International Journal of Soft Computing 6 (5-6): 210-215, 2011
ISSN: 1816-9503
© Medwell Journals, 2011

# Intelligent Secured Fault Tolerant Routing in Wireless Sensor Networks Using Clustering Approach

[1]K. Kulothungan, [1]S. Ganapathy, [2]S. Indira Gandhi, [1]P. Yogesh and [1]A. Kannan
[1]Department of Information Science and Technology, College of Engineering,
[2]Department of Electronics Engineering, MIT, Anna University, Chennai, India

**Abstract:** In wireless sensor networks, the nodes are deployed randomly over a large geographical region for monitor and collect the data. These nodes are powered by battery and are impossible to get recharged after deployment. Thus, minimizing the energy consumption of the sensor nodes is a challenging issue in wireless sensor networks for guaranteeing the network's lifetime. Clustering is one of way to maintain an effective topology in wireless sensor networks in order to reduce the overall network's energy consumption. In wireless sensor network providing an energy efficient in sensor networks is more difficult due to lack of infrastructure in the predicting the location of each node in the network. In this study, researchers propose a new clustering scheme that optimizes energy using a clustering algorithm to enhance the performance of the network. In addition, fault tolerant routing is proposed in this research by considering cluster sub heads. Therefore, we have modified the AODV with a clustering and security features to reduce the number of nodes involved in routing and to avoid denial of service attacks. We compare the performance of this proposed protocol with AODV with respect to distance and energy metrics. This modified AODV with clustering improves the QoS in terms of packet loss, packet delivery ratio and end-to-end delay.

**Key words:** WSN, QoS, AODV, clustering, packet loss, end-to-end delay

## INTRODUCTION

Wireless Sensor Networks (WSNs) are used in many applications including disaster and emergency recovery, battlefields and mobile conferencing. Traditional routing protocols of wired networks cannot be applied directly in sensor networks due to its energy constrained nodes. Ad hoc on-demand Distance Vector (AODV) routing protocol uses an on-demand approach for finding routes (Tang and Zhang, 2004). The main advantage of this routing protocol is that the routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The major limitations of AODV are multiple RouteReply (RREP) packets in response to a single RouteRequest (RREQ) packet and inconsistent routes in intermediate. The heavy control overhead of high-density WSN requires a cluster structure for achieving better performance and since cluster structure reduces the routing overhead. Clustering helps to form small groups of nodes by dividing a large network into sub groups based on certain rules (Chansu *et al*., 2004; Chao and Chang, 2008). Any node in each cluster is dynamically elected to the role of cluster head based on some criterion (energy, distance from the base station and lowest ID). Nodes within minimum hop within the transmission range of a cluster head will become the cluster member. A gateway is a non-cluster head node with inter-cluster links, so it can access neighboring clusters and forward information between clusters. Various distributed computation techniques can be applied to create clusters dynamically in WSN. A cluster topology provides effectively manage the resources to improve the computation power reduced overhead during data transmission even, minimize end to end delay and maximized throughput.

In wireless sensor network, clustering the network in order to improve the packet delivery is more challenging task than in wired networks because of the complexity in identifying the location of each node and power requirements in these nodes. Moreover, dynamic routing is very difficult in the sensor networks while finding the best route by taking the special characteristics like energy, distance, mobility, limited bandwidth, limited processing power and high bit-error rate. In addition to that every node needs to forward other node's data. The network resource should be fairly distributed across the network in order to avoid the high consumption of the resources in few nodes in the network.

**Corresponding Author:** K. Kulothungan, Department of Information Science and Technology, College of Engineering, Anna University, Chennai, India

The routing algorithm for sensor networks should be designed in such a way that it should have the capability to self optimize during frequent changes in the network environment. Most of the existing routing algorithms for wireless sensor networks have been implemented by considering static nodes and only with power metric. However, power reduction is not the only metric for selecting cluster heads. Therefore, it is necessary to propose a new power aware routing algorithm that considers other QoS metrics also. In this study, researchers introduce a self optimized clustering algorithm with the routing layer with modified clustering algorithm based on K-hop clustering algorithm. Then, we also develop a clustering agent that runs as a supporting module for the routing process, this receives information from routing layers and makes the update in the routing tables.

To enhance the cluster structure, the metric or the cost used for cluster formation is the key issue that needs to be addressed. In this regard, a control packet needs to be exchanged between the nodes in the sensor network during the re-clustering and the stationary assumption for cluster formation while compared with a flat structure. Various clustering schemes need to re-form the cluster and to elects a cluster head whenever there is any node failure, cluster head failure or on regular interval. This is called the ripple effect of re-clustering.

In addition to clustering, researchers consider the path length to the cluster head as a main metric in order to maximize the network lifetime. The energy consumption of each node is reduced by minimizing the number of participating nodes during the transmission of data from the source node to base station. Shortest path is obtained in this research using Minimum cost Spanning Tree (MST) algorithm. This algorithm helps to find the suitable node for cluster head by computing the cost of all the links between nodes using energy and distance. Moreover, a sleep scheduling strategy has been adopted by identifying the nearest neighbor of each participating node. This research also addresses the issues related with node and cluster head failure by a fault tolerant (Chao and Chang, 2008) mechanism.

**Related work:** Due to the sensors limited power nature, an innovative techniques that improve energy efficiency to prolong the network lifetime. There are many works in the literature that detail with power aware routing in networks (Chansu *et al*., 2004; Heo *et al*., 2009). In many applications of WSNs, clustering scheme is usually adopted to reduce the communication overhead and eliminate redundant information during the transmission of the data from the node to base station.

Kim *et al*. (2007) proposed a two-phase scheme called Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm based on single-hop communication of each node with their base station. This uses a dynamic clustering approach that constantly changing clusters and randomly choose the role of the cluster head among sensor nodes in the network. LEACH is a typical clustering algorithm used in WSNs. There are many researchers studying the WSNs' clustering routing scheme based on LEACH. HEED (Younis and Fahmy, 2004) periodically selects cluster heads based on various parameters such as node residual energy, node proximity to their neighbors and node degree, to reduce the energy consumption during the multi hop communication. In this study, researchers analyze the energy consumption during the transmission of the aggregated data to the base station.

In a WSN, data dissemination and data gathering are involved during the transmission of data from the source to the destination. Due to the inherent nature of these networks, a sensor node may fail and hence the route discovered earlier will also fail. As a result of these failures, a data packet may not reach the sink instead it may be discarded. Therefore, it is necessary to consider the fault tolerant issue in routing protocols. However, most of the existing routing protocols do not consider fault tolerant as an important issue (Chao and Chang, 2008; Mengjie *et al*., 2007). In order to handle this problem, this research work proposes a Fault Tolerant Routing protocol with a capability for error reporting in sensor networks.

Security is another important issue to be considered while designing wireless sensor networks as wireless sensor networks may be deployed in hostile areas such as battle fields (Mulay *et al*., 2010). Therefore, clustering and fault tolerant routing protocols should be provided with effective security mechanisms so that it can avoid Denial of Service (DoS) attacks leading to higher energy consumption when packets are made into multiple packets by the intruders (Liu and Yu, 2005; Tavallaee *et al*., 2010). In this research work, a secure routing protocol that considers energy consumption problem, fault tolerance issue and intrusion detection has been proposed and implemented in order to improve the Quality of Service (QoS) in WSNs. The major applications of this new fault tolerant secure routing algorithm are civilian and military scenarios including environmental monitoring, surveillance for safety and security, automated health care, intelligent building control, traffic control and object tracking.

In this study, researchers propose a scheme to self optimized clustering by modifying the K-hop clustering with Minimum Spanning Tree (MST) algorithm. We provide MST, to interface with the cluster formation and analyze the performance of WSN network with hierarchical architecture. This algorithms are analyzed in wireless sensor network in terms of packet delivery ratio, end-to-end delay, throughput and overhead in control packets.

## MATERIALS AND METHODS

The architecture of the system proposed in this research work is shown in Fig. 1. It consists of seven modules namely trace data set, cluster formation module, threshold setting module, fault tolerance manager, security module, rule base and administration module. The trace data set is collected from the network. The cluster formation module consists of three sub modules namely cluster head selection module, minimum spanning tree formation module and the cluster optimization module. All these three sub modules are responsible to form clusters for the network. The threshold setting module is useful for setting a threshold to select the cluster head. The fault tolerance manager consists of two components, one for handling the node failures and the other to handle link failures. The overall control of the system is with the administration module. This module initiates the communication and on receipt of the acknowledgement or expiry of the timer, it closes the communication. This module controls the cluster formation, cluster head election, failure analysis and is also responsible for secure communication. In order to provide effective security to the packets sent through the network, this module uses the services of the security module. The security module consists of intrusion detection module. This modules use intelligent agents that use rules present in the rule base for effective decision making.

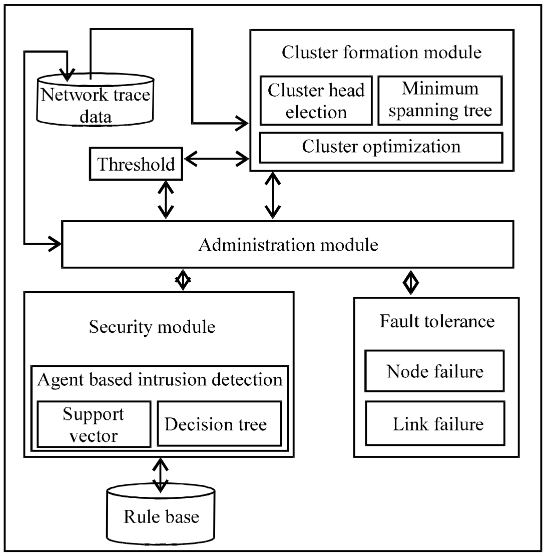

Fig. 1: System architecture

**Proposed work:** This proposed research focuses on three important aspects namely, cluster based routing, fault tolerance in routing and security through key management and intrusion detection. This system collects trace data from the network periodically and performs clustering. After performing cluster head election, sub cluster head is also elected that will change periodically. The cluster sub heads are used for fault tolerant routing. Finally, the sender and receiver will use known algorithms for key exchange. In this research, location based key authentication and encryption is performed using ElGamal cryptography for transmitting data securely. In addition, the trace data are analyzed for intrusions in order to avoid DoS attacks. The proposed clustering algorithm which is the main focus of this study consists of three important phases namely, cluster formation, cluster head election and cluster reformation. The phases are explained using the algorithms given:

**Cluster formation phase**

**Step 1:** Choose all the nodes with high energy levels.

**Step 2:** Measure the distance of these nodes from the base station.

**Step 3:** Find the distance of neighbor nodes for these nodes.

**Step 4:** Form k clusters based on nearest neighbors for the K cluster heads which are elected using cluster head election algorithm.

**Step 5:** Check whether the energy and distance are optimal.

**Step 6:** If they are optimal construct the minimum spanning trees for routing.

**Step 7:** Find the cluster sub head using energy and distance.

**Step 8:** Repeat this procedure periodically at regular interval.

**Cluster head election process**

**Step 1:** Find the neighbors of each node n.

**Step 2:** Compute the energy e and distance d of nodes.

**Step 3:** For every node, compute the sum of the distances s with all its neighbors.

**Step 4:** Select the node with maximum energy and minimum total distance as the cluster head.

**Step 5:** Find the next node with second highest maximum energy and total distance. Assign this node as cluster sub head.

**Step 6:** Repeat steps 1-5 for all clusters.

**Cluster reformation process**

**Step 1:** Perform cluster formation algorithm on demand or periodically.

**Step 2:** Compute the new energies and new distance d of nodes after time t.

**Step 3:** Check whether former cluster head energy satisfies the minimum requirements for transmission.

**Step 4:** If the previous cluster head is below threshold, select the node with maximum energy and minimum total distance as the cluster head.

**Step 5:** Find the next node with second highest maximum energy and total distance. Assign this node as cluster sub head.

**Step 6:** Repeat steps 1-5 for all clusters.

**Fault tolerance manager:** This algorithm is proposed to handling link and node failures during the transmission of packet from the source to the destination. The sensor nodes are self energized and low computational power. The failure of the network may occur either internally due to low battery, transmission loss, malfunction of the node or externally due to attacker or environment conditions. When there is a failure, the packets loss is enormous this cause complete drain of battery energy of the nodes during transmission. Even thought the MST can call for cluster but this algorithm is not aware of error condition. In order, to overcome this issue, researchers have proposed a supporting module for the clustering algorithm as a fault manager algorithm. This algorithm not only addresses the error condition in the network but also critical battery issues. The critical battery is a status of the node during which the node itself release from the participation by announcing it status, so that nodes will stop sending packets. All these conditions are addressed with handle with alternate mechanism are explained in the algorithm:

- Algorithm: Fault tolerance management algorithms (fault condition during routing)
- Input: Data for transmission
- Output: Error report of failure condition
- Assumption: Routing path is available for the entire participating node in the data transmission. At any particular time if there is a drop in the packet

**Step 1:** Packet are transmitted form sensor node to the sink node.

**Step 2:** If the next hop node is failed, go to 5 else.

**Step 3:** Remaining energy of the node is less than critical battery (check with threshold $Th_3$), go to 7 else.

**Step 4:** Route to the destination node is not available. Go to step 9 else go to 11.

**Step 5:** Generate link failure message and inform the source node.

**Step 6:** Select the back up route and send the packet. Then go to 3.

**Step 7:** Generate critical energy message and broadcast to all the node in the cluster.

**Step 8:** Neighbor nodes and cluster head remove the node information from the routing table.

**Step 9:** Send a message as the route or link failure to all node along the path.

**Step 10:** Update the route metrics as more the K-hop (K+1).

**Step 11:** Forward the packets to next hop to the destination.

**Intrusion detection module:** In sensor network, DoS attack is one of the most important that need to be addressed. This attack may be done by attacker either internally or externally. The internal attacker are the node within the network will send unwanted packets due to their mal function and external attacker are the attacker which are deliberately floods the packet to make the network stale. Both attackers need to be identified and blocked from unwanted handshake with the legitimate nodes otherwise the DoS attack will be multiplicative and send enormous packet may collapse the entire network. This can be done with following algorithm which is not only filter the DoS packet but also improve the overall network performance.

**Attribute selection algorithm**
**Steps of the algorithm:**

- Compute the information gain ratio for each attribute $A_i$€D
- Choose an attribute $A_i$ from D with the maximum information gain value
- Split the training data D into K sub-data sets using the K-means clustering algorithm to get {$D_1$, $D_2$,.. $D_k$} depending on the attribute values of $A_i$
- Calculate the prior and conditional probabilities P ($C_j$) and P ($A_{ij}$ | $C_j$) for each sub-dataset $D_i$
- Classify the examples of each sub-dataset $D_i$ using EMSVM
- If any example of sub-dataset $D_i$ is misclassified then calculate the information gain ratio of corresponding attributes. Sub data set also classified into sub-sub data set. Compute the prior and EMSVM for each attributes. Classify the sub/sub-sub data set examples of their prior and EMSVM. Continue this process until all the examples of sub | sub-sub-datasets are correctly classified
- Preserve all the prior conditional probabilities for each sub-dataset $D_i$ or sub-sub-dataset $D_{ij}$ for future classification of unseen examples

## RESULTS AND DISCUSSION

This research has been implemented using NS2 simulator. On implementing this algorithm the results obtained have been analyzed and are compared with AODV as given. Table 1 shows the comparison of energy consumption between AODV and the proposed cluster based routing algorithm. From this Table 1, it can be observed that the energy consumption is reduced by 10% in the proposed algorithm when it is compared with the existing AODV algorithm. Figure 2 and 3 show the performance analysis between AODV and the cluster based routing protocol. From these figures, it can be observed that the performance is improved considerably in the cluster based routing protocol proposed in this research when it is compared with AODV.

Table 1: Comparison of energy consumption

| No. of nodes | No. of clusters | Energy consumed with AODV (%) | Energy consumed in proposed algorithm (%) |
|---|---|---|---|
| 100 | 5 | 60.00 | 48.70 |
| 200 | 10 | 62.00 | 49.20 |
| 300 | 15 | 61.70 | 50.30 |
| 400 | 20 | 63.20 | 47.10 |
| 500 | 25 | 64.12 | 48.25 |
| 600 | 30 | 65.00 | 53.40 |
| 700 | 35 | 62.11 | 51.20 |
| 800 | 40 | 64.00 | 52.30 |
| 900 | 45 | 61.50 | 51.56 |

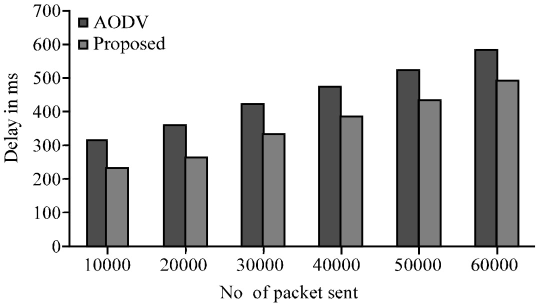

Fig. 2: Performance analysis of packet transmission

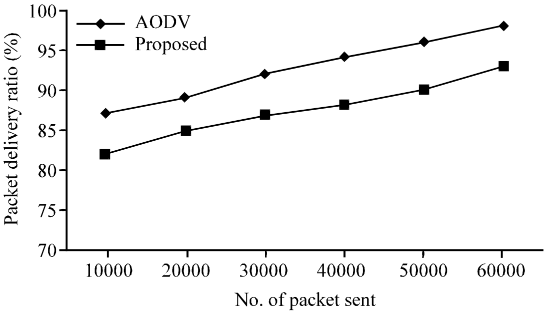

Fig. 3: Throughput analysis

## CONCLUSION

In this research, a cluster based fault tolerant routing protocol has been proposed. The main focus of this study is the design and implementation of a new cluster based routing protocol by modifying the existing AODV algorithm. The metrics used for clustering in this research are energy and distance between nodes. From the experiments carried out on clustering, it has been observed that the QoS metrics such as packet delivery ratio, end to end delay and energy consumption are improved using clustering. Further researchs in this direction could be the use of intelligent agents for improving the clustering efficiency.

## REFERENCES

Chansu, Y., K.G. Shin and B. Lee, 2004. Power stepped protocol: Enhancing spatial utilization in a clustered WSNs. IEEE, J. Areas Commun., 22: 1322-1334.

Chao, H.L. and C.L. Chang, 2008. A fault-tolerant routing protocol in wireless sensor networks. Int. J. Sen. Networks, 3: 66-73.

Heo, J., J.M. Hong, and Y. Cho, 2009. EARQ: Energy aware routing for real-time and reliable communication in wireless industrial sensor networks. IEEE, Trans. Ind. Inf., 5: 3-11.

Kim, J., K.Y. Jang, H. Choo and W. Kime, 2007. Energy efficient LEACH with TCP for wireless sensor networks. Comput. Sci. Appl., 4706: 275-285.

Liu, H. and L. Yu, 2005. Toward integrating feature selection algorithms for classification and clustering. IEEE Trans. Knowl. Data Eng., 17: 491-502.

Mengjie, Y.u., H.A. Mohktar and M. Merabti, 2007. Fault management in WSN. IEEE, Wireless Commun., 14: 13-19.

Mulay, S.A., P.R. Devale, G.V. Garje, 2010. Intrusion detection system using support vector machine and decision tree. Int. J. Comput. Appl., 3: 0975-8887.

Tang, S. and B. Zhang, 2004. A robust aodv protocol with local update. Proceedings of the 10th Asia Pacific Conference on Communications, August 29, September 1, 2004, pp: 418-422.

Tavallaee, M., N. Stakhanova and A.A. Ghorbani, 2010. Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE, Syst., Man Cybern. Soc., 40: 516-524.

Younis, O. and S. Fahmy, 2004. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mobile Comput., 3: 366-379.