ISSN:0975-9646

Improving QoS in Spontaneous Ad hoc Neworks

Gayathri Pradeep[1], Anna Prathiba Shobak[2]

Student[1], Assistant Professor[2]

Department of Computer Science and Engineering

Mangalam College of Engineering

Ettumanoor, Kerala, India

Abstract— **Now a days the use of mobile devices and wireless networks are increasing day by day, the wireless ad hoc network has now become one of the field of active research. A spontaneous ad hoc network is a network that consist of number of mobile terminals which are in a short range and communicate each other for sharing services, resources etc. Quality of service (QoS) refers to the level of quality of service. In the proposed system a node can join a network and use the services of other nodes in the network. There may be many nodes that provide the same service. To get a quality service the nodes which need service seek guidance from other nodes that have used service from a particular node. Based on the information provided a trust value is calculated for each node. Based on the trust values the node decides from which node service should be taken.**

Keywords— **Spontaneous ad hoc networks, QoS, Trust value.**

I. INTRODUCTION

A spontaneous ad hoc network[1] is a network that consist of number of mobile terminals which are in a short range and communicate each other for sharing services, resources etc. In an ad hoc network there is no fixed infrastructure. These types of networks usually have independent centralized administration. There is both wired and wireless spontaneous network. Here wireless spontaneous network is considered. Spontaneous ad hoc networks require well defined, effective security mechanisms. Tasks to be performed in this type of network include: Identification of User, their authorization, Address to be assigned, service name, safety and operation.

Because of the self-creating, self-organising and self-administering capabilities, ad hoc networks can be rapidly deployed with minimum user intervention. There is no need for detailed planning of base station installation or wiring. Also, ad hoc networks do not need to operate in a stand-alone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users.

Clustering is one of the solutions for communication in sensor networks due to its inherent energy saving qualities and its suitability for highly scalable networks. Clustering helps in data aggregation. It is an efficient technique where nodes forwards to a cluster head for processing and fusion before transmitting to base station. Clustering is effective in multicast and broadcast communication.

In the proposed system first a spontaneous ad hoc network is created. After that nodes are clustered and a cluster head is assigned for each cluster. When a node in a cluster need a service there may be many nodes in the same cluster that provide similar service. To get a quality service the nodes which need service seek guidance from other nodes that have used the same service from a particular node. Based on the information provided a trust value is calculated. Based on the trust values the node decides from which node service should be taken. Thus the best quality service will be acquired.

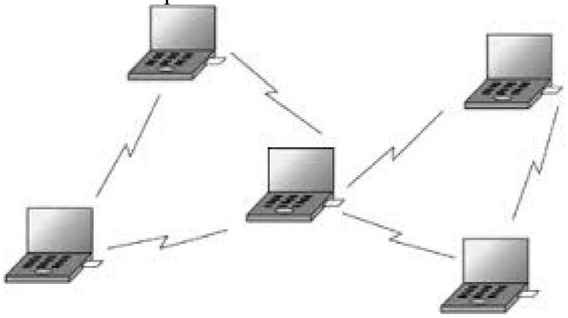

Fig.1 Example of a Spontaneous ad hoc network

II. RELATED WORKS

A. Network creation

In [2], the design of a protocol is shown that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. A user-friendly application has been used that has minimal interaction with the user. A user without advanced technical knowledge can set up and participate in a spontaneous network. The security schemes included in the protocol allow secure communication between end users.

B. Clustering and cluster head selection

Clustering provides one of the best solutions for communication in sensor networks due to its inherent energy saving qualities and its suitability for highly scalable networks. Clustering naturally facilitates data aggregation, an energy efficient technique where nodes forwards to a cluster head for processing and fusion before transmitting to base station. Clustering can be extremely effective in multicast, or broadcast communication.

In [3], a framework is presented for distributed trust in wireless sensor networks, a trust model with a novel quantitative measure of trust and, a mechanism that elects trustworthy cluster heads.

III. PROPOSED SYSTEM

First a spontaneous ad hoc network is created. After that nodes are clustered and a cluster head is assigned for each cluster. When a node in a cluster need a service there may be many nodes that provide similar service. To get a quality service the nodes which need service seek guidance from other nodes that have used the same service from a particular node. Based on the information provided a trust value is calculated. Based on the trust values the node decides from which node service should be taken. Thus the best quality service will be acquired.

A. *Network Creation*

The protocol helps to create secure spontaneous network which will be in decentralize and distributed in nature with use of different devices .Cooperation between the devices allows for group service, communication, security. Spontaneous network will be created in following way:

1) Node joining

The joining procedure depends on the IDC i.e. Identity card which is owned by every node. The IDC contain public and private component. Public component is nothing but the unique name, photograph, public key, creation, and expiration time, IP. In private component contain private key which will be used for issuing certificate to valid user. When any node, suppose B wants to join an existing network, it must choose the node which is in communication range to validate itself (e.g. Node A) A will send its public key. Then, B will send its IDC signed by A's public key. Next, A validates the received data and verifies the hash of the message in order to check that the data has not been modified. In this step, A establishes the trust level of B by looking physically at B (they are physically close), depending on whether A knows B or not.
Finally, A will send its IDC data to B (it may do so even if it decides not to trust B). This data will be signed by B's public key (which has been received on B's IDC) [4]. B will validate A's IDC and will establish the trust and validity in A only by integrity verification and authentication. If A does not reply to the joining request, B must select another network node (if one exists). After the authentication, B can access services, data and other nodes certificates by a route involving other nodes in network. Once the node is validated then session key which is randomly created by first node of network is then distributed to all nodes of network.

2) Service Accessing

In the proposed system the service used is file transmission. The nodes in the network are clustered based on the location. For each cluster a cluster head is selected. In a cluster there may be many nodes that provide similar service. When a node needs to access the service it needs to know from which node the service must be used. So the node first seeks advice from other nodes that have used the same service. They provide information such as delay, transmission rate etc. Based on these information trust value will be calculated for those nodes. Based on these trust values the nodes that need service decide from which node the service must be accessed [5].

B. *Cluster Head Selection*

The self-election is allowed for the first sets of cluster-heads(CH).When the current cluster head's battery power level falls below a predetermined threshold or serve for a predetermined period of time, it broadcasts (within the cluster) a new election message. All the nodes then vote for a new cluster head by using secret ballot. This is done by replying to the new election message with its choice of candidate. The reply, or vote, is encrypted with the pair wise key with the cluster head. Neighbours therefore have no idea of the political affiliation of each other since the key is private and, different for each node–cluster head pair. The cluster head then tallies the votes and decides the winner based on simple majority.

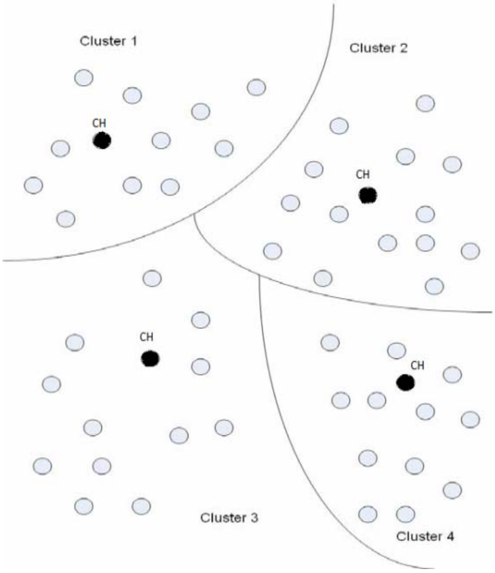

Fig. 2 Clustering and cluster heads

C. *Service History Management*

When a node providing service in a cluster move to another cluster, the nodes in the new cluster does not know the information about the migrated node. The CH of new cluster asks the old CH to provide information about the migrated node. The old CH collects information from other nodes about migrated node and gives it to the new CH.

IV. EXPERIMENTAL RESULTS

The environment consist of many devices that move randomly and communicate with neighbouring devices in the network.

Fig. 3 is a graph showing the hit ratio. The hit ratio shows the percentage which the nodes can access the quality service available. Here the proposed scheme is compared with existing scheme. Here the graph shows that proposed system has more hit ratio than existing system.

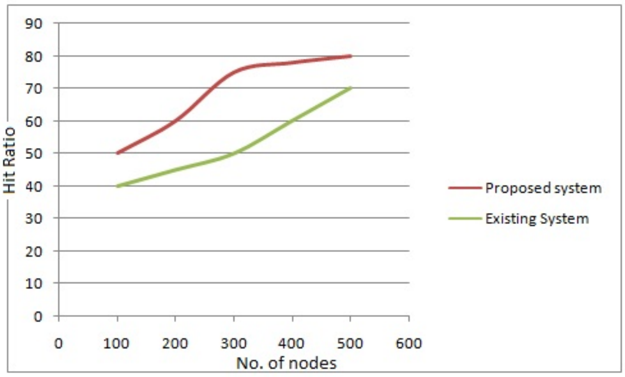

Fig. 3 Graph showing the Hit Ratio (comparison between Proposed Scheme and Existing Scheme).

Fig 4 is a graph showing the overhead versus number of nodes. The proposed system and existing system are compared here. The graph shows that proposed system has less overhead compared to the existing system.

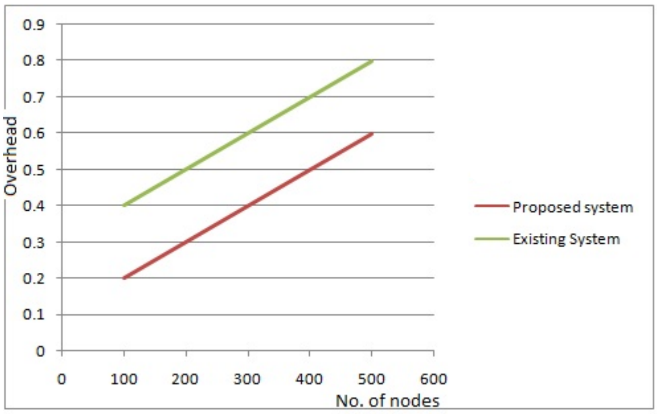

Fig. 4 Graph showing the Overhead (comparison between Proposed Scheme and Existing Scheme).

V. Conclusions

The paper creates a spontaneous ad hoc network and allows the nodes in the network to use the available services in the network. The nodes in the network are clustered and each cluster has cluster heads. When a node need to access a service there may be many nodes that provides same service in the cluster. Here we use method to find the best available service using trust value. When a node providing service move to another cluster service history management is used to provide information about the migrated node. Thus the proposed system helps to access best available service in the network.

Acknowledgment

We take this opportunity to thank all people who helped us for the study and preparation of this paper.

References

[1] L.M. FEENEY, B. AHLGREN, AND A. WESTERLUND, "SPONTANEOUS NETWORKING: AN APPLICATION-ORIENTED APPROACH TO AD-HOC NETWORKING," IEEE COMM. MAGAZINE, VOL. 39, NO. 6, PP. 176-181, JUNE 2001.

[2] Raquel Lacuesta, Jaime Llore t, Senior Member, IEEE,Miguel Garcia, Student Member, IEEE, and Lourdes Penalver "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 4, APRIL 2013.

[3] Garth V. Crosby, Niki Pissinou, James Gadze A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks " IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 4, APRIL 2013.

[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.

[5] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing, pp. 254-265, 2005.