of communications and computing overhead and energy consumption in wireless sensor network is improved and thus extend the life of the sensor nodes. .For computation of the aggregate functions, the following requirements are to be satisfied: (i) privacy of the individual sensor data is to be protected, i.e., each node's should be known none other expect the node itself, (ii) the number of messages transmitted within the WSN for the purpose of data aggregation should be kept at a minimum, and (iii) the aggregation result should be as accurate as possible. Data aggregation in intermediate nodes (called aggregator nodes) is an effective approach for optimizing consumption of scarce resources like bandwidth and energy in Wireless Sensor Networks (WSNs).

A. Dynamic Clustering

In energy-constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink in such scenarios, Cluster based approach is hierarchical approach. In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to base station (sink). Recently, several cluster-based network organization and data-aggregation protocols have been proposed for the wireless sensor network.

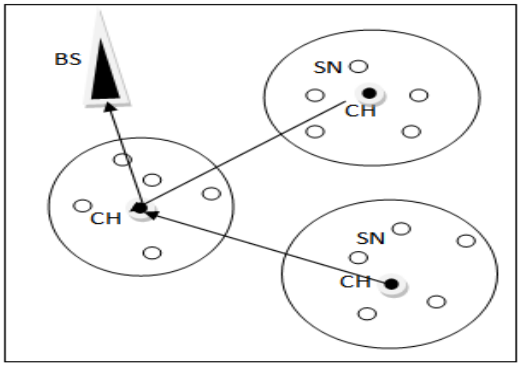

Fig. 2b. Cluster Based Sensor Network

The cluster heads can communicate with the sink directly via long range transmissions or multi hopping through other cluster heads .Energy being the very key concern area with sensor networks, so the main focus lies in developing a mechanism to increase the lifetime of a sensor network by energy balancing. To achieve energy balancing and maximizing network lifetime we use an idea of clustering and dividing the whole network into different clusters. In this paper we propose a dynamic cluster formation method where clusters are refreshed periodically based on residual energy, distance and cost. Refreshing clustering minimizes workload of any single node and in turn enhances the energy conservation. Sleep and wait methodology is applied to the proposed protocol to enhance the network lifetime by turning the nodes on and off according to their duties. The node that has some data to be transmitted is in on state and after forwarding its data to the cluster head it changes its state to off which saves the energy of entire network. Simulation results prove the betterment of our proposed method over the existing Leach protocol.

B. Cluster Formation

Transmitted data can be encrypted and end null packet. The cipher text can be encrypted along with the required random number. The proposed DC-SHP proposes formation of clusters depending upon the respective energy level of each node. It introduces the concept of assigning different energy levels to different nodes to balance the responsibility among the nodes with in a cluster. The node with the highest energy level looks for nodes within its transmission range forms a cluster and appoints itself as the cluster head of the cluster formed .Once the cluster head is identified for a cluster, transmission of data takes place from all the other nodes to the cluster head. Cluster head behaves as the data aggregating node for that particular time interval. As soon as nodes forward the data to the cluster head they move to the wait state and remain in the sleep mode until they have something more to transfer. The proposed protocol helps in conserving energy by only allowing cluster head to communicate with other cluster heads. All other nodes except cluster head are in sleep wait so their energy is preserved. Indirectly as energy is preserved the lifetime of node is increased because lifetime of

a node is defined as the time period till it is capable of transmitting data.

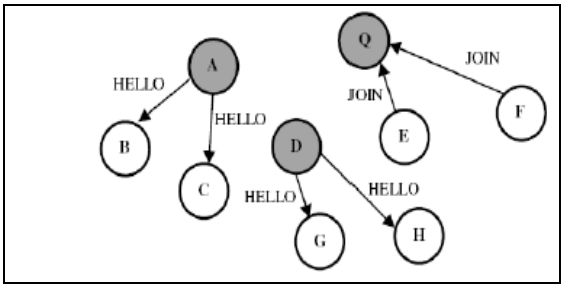

Fig. 3a. Selection of cluster Heads

The data when aggregated [8] at cluster head of each cluster is forwarded to the base station and the energy level of the cluster head is decremented. After a fixed interval of time the energy level of each node in a cluster is revaluated and compared with other nodes and the node having the highest energy is assigned to be the new cluster head of the cluster.

This enables cluster formation even when energy and position of nodes is changing i.e. dynamic clustering. This leads to an effective utilization of energy of each node in the network. Only the nodes with highest energy levels are used for transmission and the energy of all the other nodes is conserved for future use.

C. Key Distribution Technique

Implementing Dynamic Clustering with Hash technique for secure data aggregation in wireless sensor networks eliminates redundancy to improve bandwidth utilization and provide security in energy efficiency of sensor nodes. One node, called the cluster head which is selected based on energy efficiency. It collects data from other nodes and aggregate the data then send to the neighboring cluster head. Hashing technique used for the purpose of security. It uses a random key distribution mechanism proposed for encrypting messages to prevent message from attacks. The key distribution scheme has three phases:

Key pre distribution
Shared-key discovery
Path key establishment.

Target location and distance is identified and then the data is aggregated by cluster head. It is then distributed to other neighboring cluster head.

- CH send the id to centralized Key Manager.
- The CH in the network accept Session Key from centralized key manager.
- CH send target location and distance to all its neighbor.
- CH send rekey to Cluster Member.
- CH sends target location and distance to neighbour head Analyzing.
- Geography location and time.

The Fig.3b shows the cluster head acting as aggregator

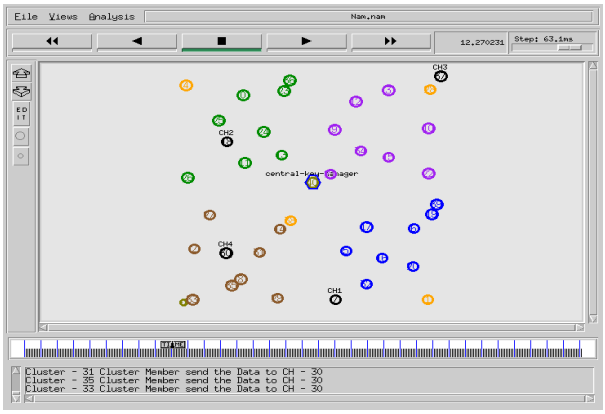

Fig. 3b. Cluster Head Act as an Aggregator

D. Computation with clusters

In this phase, aggregation is done in each cluster. The computation is illustrated with the example of a simple case where a cluster contains three members: A, B, and C, where A is the assumed as the cluster leader and the aggregator, B and C is the cluster members. Let a, b, c represent the private data held by the nodes A, B, and C respectively. The encrypted data is send to the sink node via intermediate node. This intermediate node calls forward subroutine to forward encrypted data to the sink. The encrypted data is set of cipher texts. Sink is a base station, this is a final stage, and the data are received from different wireless sensor node by this stage. In this stage sink receives the cipher texts and performs decryption process by using the private key. Once the decryption is done plain texts are generated which original message or data is sent by the source (sensor).

E. Encryption Function

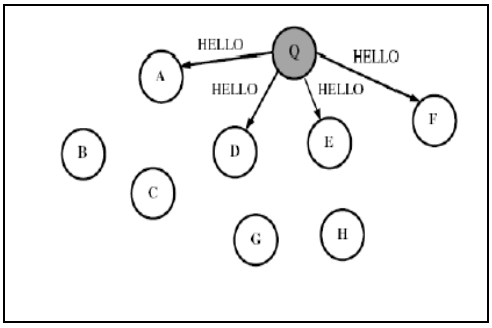

Fig.3c. Query server Q sends HELLO message to its neighbours. A and D randomly elect themselves as the cluster leaders

A query server Q triggers a query by a HELLO message. When the HELLO message reaches a sensor node, it elects itself as a cluster leader with a pre-defined probability pc. If a node becomes a cluster leader, it forwards the HELLO message to its neighbours. If any HELLO message arrives at the node, it decides to join the cluster formed by its neighbour be broadcasting a JOIN message. This process is repeated and multiple clusters are formed so that the entire WSN becomes a collection of a set of clusters. A closely related notion to homomorphic encryption is functional encryption, where our goal is to reveal the result of the computation to the server, but

protect all other information about our encrypted input. For a motivating example consider the problem of spam filtering for encrypted email without interacting with the client. Then the function is used to evaluate would be a classifier that sorts e-mails as either \spam" or \not spam". If we had used homomorphic encryption, the server would learn the encrypted bit (spam/not-spam) Enc (f(x)), but it would be useless for sort e-mail messages. Instead like to allow the server to evaluate Enc (x)! f(x) but just for the particular function f and nothing else (e.g). We don't want the server to compute this for f(x) = (x). As a key approach to fulfilling this requirement of private data aggregation, concealed data aggregation schemes have been proposed in which multiple source nodes send encrypted data to a sink along a converge-cast tree with aggregation of cipher-text 4. Cluster-Based Private Data Aggregation.

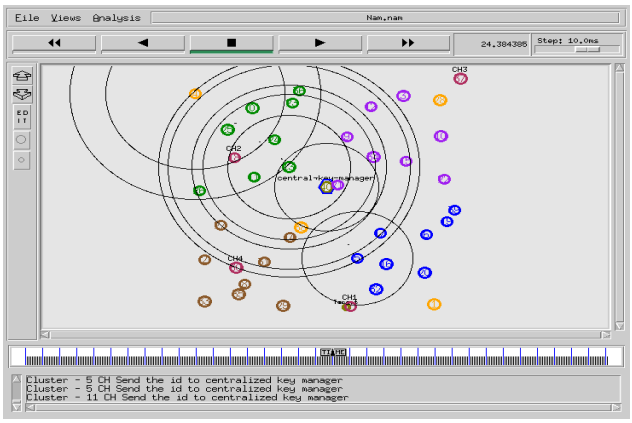

Fig. 4a. CH send the id to centralized Key Manager

4. Performance Evaluation

A. Simulation Results and Comparison

In order to evaluate the performance of the proposed DCSHT technique, we compare MILP with the energy consumption and delay constrained routing protocol. In the fig 4b represents the number of nodes varying with respect to the delay as compared with MILP optimal formulation.

It explained our proposed algorithm is better than the MILP formulation. Performance has been analyzed for Efficiency, Packet Delivery Ratio and Time Delay.

B. Efficiency

Efficiency is the (often measurable) ability to avoid wasting materials, energy, efforts, money and time in doing something or in producing a desired result in a more general sense, it is the ability to do things well, successfully and without waste. In more mathematical or scientific terms, it is a measure of the extent to which input is well used for an intended task or function (output).

It often specifically comprises the capability of a specific application of effort to produce a specific outcome with a minimum amount or quantity of waste, expense or unnecessary effort. Efficiency of course refers to very different inputs and outputs in different fields and industries.

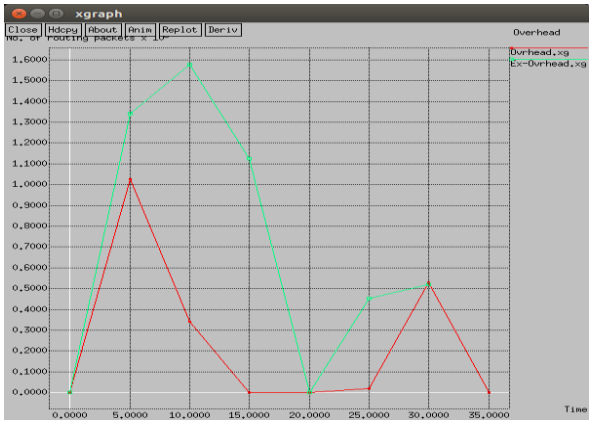

Fig. 4b. Time Vs Overhead

C. Packet Delivery Ratio

Packet Delivery Ratio: The ratio of the number of delivered data packets to the destination.

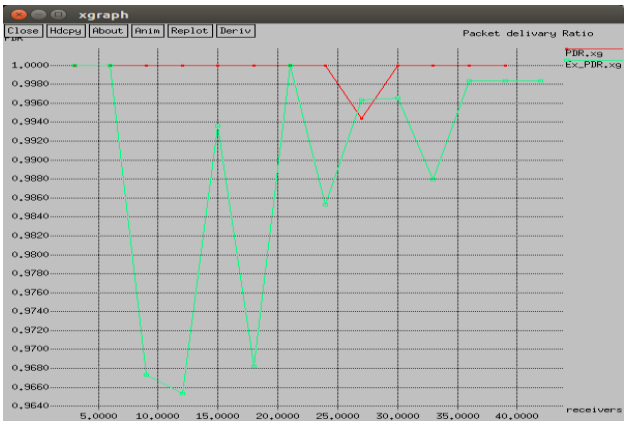

Fig. 5. Time Vs Packet Delivery Ratio

D. Time Delay

Time Delay is an important design and performance characteristics of a computer network or tele communication network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or end point to another. It is typically measured in multiples or fraction of seconds.

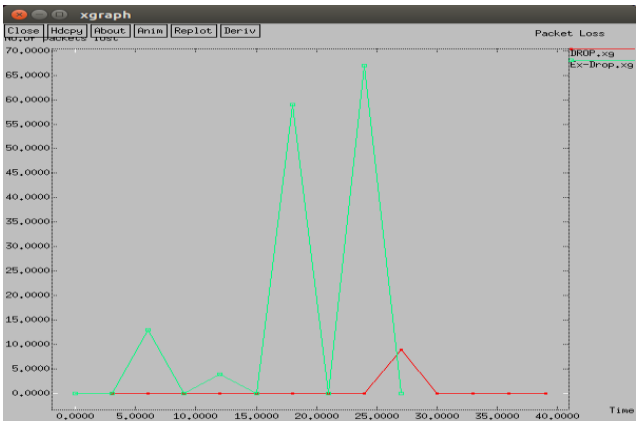

Fig.6. Time Vs Packet Loss

Time Delay is the difference between end time and start time. Transmission delay (store and forward delay, also known as packet delay**)** is the amount of time required to push all the

packets bits in to the wire. In other words this the delay caused by the data rate of the link.

5. CONCLUSION

Data privacy is the important parameter for the secure transmission in wireless sensor network. The optimal probabilistic encryption scheme can be provide more security in the transmission but while considering the data privacy this encryption technique can alter the information. The proposed scheme has no communication overhead and minimal processing requirements making it suitable for sensors with limited resources. In future, mobility based energy conservation schemes are relatively new in the field of wireless sensor networks and many aspects need to be studied with more attention. Developing a scheduling mechanism based on the past history and choosing appropriate communication parameters to achieve the above goal can be considered as a future work.

REFERENCES

[1] K. K. Gupta1, R. Gupta, Wavelet Based Speckle Filtering of the SAR Images, *International Review on Computers and Software*, Vol. 1, n. 3, pp. 224-232, 2006.

[2] C. de Kerchove and P. Van Dooren, "Iterative filtering in Reputation systems," *SIAM. J. Matrix Anal. Appl.*, vol. 31, no. 4, pp. 1812–1834, 2010.

[3] M. Abou-Nasr, Real world data mining applications. *Springer Publishing Company, Incorporated*, 2014.

[4] K. Ni, N. Ramanathan, M. N. H. Chehade, L. Balzano, S. Nair, S. Zahedi, E. Kohler, G. Pottie, M. Hansen, and M "Sensor network data fault types," *ACM Trans. Sen. Netw.*, vol. 5, no. 3, pp.25:1–25:29, Jun. 2009.

[5] D. Wagner, "Resilient aggregation in sensor networks," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '04. New York, NY, USA: ACM, 2004, pp. 78–87.

[6] Y. Zhang, N. Meratnia, and P. Havinga, *"Outlier detection techniques for wireless sensor networks: A survey," Commun. Surveys Tuts.*, vol. 12, no. 2, pp. 159–170, Apr. 2010.

[7] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy constrained modulation optimization," *IEEE Trans. Wireless Commun., vol. 4, no. 5*, pp. 2349–2360, Sep. 2005.

[8] .R. A. Leon, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *IEEE Trans .Power Del., vol. 22, no. 2, pp. 1021–1028, Apr. 2007.*

[9] G. S. A. Kumar, G. Manimaran, and Z. Wang, "End-to-end energy management in networked real-time embedded systems," *IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 11, pp. 1498–1510,* Nov. 2008.

[10] M. Burkhart, P. von Rickenbach, R. Wattenhofer, and A. Zollinger, "Does topology control reduce interference," *in Proc. ACM 5th Int. Symp. Mobile Ad Hoc Netw. Comput.* 2004, pp. 9–19.