CHAPTER 2

LITERATURE SURVEY

Ad hoc networks are the category of wireless networks that operate without the need for fixed infrastructure. They rely on multi-hop radio communication among its nodes for data transfer. The lack of fixed infrastructure complicates the process of routing within an ad hoc network. The nodes in the network participate in the data or control message routing process by forwarding them to other nodes. The decision on how to forward the information or to whom to forward them dynamically is taken based on the network connectivity as studied in Chai Keong Toh (2002); Siva Ram Murthy & Manoj (2004).

The wireless ad hoc networks were made prominent after the initiative made by Defense Advanced Research Projects Agency (DARPA) during the 1970s. They were named as ‘packet radio’ networks, as explained by Kahn et al. (1978) and were solely used for defense purposes. Being decentralized in its nature, wireless networks slowly penetrated into varied applications wherein centralized control was not possible. They became a better choice in improving the scalability of the network in comparison with wireless managed networks. These networks also find its use in emergency situations such as natural disasters or military conflicts that require minimal configuration and quick deployment. Wireless ad-hoc networks are classified in terms of their application as follows:

Mobile ad hoc networks (MANETs) comprise of mobile devices that are continuously self-configuring, infrastructure-less and wireless.
1. Vehicular Ad hoc Networks (VANETs) are networks used for communication among vehicles and vehicle-related equipment. They are also integrated with artificial intelligence to help vehicles behave intelligently during vehicle-to-vehicle collisions, accidents, etc. Such specialized networks are called intelligent vehicular ad hoc networks (InVANETs).

2. Smart Phone Ad hoc Networks (SPANs) are prominent replacements to Bluetooth and Wi-Fi. This type of network is commercially available and is used to create peer-to-peer networks without the need for cellular carrier networks, wireless access points, or traditional network infrastructure.

3. Internet-based mobile ad hoc networks (iMANETs) are a type of ad hoc networks that are capable of associating nodes that are mobile with fixed Internet-gateway nodes.

4. Military or Tactical MANETs are used by military applications giving priority to security, a range of operation, and integration with existing war camp headquarters.

Ramanathan & Redi (2002) in their survey work present an overview of ad hoc networks, its challenges, and future directions. Ad hoc networks are one of the most vibrant and active field study in today’s scenario and has seen fast expansion and gained greater visibility due to the propagation of inexpensive, readily available wireless devices. The network community has also shifted its keen interest to mobile computing. Some of the open problems such as scalability, energy efficient routing, quality of service, security, integration with new hardware technologies such as RF energy, robots, sensors, embedded systems, etc. have been explained in detail.
Ad hoc networks have many issues and challenges. Some of the issues are handled by the concept of clustering. Evident research has been carried out in the area of clustered architecture for ad hoc networks. Some of the issues relevant to the proposed research work are studied in detail and listed.

2.1 OVERVIEW OF CLUSTERING IN AD HOC NETWORKS

Ad hoc networks are different from traditional networks due to their capability of connecting several nodes without a centralized access point. The mobile nodes are however energy-constrained and thus if all the nodes in the network involve themselves in the network services, they tend to lose their constrained resources collectively, as explained by Charles E Perkins (2001).

To overcome these issues, Lin & Gerla (1995) suggest the network to be divided into a set of clusters. Each cluster has nodes that are spaced at a distance of one or two hops. The clustering algorithm ensures that each node becomes a member of at least one cluster. The nodes belonging to a cluster elect a cluster head (leader node) to perform the network services.

Lin & Gerla (1997) also elaborate that the concept of clustering assists in resources being reused thereby increasing the capacity of the network. The transmission events are coordinated effectively with the help of a special node termed as the cluster head. The approach enables saving of resources that are used during retransmission due to the fact that transmission collisions are reduced.

Kozart et al. (2001) and Pearlman & Hass (1999) have observed that the set of cluster heads and cluster gateways establish themselves as a
virtual backbone for routing within the cluster. Thus, the spreading of routing information is restricted among the set of nodes in this cluster.

Since the entire ad hoc network is divided into clusters, McDonald & Znati (2001) illustrate that it makes the network appear smaller and more stable. The local changes happening in the cluster need not be seen and updated by the entire network. The information processed and stored by each mobile node is thus greatly reduced.

As surveyed by Yu & Chong (2005), the main purpose of cluster based architecture is to use the network resources efficiently, enhance availability, reduce overheads and provide scalable architecture. Clustered architecture does have its share of costs to contribute. The main costs incurred are the exchange of explicit control messages, ripple effect due to re-clustering, and stationary assumption during the cluster formation phase. However, in comparison to the existing and conventional routing protocols, topology updates in the clustering approach experience lower overhead and quicker merging of clusters. Each of the many schemes listed for clustering by the authors is well suited for specific situations. It cannot be assured that any one of the schemes is best suited for all situations.

Krishna et al. (1997) have suggested a cluster-based novel methodology for the maintenance of routing and topology information in dynamic ad hoc networks. The approach illustrates algorithms for the creation and maintenance of clusters in the incidence of dynamic network events. The network is specified as a graph and is divided into overlapping clusters. The approach is illustrated to incur less overhead in the case of topological changes. These frequent topological modifications in the network affect the routing of data and information, which is managed by the algorithm by providing rapid changes in routing.
Ramachandran et al. (2000) have focused their work on a communication model directly derived from the merging technology of pervasive computing, namely Bluetooth. The two algorithms suggested by the author’s aid in speeding the time taken by a node to discover and to connect to another node in its radio range namely, device discovery time. The suggested randomized and deterministic algorithms can be applied to address the issues in the distributed cluster formation in ad hoc networks. By simulation, the authors have illustrated that the algorithms are exceedingly suitable as an alternative for applications to Bluetooth scatternets.

Chan & Perrig (2004) present an algorithm that is capable of creating uniform clusters. It applies three rounds of feedback among the nodes wherein the self-organizing properties of the nodes are used to form efficient packing of the nodes in the cluster that is similar to hexagonal close-packing. The algorithm efficiently covers the entire network in its cluster formation and ensures less overlapping among the clusters. The salient features of this algorithm are its speed, considerably reduces packet loss and node failure and ensures well-organized communication among the members of the network. Knowledge on geographic location and distance or direction estimation among the nodes is further not required.

Er & Seah (2004) suggest the formation of clusters of varying diameter relative to the mobility patterns in an ad hoc network. The cluster diameter is not restricted as two-hops but determined based on the stability of the network and thus flexible and enhances the scalability of the network. The authors have proposed two metrics based on the relative mobility of the nodes namely, the variation of estimated distance between nodes over time and the estimated mean distance for a cluster, to measure the stability of a cluster. Nodes that are found to move in the same direction are grouped as a cluster.
The suggested approach is found to form a lesser number of clusters in comparison with Lowest-ID and MOBIC algorithms.

Chen et al. (2005) have given a detailed survey on several clustering algorithms, mainly concentrating on graph domination based algorithms. They have also shown through results that building clustered hierarchies are affordable. Further, they have studied that in order to enhance the network quality of service clustering algorithms can be used to build virtual backbones. Here, deterministic and probabilistic distributed algorithms have been discussed for cluster formation. It has been shown that the average communication costs suffered in building, maintaining, and utilizing such hierarchies are logarithmic in the measure. Furthermore, it has been shown that due to network clustering many other aspects of ad hoc networks, such as broadcasting of messages and quality-of-service, can also be benefitted.

Xue et al. (2006) have studied the control overhead that persists in clustering and routing algorithms that work on one-hop based clustering for mobile ad hoc networks. The authors have observed that if the control overhead is not managed correctly it is likely that it will lead to adverse effects on the network’s performance. Studies have shown that control overhead in clustered networks is mainly dependent on the network parameters such as node mobility, node transmission range, network size and network density. By managing these parameters it is evident that the control overhead can be minimized. The study has been done with the Lowest-ID algorithm as the basis.

Asterjadhi et al. (2010) have made their study on large cognitive radio networks. The authors suggest the inclusion of spectrum-aware neighbor discovery and clustering scheme that can be used along with a network coded cognitive control channel in order to allow the cognitive radio devices to effectively access the spectrum that is normally not in use. Evaluation of this
algorithm has been done with reference to the two approaches namely, the lowest id algorithm (Lowest ID) and the distributed clustering algorithm (ConID). Performance is shown to improve with the suggested approach based on metrics such as the number of clusters in the network, the average cluster size and the ratio of the average number of common free channels in a cluster to the total number of free channels.

2.2 OVERVIEW OF CLUSTER HEAD ELECTION ALGORITHMS

The presence of a cluster head is essential to any clustering application such as routing as explained by Basagni (1999) and key distribution as suggested by DeCleene et al. (2001); Bechler et al. (2004) and in the implementation of Intrusion Detection System (IDS) for the entire cluster have been studied by Anantvalee et al. (2006). All these methods ensure that one of the nodes is alive and operational actively and the rest of the nodes in the network can be in the energy-saving mode.

Although the concept of clustering in ad hoc networks has existed for many decades, the idea of enabling the cluster head to perform special functions was first recommended in the literature by Huang (2003). In an ad hoc network, the nodes have limited battery power making it inefficient to consider each node as a monitoring node at all times, especially when the threat level is low. An alternate approach, as suggested by the author is that of a set of neighboring nodes fairly elect a monitoring node, termed as the cluster head periodically. Thus, the responsibility of monitoring for intrusions is shared among nodes that get elected as cluster heads for the cluster. However, the election of a single cluster head that is given the overall responsibility to act as the monitoring node makes the system vulnerable to attack the Intrusion Detection System (IDS) itself.
The research work by Little et al. (2005) shows the selection of two cluster heads. The authors have suggested a Vehicular Ad hoc Network (VANET). It is assumed that the vehicles that travel on the same direction of the pathway to form an interconnected block. Those vehicles that are within the range and able to maintain connectivity for a minimum period of time are said to form a cluster. Each cluster comprises a header and a trailer, located at the front and rear of each cluster respectively. They are assigned with the task of maintaining communication with other neighboring clusters. The selection of only two nodes for communication limits congestion caused by all the nodes participating in data forwarding. The remaining nodes in the cluster that are not a header or trailer are treated as intermediate nodes. The intermediate nodes maintain a passive role in terms of receiving messages and acknowledgments from opposing nodes and sending them to the header or trailer. Thus the data forwarding task is managed by only two nodes in the network and thus increases the network lifetime.

A multi-head clustering algorithm for VANET has been suggested by Shou-Chih et al. (2013). In this paper, the authors suggest the vehicular environment as a cluster in a rectangular shape that captures a particular road region. Each region is further divided into sectors. Each region has a master cluster head which in turn elects slave cluster heads for each sector. The rest of the nodes become cluster members. These cluster heads serve as local file servers and enable surrounding nodes to upload and download shared data, mainly multimedia data.

An implementation of the computational complexity analysis of multicast models in distributed systems is elaborated by Elijah Blessing et al. (2002). The LeaSel model suggested by Elijah Blessing et al. (2003) is very difficult to attack as the model consists of two entities that manage and control the groups and subgroups, namely deputy controller and leader. The
former decides the rank of all the members in the subgroup and maintains a rank list. The member which ranks first is designated as the leader. The leader is authorized to perform key generation and distribution. As a continuation of this work, authors in Mary Vennila et al. (2006); Rhymend Uthariaraj et al. (2007) suggest a model based on this LeaSel multicast model, wherein concept of multiple leaders can be used for load sharing, increased robustness and added security.

Dang et al. (2011) have oriented their research on providing scalability to large, dense MANETs. One way of achieving this as suggested by the authors is to optimize the cluster head selection. The two variants for cluster head selection namely distance in which the members are located from its respective nearest cluster head and the cluster size have been examined to be NP-Hard. Hence the authors have suggested two distributed selection algorithms that are equipped with logarithmic approximation ratio for the variants. Simulations have been carried out to analyze the performance of the resulting cluster size distribution and cluster head density, which are directly responsible for the operation of the network proficiently.

The authors of Ye et al. (2006) have focused their work on improving the data gathering capabilities of nodes in sensor networks. The nodes that possess more residual energy are selected as cluster heads. The election procedure is made autonomous as it is not possible to have centralized control in sensor networks. Control overhead is minimized through localized communication. Simulation results show that the suggested algorithm extends the lifetime of the network appreciably in comparison with clustering protocols such as LEACH and HEED.

The approaches surveyed on electing multiple cluster heads keep all the elected cluster heads active always. Although they share the overhead of the cluster head or leader, they also contribute to the overhead in maintaining
the multiple cluster heads or leaders simultaneously. New sets of cluster heads / leaders are to be elected when the existing sets either get compromised or lose their energy levels essential for the operation of the network services.

The backbone formation procedure suggested by Dagdeviren & Erciyes (2006) is a useful suggestion to alleviate routing and resource management in ad hoc networks. The suggested approach constructs a directed ring of the cluster heads in a clustered network. The algorithm has been analyzed for parameters such as running time and round trip delay for their scalability. These parameters are mapped to mobility, surface area, the number of nodes and number of cluster heads. The approach is shown to create clusters that are balanced thereby reducing the routing delay to a minimum. In the proposed approach a similar backbone formation is suggested so as to enjoy the above mentioned advantages in a clustered network.

A list of evaluation methods for cluster election in ad hoc networks is presented below:

- **DS-based clustering** finds a weakly connected dominating set that reduces the number of nodes taking part in route search or routing table maintenance. Clusters are formed with one hop distance and the communication complexity is greater than $O(2|V|)$ where $|V|$ represents the number of mobile nodes in the network. This technique is found to be more feasible for networks that have low mobility as suggested by Wu & Li (1999), Das & Bharghavan (1997) and Das et al. (1997).

- **Low-maintenance clustering** provides a cluster infrastructure with minimum maintenance cost for cluster formation. Cluster members are one hop distance from the CH and the
communication complexity is between 0 to $O(m|V|)$, where $m$ indicates the average cluster degree of a mobile node and this has relation with the overlap of clusters as studied by Chiang et al. (1997), Ephremides et al. (1987) and Gerla & Tsai (1995).

- **Mobility-aware clustering** utilizes the mobility behavior of the nodes for cluster construction and maintenance. Nodes with low relative speed are assigned to the same cluster and this tightens the connections between nodes in the cluster. The schemes of this type are more suited for scenarios consisting of mobile nodes which move around in groups for a long duration of time. They also work well in a dynamic environment where mobile nodes are continuously in motion as suggested by Basu et al. (2001) and McDonald & Znati (2001).

- **Energy-efficient clustering** avoids unnecessary consumption of energy for mobile nodes thereby prolonging the lifetime of mobile nodes and that of the network. The schemes either balance the leader node’s serving time between all mobile nodes or tries to reduce the size of a cluster thereby avoiding unwanted consumption of energy by the mobile nodes serving as dominating nodes without affecting its performance as studied by Amis & Prakash (2000), Wu et al. (2002) and Ryu & Cho (2001).

- **Load-balancing clustering** forms uniform size of clusters and distribute the capacity of a network more equally among the clusters. These schemes assign upper and lower limits for the number of nodes that a cluster can handle efficiently. When the size of the cluster exceeds the predefined limit, re-clustering
procedures are invoked to adjust the number of member nodes in that cluster as presented by Amis & (2000); Ohta & Kakuda (2003).

- **Combined-metrics-based clustering** considers multiple metrics such as node degree, mobility, battery energy, cluster size, etc. for its weight computation. The inclusion or exclusion of certain metrics during the computation can be adjusted for different application scenarios. The advantage of this scheme is due to the nature of it being able to flexibly adjust the weighting factors for each metric and also pertaining to different scenarios. The disadvantage of the scheme is that not all of the parameters may always be available and also with accuracy. This inaccuracy in the obtained information affects the performance of the clustering scheme. The weighted clustering algorithm is presented by Chatterjee et al. (2000; 2002).

Turgut et al. (2003) have suggested the procedure for optimizing the performance of weighted clustering algorithm (WCA) with the aid of simulated annealing, which is a powerful stochastic search method that is useful in the combinatorial optimization problems. The suggested algorithm takes its input consisting of a dominant set of cluster heads and its members from the output of WCA. This input is used by the simulated annealing technique to find the best solution. This is done by calculating the best fitness values and the objective function. Thus each cluster head assigns for itself only the optimal number of members to enable efficient functioning of the MAC protocol. The procedure automatically produces a lesser number of clusters and also lesser number of cluster heads resulting in improved performance in comparison with WCA.
Zouhair et al. (2006) have also oriented their work on improvising the performance of WCA by computing the weighting factors rather than randomly assigning the same. This provides flexibility in assigning the weights to the decision parameters by dynamically computing them based on the network scenario during that time period. The performance is compared with WCA and shows improvement in comparison with the metrics namely, the number of clusters formed, number of re-affiliations, the number of states transitions on each cluster head and the number of cluster heads changes.

Hong & Wu (2011) have worked on improving the performance of WCA by incorporating the specific constraints of sensor networks in the weight computation. The approach is shown to improve the lifetime of the network in comparison with WCA.

Exhaustive studies have shown that the concept of clustering can be implemented in wireless sensor networks (WSNs) also, thereby increasing the lifetime of the network. The cluster head takes up the task of collecting information from the member nodes, aggregating the collected data and sending them to the destination node. Thus it is essential that the most appropriate node gets selected as the cluster head. Puneet & Vidushi (2013) have presented a cluster head selection method that uses fuzzy logic. The fuzzy approach also applies multiple attribute decision-making (MADM) methodologies using residual energy, number of neighbors, and the distance from the base station of the nodes as criteria for cluster head selection. Simulations show the proficiency of this approach in comparison with the distributed hierarchical agglomerative clustering (DHAC) protocol when put to use in homogeneous environments.

Mustafa et al. (2013) suggest an enhancement over the approach given by Puneet & Vidushi (2013) by including an additional parameter for the cluster head election namely, an average distance between a node and its
neighbors. Here the fuzzy logic is used for the decision-making role and Technique for Preference by Similarity to Ideal Solution (TOPSIS) method is suggested for cluster head selection of the best suited nodes. Further, instead of the traditional single-hop communication, the authors have suggested multi-hop communication for communicating among the members of a cluster and among the cluster heads of different clusters. Simulation results have shown that the technique performs well in terms of parameters such as energy efficiency, network’s life time, less cluster head deformation and control overhead.

Aissa et al. (2013) have suggested an analytical model to decrease the number of clusters. It is also shown that the algorithm maintains the network more stable and performs better during cluster formation phase in comparison with WCA. However, the problem due to missing values for the parameters used in weight computation is not addressed in these approaches that use combined-metrics for cluster head election.

The Analytical Hierarchy Process (AHP) method has been illustrated as a useful decision-making tool as explored by Mansoor (2013) and Heng & Chen (2014). The process is used exhaustively in decision making situations specially that involve group dynamics. Rather than randomly assigning a right decision, the method aids the user to find the best suited solution. The basic procedure for using AHP has been suggested by (Saaty 1990).

Han Xuli (1997) has studied the priority computation of comparison matrix. He suggests changing the comparison matrix into a weighted matrix. The theoretical basis for taking the eigenvector of weight matrix as priority vector is also discussed in the paper. The computational method for the priority vector of weight matrix and its effectiveness are
illustrated. The author suggests this eigen value method on weight matrix for the AHP process.

Hui Xia et al. (2011) have incorporated trust concept in MANET and have built a subjective trust management model that uses multiple parameters for decision making. The approach uses the fuzzy method and AHP to cater to threats from malicious nodes in the network. The authors consider multiple decision factors, that include trust computed directly by the node, or trust recommended by other nodes, incentives assigned, etc. in their model to reflect the complexity and uncertainty of trust relationships. The shortage of decision factors that are incomplete is overcome here. In comparison with the existing trust management models, the exhaustive simulations conducted show the efficiency of the suggested model in the improvement of the quality of interaction in the network, flexibility in making a choice about nodes, identification of malicious nodes, resisting attacks and improving the security of the system.

tEval is a free downloadable tool for comparing the decisions taken. It works using the Analytical Hierarchy Process in a bottom-up approach. It aids in the evaluation of decisions when the core decision is dependent on multiple choices. The AHP method is further improvised by including normalization whereby rank reversal is eliminated. An improved metric is present to measure inconsistency for a set of pair-wise comparisons. This metric improves the Consistency Ratio, which performs poorly under reasonable models of imprecise judgment. tEval has been developed and tested for many applications related to AHP concept by Jeremy Chen (2012).

Vasudevan et al. (2004) have implemented an algorithm for leader election in mobile ad hoc networks that is adaptive to dynamic topological modifications in the network. Unlike the scenario where the leader election occurs periodically, the suggested approach invokes the algorithm only on the
departure of the leader or when considerable topological changes occur in the network and is based on diffusing computations.

The vote-based clustering (VC) algorithm suggested by Li et al. (2004) uses the location of nodes, their identifier information and battery life of the nodes for electing the leader node. Here, each mobile host maintains a count of the Hello messages received from the neighbouring nodes. Each node also considers its own residual battery life and computes its vote as the weighted sum of the normalized number of valid neighbors and its normalized residual battery life. The cluster head is the node with the highest vote when compared with its neighbors. Periodically the number of dominating mobile nodes is checked for a threshold value. If it has reached the threshold value, no other nodes are permitted to join the present cluster. The detailed analysis through simulations shows that the suggested method improves the cluster structure when compared with Lowest ID (LID) algorithm and Highest Degree (HD) algorithm.

Mehdi Maleknasab et al. (2013), present a detailed survey on several trust based clustering algorithms. The properties and features of the algorithms have been analyzed elaborately. Their main focus is on algorithms that apply trust based mechanisms both for the cluster formation and cluster maintenance processes. The authors have compared the techniques relating to direct and indirect trust computations. The authors further point out the fact that in spite of having several secure clustering schemes for mobile ad hoc networks, there are not sufficient clustering schemes that can operate in trusted as well as hostile environments. The authors predict that if the suggested algorithms are applied to trusted environments they are likely to reduce overheads and when applied to hostile conditions they are likely to enable high security.
2.3 ISSUES RELATED TO MISBEHAVING NODES IN THE NETWORK

The open nature of ad hoc networks exposes it to innumerable security threats. There are basically two types of threats namely due to selfish nodes that do not take part in the network services in order to conserve its resources and malicious nodes that have penetrated into the network with the aim of disrupting the network services. Considerable work on such threats helps in understanding the behavior of such misbehaving nodes. Anantvalee & Wu (2006) present a comprehensive survey on IDS architectures that have been introduced for MANET. Several techniques such as Pathrater / Watchdog by Marti et al. (2000), CONFIDANT by Buchegger & Boudec (2002), CORE by Michiardi & Molva (2002), OCEAN by Bansal & Baker (2003) and cooperative IDS have been compared for their efficiency in detecting misbehaving nodes in MANET.

In ad hoc networks, to overcome misbehavior related issues, trust management is suggested in the literature by Koltsidas & Pavlidou (2011); Feng et al. (2014). Common trust evaluation strategies neglect the selfishness of normal nodes and conclude that malicious nodes are non-cooperative. To induce cooperation among the nodes, incentive assigning mechanisms are suggested. Incentives provided to the cooperating nodes is in the form of virtual currency called NUGGETS as presented by Buttyan & Hubaux (2001) or as premium paid to the forwarding intermediate nodes by a central bank like entity as presented by Zhong et al. (2003).

The authors Jin et al. (2005) have suggested a trust evaluation scheme for ad hoc networks to cater to nodes that are unfamiliar and for reducing the available scare memory space in each node. The nodes in a group say cluster, select their leader. This leader issues certificates to its members based on their trust values. The trust value is calculated using the
metrics communication data rate and data delivery rate of each member node. Whenever a node needs to join another cluster it is mandatory for it to show its trust certificate thereby securing the routing process.

Govindan & Mohapatra (2012) have focused their detailed survey on the varied approaches employed for trust computations in mobile ad hoc networks. The authors aim at providing the multiple facets of trust computation, the properties in trust computation that are useful to be developed as a metric and the methodology of trust computation itself. Additionally, the authors also analyze important dynamics in the network related to trust such as trust propagation, prediction and aggregation algorithms, the influence of network dynamics on trust dynamics and the impact of trust on security services. The analysis has been done for varied applications as it is a universal truth that no single technique can cater to the entire problem domain. The authors have identified the following as future research areas namely, the impact of the network dynamics on trust, impact of heterogeneous nodes on trust, the role of trust in cooperative and non-cooperative games and issues due to context-dependent trust.

Velloso et al. (2010) suggest a solution for an uncompromising cluster head, thereby protecting the monitoring task it is assigned with, by utilizing the node’s trust value. The authors suggest a trust model that helps the nodes evaluate the trust of its neighboring nodes. The nodes in the network compute the trust level for its neighbors based on past history and the judgment from their neighboring nodes. The behavior of the neighboring whether good or bad is kept track of. The neighboring nodes thus share their own opinions truthfully thereby improving their trust level evaluation. This sharing of opinion is defined as the recommendation. The recommendation is used as criteria for cluster head election. But if the nodes decide to lie about
their opinions, the calculation of trust will not be accurate causing selfish nodes to thrive at large.

Feng et al. (2014) have suggested a technique of assigning incentives based on game theoretical concepts to enforce cooperation among the network nodes. The approach models the interactions among the malicious and normal nodes as a Bayesian game. The nodes in the network are considered as players in the Bayesian game and thus a set of parameters that include the action sets of the nodes and their payoff matrix are formulated and analyzed. The equilibrium of the game enables in showing the dynamics of the node in taking part in the game with respective to its actions and the payoff it aims at to make maximum profit for itself. It is evident from simulations that the suggested incentive mechanism effectively motivates normal nodes to be unselfish and cooperate among themselves and as far as possible compels malicious nodes also to cooperate.

Jin-Hee Cho (2011) gives a detailed survey on the cluster-based trust evaluation schemes. The survey enlightens researchers with multiple perspective views to aid in the design of trust-based protocols, a comprehensive study on the trust metrics that can be considered and the ways in which the trust metrics can be customized to meet the needs of the application. The survey has also considered the algorithms employed in social networks and also those used in trivial military applications.

There are several methods available for hybrid trust computation can be implemented. The approach suggested by (Josang 1998;2001;2006) uses the belief ($b$), disbelief ($d$) and uncertainty ($u$) understood by one node over the other. The approach works on the basis of subjective logic which is a type of probabilistic logic that explicitly takes uncertainty and belief into account. The suggested subjective logic is suitable for modeling and analyzing situations involving uncertainty and incomplete knowledge such as
modeling trust networks and for analyzing Bayesian networks. According to the definition of subject logic is, “if x is a proposition, the binomial opinion about the truth of x is the ordered quadruple $w_x = (b, d, u, \alpha)$ where b (belief) is the belief that the specified proposition is true; d (disbelief) is the belief that the specified proposition is false; u (uncertainty) is the amount of uncommitted belief; \alpha (base rate) is the a priori probability in the absence of evidence” (Josang 1998; 2001; 2006). The advantage of this approach is that the uncertainty component in the quadruple is evaluated at every step of the analysis and is made explicit in the end result. The distinction between the certain and uncertainties are thus identifiable.

Game theory has been in use in the fields of economics and biology for many years, but recently it has been put to use to improvise the routing and packet forwarding operations in wireless ad-hoc and sensor networks. There still exists the problem in nodes forming proper clusters by self-organizing themselves, due to the selfish behavior of nodes. Koltsidas & Pavlidou (2011) have suggested a game-theoretical approach for ad hoc and sensor networks to overcome the above mentioned problem. The fact that each sensor tends to act selfishly to conserve its power and increase its lifetime is obvious. This is modeled as a non-cooperative game approach and the authors prove that the Nash Equilibria of the game can be normally calculated for pure (among normal nodes) and mixed strategies (among both normal and misbehaving nodes). The payoffs and the price of anarchy corresponding to these equilibria are helpful is identifying the nature of the nodes. The simulation results are compared with popular clustering techniques and it is shown that the suggested mechanism achieves better performance.

Anderegg & Eidenbenz (2003) have come up with a game-theoretic approach to study the routing mechanism in a mobile ad hoc network that
contains misbehaving (selfish and misbehaving) nodes. The approach enables nodes to accept payments or incentives for the data forwarding operations in the network. Incentives are assigned to the nodes so as to make up for the costs individually suffered by each node during the process of data propagation. The suggested solution uses a modified Vickrey, Clarke, and Groves (VCG) mechanism and guarantees routing to be done in the most cost-effective path in the network.

The VCG mechanism belongs to the category of canonical mechanisms under game theory that can be useful to motivate the auction-goers in auctions and exchanges to orient towards honest bidding. The mechanism, however, does not guarantee revenue maximization or is capable of avoiding bidder collusion as shown by authors Vincent & Tuomas (2006). Thus when applied to the problem of addressing selfish nodes, it can be concluded that the VCG mechanism is useful to detect only a single misbehaving node. If more than one node forms a collusion to misbehave, the mechanism fails. The existing solutions that use VCG mechanism are equipped to be cost-effective and truthful only in cases of single communication nodes that are selfish. Experiments have shown that the mechanism works fine for long duration communication sessions between two nodes in an ad hoc network and the routing path is not being disrupted drastically during a transmission session. Moreover, as studied by Rothkopf (2007) and Dobzinski (2007), the VCG model suggested in the existing works is suitable only when the goal is cooperation among nodes. Goals such as assigning economic incentives for encouraging nodes to cooperate to provide its services are not addressed.

The Optimized Link State Routing protocol (OLSR) is a proactive routing protocol intended for ad hoc networks. Rather than involving all the nodes in data forwarding, special nodes called as Multi-Point Relay nodes
(MPRs) are used. The MPRs are also liable to act selfishly and thereby affect the lifetime of the network. Nadia et al. (2014) suggest a modification to OLSR, termed as QOLS R which includes QoS in terms of overcoming the issues due to selfish nodes in the data forwarding process. The authors recommend a reputation system that works using VCG mechanism to motivate nodes to honestly participate in the selection of MPRs. Further, it has been discovered that even after the selection/election process the MPRs could misbehave which might lead to a denial of service attack as the packets are dropped. To overcome this issue the authors have suggested a hierarchical cooperative watchdog detection model for the cluster-based QOLSR. This scheme enables the nodes to cooperate in a hierarchical manner to enable detect selfish nodes. Results reveal the supremacy of the cluster-based QoS-OLSR model as it is more reliable and efficient in the detection of selfish nodes.

Game theory as explained by Fudenberg & Tirole (1991 and Osborne (2004) is applicable in solving major problems of wireless networks. Major areas of application include cooperation enforcement among the nodes as suggested by Buttyan & Hubaux (2003); Crowcroft et al. (2003); Michiardi & Molva (2005); Srinivasan et al. (2003), routing protocols as studied by Jaramillo & Srikant (2007), Milan et al. (2006), Wang et al. (2006) and Zhong et al. (2005) and system design issues as presented by Li et al. (2008) and Mackenzie & DaSilva (2006). Most of the existing approaches consider the entities in the network which can also be termed as nodes, as selfish and rational. The nodes that are selfish are defined in terms of their utility functions and thus are alert to only their incentives. The nodes are always keen on choosing strategies to increase their incentives.

There are two branches of game theory namely, non-cooperative as shown by Basar & Olsder (1999) and cooperative game theory as explained
by Myerson (1991) and Owen (1995). The Non-cooperative game theory deals with the strategic choices as a result of the communications among competing players. Here, the choice of strategy by each entity is independent and is targeted to improve its own utility or reduce its losses. Cooperative game theory deals with the study of the behavior of cooperating entities. Further, the main sub-division of cooperative games is the occurrence of groups of entities that cooperate to increase the strength of the entity, which is termed as coalitions as presented by Myserson (1991) and Saad et al. (2009). The implementation of cooperation in large scale communication networks has several challenges in terms of adequate modeling, efficiency, complexity, and fairness. Coalitional games have been proven to be powerful for designing fair, robust, practical, and efficient cooperation strategies in communication networks. The network scenario is considered as a forwarding game due to the cooperation of all the nodes in the network.

The nodes in a network can form coalitions either to forward information (normal nodes) or act selfishly (misbehavior). The first type of scenario characterizes coalition games are termed to be in characteristic form. Here the value of the coalition $S$ does not dependent on how the coalition has been structured, but exclusively depends on the participants of the said coalition. These types of games are known as games with transferable utility (TU), as proposed by Von Neuman & Morgenstern (1944).

Saad et al. (2012) have investigated the use of game-theoretical solutions on the issues related to spectrum sensing and spectrum access in the network consisting of secondary users (SUs). If the network is modeled as a cooperative game, these users can be imagined to cooperate to improve their view of the spectrum (sensing), and also reduce the possibility of interference with each other, and thereby improve their transmission capacity during access. The problem has been exhibited as a coalitional game in partition
form and an algorithm for the same is suggested. Simulations show the performance improvement yielded by this algorithm when compared with similar results from non-cooperative modeled games. The results also show that the SUs tend to adapt itself to changes in the traffic or slow mobility.

Xiaoqi Li & Michael (2008), have suggested an improvised coalitional game model for security issues in wireless networks. To analyze the network performance and quantify the security in the network, throughput characteristic function has been identified as the metric. This function defines the maximum throughput and most reliable traffic that can be achieved by the coalition. The coalition is encouraged by assigning fair payoff using Shapley Value. Apart from this the authors also define a set of rules, termed as a threatening mechanism, to all nodes that do not take part in the coalition constructively. The procedure for the formation of coalitions and the way in which it can be integrated with the suggested model is elaborately dealt with. Theoretical analysis has been conducted to illustrate the convergence situation and justify the correctness of the formulation.

Noam & Amir (2007) and Mohammed N Otrok et al. (2011) suggest solutions to elect the trusted node as the leader node of a cluster in terms of VCG model to ensure truth-telling to be the dominant strategy for each node in the network. The VCG setup (Jaydip 2010) considers $n$ players and a set $A$ of alternatives (or outcomes). The player $i$ has a valuation function $v_i$, and $v$ represents the vector of valuation functions or the players under consideration. The payment due to a player for performing well is expressed by $p_i(v)$ and the allocation under valuation $v$ is expressed by $f(v)$.

One of the profound solution concepts for coalition games is the Shapley value as presented by Myserson (1991). It has been designed to associate with every coalitional game a unique payoff vector known as the value of the game, which is quite different from the value of a coalition as in
the case of other solutions such as the core. In situations where the contributions are unequal, the Shapley value as proposed by Lloyd S Shapley (1953) can be applied. It ensures that each entity gains as much or more as they would have from acting independently. In the studied network scenario, the approach interprets coalitions of misbehaving nodes as appearing with the same probability.

Further, Shapley value mechanism is a class of budget balanced strategyproof mechanism suggested by Moulin & Shenker (2001). It gives the designer fair amount of flexibility by means of an asymmetric cost sharing formula. The formula typically ranks the nodes randomly but in a fixed fashion. It charges the stand alone cost to the first ranked node requesting service and an incremental cost to the second ranked node requesting service, and so on. However, the technique is indifferent to joint misreports due to coalitions which could be of any size. Authors have compared the use of Shapley value with that of marginal cost computations and proved that the former mechanism is definitely budget balanced and possess the minimax property – minimizing the maximal welfare loss. The Shapley value, thus distributes the total gains to the nodes, under the assumption that they all collaborate, making it as a “fair” distribution as studied by Roth (1988).

Wenjing et al. (2009) have suggested the use of game theoretical solutions to study the interactions between misbehaving nodes in wireless networks comprising of unreliable channels. Continuous monitoring and observation are normally required to find the presence of misbehaving nodes in the network as they do not reveal their identities to their neighbours. The authors have modeled the detection process of misbehaving nodes in terms of a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium is achievable. The authors view that it is not profitable to isolate the malicious nodes and suggest that as long as their
co-existence does not reduce the contribution they make the destruction they cause could be neglected.

Cia & Pooch (2004) also suggest the method of encouraging cooperative works among the selfish nodes rather than eliminating them. Based on their contribution to the coalition, rewarding service providers are assigned. Nodes in a MANET can collude to reduce aggregate transmission power on each hop along a route. The incentive to each node in a coalition is determined by using Shapley value. A truthfulness achieving Contribution reward routing Protocol with Shapley value (CAP-SV) is suggested. Experimental results show that the assigning of incentives to individual nodes stimulates cooperation and improves the network lifetime without decreasing the performance of the whole network.

The next chapter 3 presents the first contribution of this research work to improve the quality of the cluster head.