ISSN 2047-3338

Performance Degradation of Heterogeneous Wireless Sensor Network in the Presence of Non Cooperative Nodes

R. Juliana[1] and Dr. P. Uma Maheswari[2]

[1]Department of Computer Science and Engineering, Chettinad College of Engineering and Technology, Karur, India
[2]Department of Computer science and Engineering, Info Institute of Engineering, Coimbatore, India

***Abstract*– Recently Wireless Sensor Networks (WSN) has gained research interest for remote area monitoring and tracking in unattended environments. WSN may be heterogeneous to provide resources and aggregation of resources will be helpful for efficient distributed computing. Sensor nodes in WSN are used to collect application specific data, perform some pre computing and send the computed values to sink nodes or base station where the application resides. Usually message sending is done by multi hop forwarding. Since each node is battery powered, the major goal of WSN is to maximize the battery life time. Among the different types of routing methods cluster based routing is the best one for energy conservation. But some of the nodes either do not cooperate for routing and forwarding the data or perform malicious activities such as fabrication, content alteration and Denial of Service attacks. In this paper the performance degradation of WSN due to non cooperative nodes is studied. Simulation result shows that performance is degraded in a significant level when some nodes of WSN are non cooperative.**

***Index Terms*– Wireless Sensor Networks, Cluster Based Routing, Non Cooperative Nodes and Performance Degradation**

I. INTRODUCTION

WSN has large number of small, cheaper and multifunctional sensor nodes that are deployed randomly. Each sensor node has a global identifier, sensing sub system, external memory, computing component, limited power source and an interface for communicating with other nodes. Each node has some coverage area and communicates with other nodes within its coverage area by a broadcast mechanism. Some WSN allows mobility for the sensor nodes, so each sensor node is self configurable and the topology may change frequently [1].

In WSN, sensor nodes operate together by monitoring some environment and collect the application specific data, perform some computing such as aggregation or compression then send to the sink node where the application resides. There are two types of WSN; Structured and unstructured. In structured WSN only few nodes are deployed in the pre-determined place. This reduces the overhead and cost of network connectivity management and failure detection. In Unstructured WSN nodes are deployed in denser in ad-hoc manner and after deployment the network is unattended. Because of having large number of nodes, the connectivity management and failure detection is hard. Based on the environment where WSN is used, WSNs are classified into multimedia WSN, mobile WSN, underground WSN, Underwater WSN and terrestrial WSN [2].

Traditionally, in WSNs major focus was on providing the Quality of service (QoS). But sometimes practically it is not possible to recharge the batteries. Therefore the recent goal of WSNs is to maximize the battery life time. Therefore energy efficient protocols are needed to minimize the consumption of energy and maximize the battery life [4]. Usually communication sub system consumes high energy than all other subsystems in a sensor node. There are three techniques used to reduce the power consumption. They are duty cycling, data driven approaches and mobility. In duty cycling nodes can go alternatively between sleep state and active state. Nodes decide to be active during the transmission of data and make neighbours also active during data transmission because data are forwarded to base station by single or multi hop transmission. In data driven approach, unneeded samples are avoided. For highly correlated data it is not needed to send the redundant data. It also reduces the power consumption of the sensing sub system. In the third approach, some nodes are made to be mobile, so mobile nodes are responsible for collecting data from static nodes. Some entities are attached to mobile nodes for roaming in the sensing field.

Because of some inherent characteristics of WSNs, routing is a challenging task [5], [6]. The inherent characteristics are: 1) Resources of WSN are power supply, processing capability and transmission bandwidth, 2) Designing a global addressing scheme is very difficult. Because if there is large number of nodes and they are mobile, then updating the address will be a great overhead, 3) Most of the sensor nodes give redundant data, 4) In time sensitive applications, data should reach the sink node within a predetermined time, and 5) Communication is of the type of many to one. All the sensor nodes send the data to the sink node where application resides. In most of the applications energy conservation is very important than QoS.

Many routing protocols are suggested for WSNs. Cluster based routing is one of the efficient routing method that conserves energy. Sensor nodes form clusters and within the cluster, cluster head aggregates the data from member nodes to sink node [7], [8]. Base station is deployed center of the cluster to reduce power consumption for data transmission. Since energy saving is a severe constraint in WSNs, some nodes may drop packets or inject false packets. Nodes which drop packets are called as selfish nodes and nodes which inject false packets are called as malicious nodes. Detecting these non cooperative nodes is very hard since they have legitimate keys. To avoid the influence of these non cooperative nodes, the following tasks should be done. 1) Paths from a normal node to sink node should not go through a selfish or malicious node to avoid packet dropping. 2) Packets originated from the selfish or malicious nodes should not be sent to the sink node [9].

Clustering algorithms can be implemented in both types of WSNs. They are homogeneous and heterogeneous WSNs. In homogeneous WSNs all the nodes have same level of energy and in heterogeneous network each node has different energy level. Low-Energy Adaptive Clustering Hierarchy (LEACH), Power Efficient Gathering in Sensor Information Systems (PEGASIS), and Hybrid Energy-Efficient Distributed clustering (HEED) are algorithms designed for homogenous WSN. Stable Election Protocol (SEP), Distributed Energy-Efficient Clustering (DEEC), Developed DEEC (DDEEC), Enhanced DEEC (EDEEC) and Threshold DEEC (TDEEC) are algorithms designed for heterogeneous WSN [10].

II. RELATED WORK

Soroush Naeimi, Hamidreza Ghafghazi , Chee-Onn Chow and Hiroshi Ishii presented a Survey on the Taxonomy of Cluster-Based Routing Protocols for Homogeneous Wireless Sensor Networks [11]. The cluster-based protocols had increased interest in homogeneous Wireless sensor networks because of their better scalability and high energy conservation. Since each sensor node had limited energy, processing capabilities and communication coverage range, routing algorithms that could operate efficiently with limited resources must be used. The different stages of cluster based routing were cluster head selection, cluster formation, data aggregation and data communication. Some of the advantages of cluster based routing are 1) It minimized the power needed for transmission. 2) It balanced the load among all the nodes. 3) It reduced the overhead of routing and topology maintenance. 4) It eliminated redundant data and highly correlated data by performing aggregation. 5) Routing step was localized in the boundaries of the clusters, so small size routing table was enough. The taxonomy of different cluster-based routing protocols was summarized for homogeneous WSNs. Each one was suitable for particular scenario.

Sajid Hussain and Abdul W. Matin presented a Hierarchical Cluster-based Routing in Wireless Sensor Networks [12]. Hierarchical cluster-based routing (HCR) was an extended version of LEACH protocol. In LEACH, the WSN was divided into several clusters randomly and each cluster was managed by a cluster head (CH). Each sensor node collected environmental data and transmitted to their cluster heads. Cluster heads aggregated the received data from the sensor nodes and sent to the base station. Energy efficient clusters were identified by heuristics-based approach. Energy efficiency clusters were created by genetic algorithms. The GA-based clusters configuration was created by the base station and broadcasted to all the sensor nodes in the network. Simulation result showed that Hierarchical cluster based routing gave energy efficiency than LEACH algorithm.

Rajni Meelu and Rohit Anand presented performance evaluation of cluster-based routing Protocols used in heterogeneous wireless sensor Networks [13]. In WSN cluster based routing was one of the efficient routing algorithms for energy conservation. Distributed Energy Efficient Clustering (DEEC) was a clustering based protocol used in heterogeneous WSNs. DEEC evaluated the dead nodes for calculating network lifetime, energy consumption and based on these details it balanced the energy. Modified form of DEEC was Clustering Technique for Routing in Wireless Sensor Networks (CTRWSN). It was a self organizing, dynamic clustering method that divided the nodes into clusters dynamically based on a priori fixed clusters. Two clustering protocols DEEC and CTWRSN were compared in terms of their network lifetime, energy consumption and the energy balancing. Simulation results showed that CTWRSN gave good energy distribution, so the network life time was 40 % prolonged when comparing to DEEC routing protocol.

Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho presented Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection [14]. Hierarchical Trust Management was a scalable cluster based routing protocol for WSNs that used trust management for dealing selfish and malicious nodes. Each node in WSN had different social and Qos behavior. Based on these behaviors a probability model was created. The model used subjective trust and objective trust of the sensor nodes. Subjective trust was generated based on the expected behavior of sensor nodes. During execution at run time objective trust was obtained based on the actual status of the node. By the comparison of subjective and objective trusts of a node best trust composition was identified to maximize the performance of the application. Optimal trust threshold was used to minimize the false positives and false negatives. This trust based method gave performance closer to ideal performance in terms of delivery ratio and message delay.

Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta presented a method for Selfish Behavior Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System [15]. This was a low cost scheme to find selfish nodes. Some nodes in network did not cooperate in message forwarding and routing to save their memory, bandwidth, and power by discarding packets from the other nodes. They were called as selfish nodes. The reliability and the performance of network were affected because of those non cooperative nodes. So finding selfish nodes and force them for cooperation was needed to improve the performance. A model to increase the detection rate of selfish node and decrease the false detection rate was developed to increase the efficiency of the system. Some of nodes were in monitoring mode. Each node in monitoring mode maintained a record of data and control packets forwarding about its neighboring node. Record had the fields: 1) Last action, 2) Last request and 3) Status. Initially the value for status was set to zero then every time it was updated by the monitoring node. For every action the first two fields were updated. By using the recent values about these three fields, selfish nodes were identified. The nodes which refused to carry out the networking tasks and used the services offered by other nodes of the network were identified as selfish nodes. Sometimes selfish nodes also ignored packets destined to them to save the power resource.

III. MATERIALS AND METHODS

In heterogeneous WSNs each sensor node has energy level and collectively they can be used to perform distributed computing. Among the different types of routing methods in WSN, cluster based routing has been proven as the best one for consuming less energy. Each node is allocated into a cluster. One node in a cluster is elected as cluster head and remaining nodes in the cluster are cluster members. Each member node senses some environmental data and sends to head of the cluster. Cluster heads (CHs) are responsible for processing, filtering and aggregating the data sent by the member nodes belonging to their cluster. This will reduce the network load and alleviate the bandwidth. The preprocessed data will be sent from the cluster head to base station either by single or multi hop transmission. Base station is deployed in the central position to reduce the power consumption for communication. So there are two types transmission occurs in cluster based routing. Intra cluster transmission and inter cluster transmission. Cluster heads are selected based on the coverage cost aware metrics, network scalability and energy consumption. Sometimes cluster head role is assigned in rotation basis.

In this paper cluster based routing is used in WSNs that had some malicious nodes and the performance of the network is studied.

IV. EXPERIMENTAL RESULTS

Simulations are conducted to compare the performance of wireless sensor networks when some sensor nodes are selfish or malicious nodes. The experimental setup is made up of 40 nodes spread over an area of 4000m x 4000m. The wireless links communicate with a bandwidth of 2 Mbps. The simulations are run for 300 sec. The performance metrics used are number of packets dropped, delay, throughput and number of retransmission attempts. These performance metrics are shown graphically from figure 1 to 4. In the following figures blue line indicates the performance of WSNs when all the nodes are normal. Red line shows the performance when some nodes are selfish nodes or malicious nodes.

Fig. 1 shows the number packets dropped in WSNs. By the comparison malicious node drops more number of packets when comparing to the normal nodes.

Fig. 2 shows the delay in WSNs. Delay increased in the presence of malicious nodes is around 60% when comparing to network with all cooperating nodes.

Fig. 3 shows the number of retransmission attempts in WSN when some nodes are malicious nodes. When comparing to WSNs with all the normal nodes, more than 30 % of packets are retransmitted if some nodes in WSNs are non cooperative.

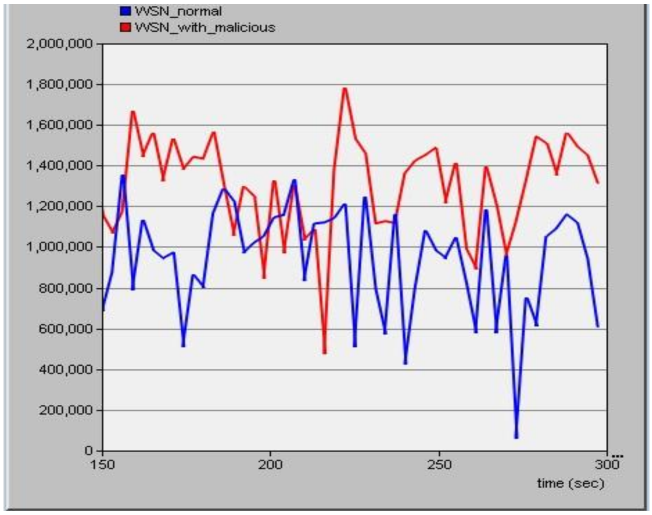

Fig. 1: Number of packets dropped

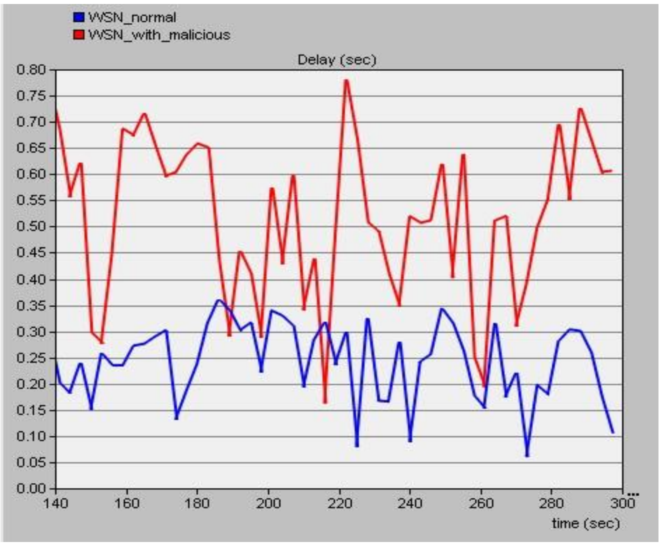

Fig. 2: Delay

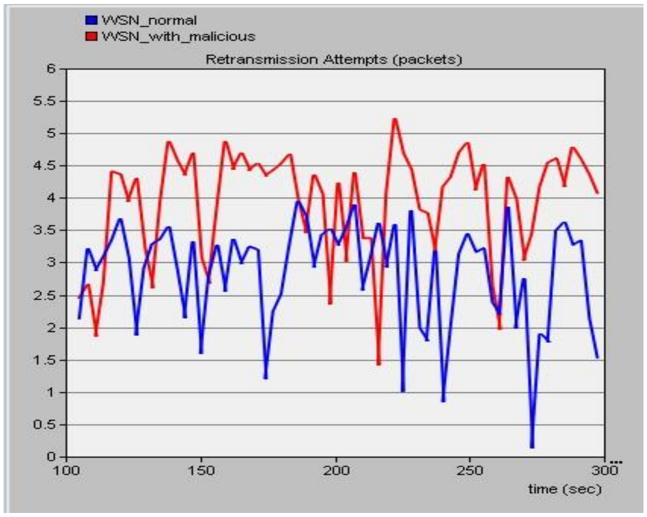

Fig. 3: Number of Retransmission attempts

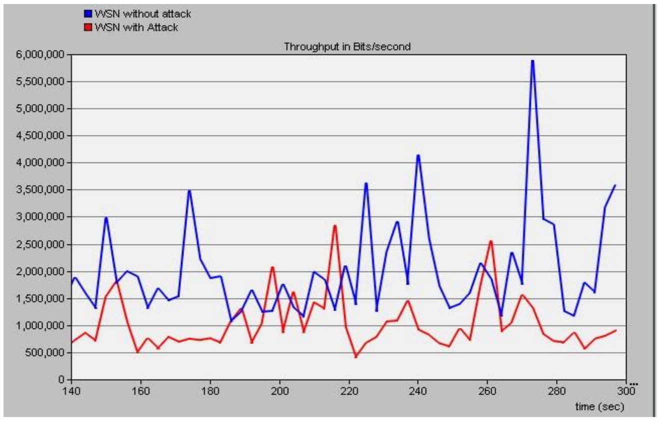

Fig. 4: Throughput

Fig. 4 shows throughput in WSNs. By the comparison, the average throughput is increased 3 to 4 times when all the nodes are cooperative.

V. CONCLUSION

Recent goal of WSN is energy conservation rather than providing the Quality of service. In the sensor nodes most of the power is consumed by the message transmission. So energy conserving routing protocol is needed. Cluster based routing has been proved as an energy conserving protocol. But some nodes either do not cooperate for routing and forwarding the data or perform some malicious activities such as fabrication, content alteration and DOS attacks. These nodes affect the performance of the network. In this paper the performance degradation of WSN due to non cooperative node is studied. Simulations are conducted to compare the performance of wireless sensor networks when some sensor nodes are selfish or malicious nodes. The performance metrics used are number of packets dropped, delay, throughput and number of retransmission attempts. Simulation result showed that performance is degraded in a significant level when some nodes of WSN are non cooperative.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Mag., Aug. 2002, pp. 102–114.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey “, International journal in Elsevier, 2008.

[3] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella, “Energy Conservation in Wireless Sensor Networks: a Survey”, www.info.iet.unipi.it

[4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan “Energyefficient communication protocol for wireless microsensor networks”, In Proceedings of the Hawaii International Conference on System Sciences, January 2000.

[5] Sustainable Wireless Sensor Networks; Seah, W., Tan, Y. Eds.; InTech Open Access Publisher: Rijeka, Croatia, 2010.

[6] Li, C.; Zhang, H.X.; Hao, B.B.; Li, J.D. A survey on routing protocols for large-scale wireless sensor networks. Sensors 2011, 11, 3498–3526.

[7] V. Mhatre and C. Rosenberg, “Design Guidelines for Wireless Sensor Networks: Communication, Clustering and Aggregation,” Ad Hoc Networks, 2(1), 2004, 45–63.

[8] L.M.C. Arboleda and N. Nasser, “Comparison of Clustering Algorithms and Protocols for Wireless Sensor Networks,” Canadian Conference on Electrical and Computer Engineering, May 2006, pp. 1787-1792.

[9] Lei Huang, Lixiang Liu , ” Extended Watchdog Mechanism for Wireless Sensor Networks “ , Journal of Information and Computing Science Vol.3, No. 1, 2008, pp. 39-48 .

[10] T. N. Qureshi, N. Javaid, M. Malik, U. Qasim, Z. A. Khan, “On Performance Evaluation of Variants of DEEC in WSNs “, arxiv.org, 2012.

[11] Soroush Naeimi , Hamidreza Ghafghazi , Chee-Onn Chow and Hiroshi Ishii , “ A Survey on the Taxonomy of Cluster-Based Routing Protocols for Homogeneous Wireless Sensor Networks “ , Open access Journal, 2012.

[12] Sajid Hussain and Abdul W. Matin, “Hierarchical Cluster-based Routing in Wireless Sensor Networks “.

[13] Rajni Meelu & Rohit Anand, “performance evaluation of cluster-based routing Protocols used in heterogeneouswireless sensor Networks “, International Journal of Information Technology and Knowledge Management January-June 2011, Volume 4, No. 1, pp. 227-231.

[14] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection”, IEEE Transactions on Network And Service Management, Vol. 9, No. 2, June 2012.

[15] Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta, “A method for Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System”, International Journal of Research Review in Engineering Science and Technology (ISSN 2278- 6643) | Volume-1 Issue-2, September 2012.