SECURED ENERGY OPTIMIZATION IN MOBILE

AD HOC NETWORKS

By

MADHUSUDHAN JAKKIDI

Master of Science in Computer Science Dept

Oklahoma State University

Stillwater, Oklahoma

2005

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
December, 2005

SECURED ENERGY OPTIMZATION IN MOBILE AD

HOC NETWORK

Thesis Approved:

Dr. Johnson P Thomas
_____
Thesis Adviser
Dr.   G.E.Hedrick
_____

Dr. Venkatesh Sarangan
_____

Dr. A. Gordon Emslie
_____
Dean of the Graduate College

ACKNOWLEDGEMENT

I wish to express my sincere thanks to my parents for their confidence in me. I would like to thank them for their encouragement at times of difficulty, love and understanding. Special thanks are due to my father for his inspiration, motivation, love and guidance.

I would like to express my sincere appreciation to my advisor, Dr. Johnson P. Thomas for his intelligent supervision, constructive guidance, inspiration, motivation and friendship. I would also like to express my sincere appreciation to Dr. Sarangan and Dr. G.E.Hedrick for providing encouragement and technical guidance throughout this study.

This interesting thesis has been chosen under the guidance of my advisor, in partial fulfillment of master's degree.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

A Mobile ad hoc network (manet) is formed by mobile nodes with wireless links. The property that makes them particularly attractive is that they don't require any prior investment in fixed infrastructure. In emergency services such as disaster recoverywhere the infrastructure may be down, these networks form the only possible option.

The main characteristics of mobile ad hoc networks include

- No base station to provide connectivity to backbone hosts or to other mobile hosts
- New members can join and leave the network at any time
- Each node acts as a router, forwarding packets from other nodes

Two important characteristics about manets are:

1) Routing - As the network is infrastructure less, the communication between source and destination (nodes) is achieved through other nodes. All nodes in the network therefore act as routers.

2) Energy optimization - nodes in a manet are resource constrained and minimizing energy consumption to improve network life is therefore an important characteristic of ad hoc networks.

1.1. Routing

Nodes in a manet depend on each other to forward packets to a given destination. In a wireless network, the routing protocol should take care of effective packet distribution and should compute multiple, cycle free routes according to the frequent changes in network topology, while keeping the communication overhead to a minimum. The route computing time plays a key factor in differentiating various routing protocols as described below.

I. *Proactive Routing protocols[Royer et.al,10]***:**

This kind of protocol is based on the routes computed to all nodes by its routing table. Routes in these protocols are computed based on shortest path technique, which is the main drawback as it consumes power and bandwidth. Whenever a change in the networks occurs, each table of every node has to be updated and this table should be exchanged between neighboring nodes, which again needs bandwidth and power. A large part of the bandwidth capacity of the network and the energy of the node is wasted in route maintenance. As a result, when the mobility rate of nodes is high, proactive protocols are infeasible since they cannot keep up with the changes in the topology.

II. *Reactive Routing Protocols[Royeret.al,10]***:**

This kind of protocol based network works in a 'on-demand' fashion to overcome the limitations of proactive routing protocols. These protocols establish the route only when a route is needed to transmit packets. All reactive protocols, such as Dynamic Source Routing, Temporally Ordered Routing Algorithm, and Ad Hoc On-Demand

Distance Vector routing protocol calculate the route just before sending the message. By passing a small control message to its neighboring nodes in the network, a path is established for communication. However, since the complete route has to be discovered prior to the actual transmission of the message, a sender may experience a long delay in waiting for the route to be computed. Furthermore, there is no guarantee that the route obtained is usable. It is possible that by the time the source node completes the route discovery, a change in network topology has invalidated the route. In a network with high-speed mobile nodes this problem becomes more pronounced as the rate of change of the network topology increases. These protocols are however efficient in terms of the data packet to routing control packet ratio saving battery power in the mobile nodes

III. *Hybrid Approach protocols[Haas et.al.11]***:**

These protocols, such as zone routing protocol, combine the best features of proactive and reactive protocols. In the zone routing protocol, the route discovery phase is divided into an intra zone discovery and inter zone discovery. Intra zone discovery, where proactive way is applied, involves all the nodes whose distance from the sender (in number of hops) < k. The appropriate choice of the zone radius k depends on the mobility rate of the nodes and on the message arrival rate. Inter zone discovery, which operates between zones, uses a reactive approach.

The route is stored as a sequence of nodes. In a proactive protocol the sequence is not explicit; it corresponds to a next hop table lookup at each node along the route. In a reactive protocol the result of a route discovery control message is the route given as an explicit sequence of nodes to follow.

1.2. Energy Optimization:-

 A wireless network consumes energy in several ways, such as to compute the next hop (as described above), to find the route to transfer to the destination, to compute the relocation of the old node etc. Since energy is an important factor that determines the effectiveness of the mobile ad hoc networks, any approach to maximize energy conservation improving the survivability of a mobile ad hoc network.

One approach to maximiz energy conservation is to choose selective nodes to be active at a time, so that these are the only nodes that transmit messages while other nodes sleep. At any time in the network, these are the only nodes that consume energy. But choosing the active nodes is important as it should not disturb the network architecture and basic functions of the network. One of the important ideas for energy optimization is to choose the nodes in the dominating set as active nodes, while the others are kept inactive.

1.2.1. Dominating set:

From a mathematical point of view, a dominating set can be defined as follows.

For a graph G and a subset S of the vertex set $V(G)$, denote by $N_G[S]$ the set of vertices in G which are in S or adjacent to a vertex in S. If, $N_G[S] = V[G]$, then S is said to be a dominating set (of vertices in G). That is each vertex should be covered either by keeping itself in the dominating set or it is covered by the node in the dominating set.

Due to limited resources, it is important to minimize the energy consumption in mobile ad hoc networks. Furthermore, in many applications it is essential to securely communicate between nodes. Security and energy consumption minimization are

4

opposing forces as securing a network results in increased power consumption. In this

thesis we optimize security and energy consumption by proposing the concept of secured

mobile dominating set networks. The literature study about proposed approach is

discussed in chapter 2.The problem domain of the existing approaches is discussed in

chapter 3.The characteristics of the proposed solution is presented in chapter 4.The

proposed solution is discussed in detail in chapter 5.The simulation study and complexity

of the proposed algorithm is presented in chapter 6.The results and conclusions are

presented in chapter 7.Future work is discussed in chapter 8.

CHAPTER II

LITERATURE REVIEW

This chapter outlines the basic literature review for our thesis.

Wu and Li [1] propose a simple and efficient localized algorithm that can quickly determine a Connected Dominating Set in ad hoc networks. This approach uses a "marking Process" where hosts interact with others in the neighborhood. Specifically, each host is marked true if it has two unconnected neighbors. It is shown that, collectively, these hosts achieve a desired global objective—a set of marked hosts forms a small Connected Dominating Set. The resultant dominating set derived from the marking process is further reduced by applying two *dominant rules*. These rules are explained below.

- A marked host can unmark itself, if its neighbors of a gateway are connected with each other via another gateway; it can relinquish its responsibility as a gateway.

- A marked host can unmark itself if its neighborhood is covered by two other directly connected marked hosts.
  The above approach is known as 2-Rule way of marking the dominating set.

The K-Rule for dominating set pruning [2] improves on the two Rules proposed in Wu and Li [1]. According to the K-rule, a marked host can unmark gateways covered by k

other gateways, where k can be any number. This K-rule based experimental results shows that it is better than the combinations of the two rules proposed earlier, especially in networks with relatively high vertex degree and high percentage of unidirectional links. However, in general the approach proposed in [1] is easier to compute when compared to the K-rule method.

The authors in [3] use the concept of active nodes and passive nodes to minimize the communication overhead and energy consumption. Only active nodes are used for communication where as passive nodes are not used as part of communication in the network. The active nodes are selected based on various constraints such as degree and energy remaining at the node. It presents and verifies various combinations of degree and energy in choosing the key for the dominating set node such as degree*energy Remaining, degree/energy Remaining, $\log_{10}$ (degree)*energy Remaining etc.

Poduri and Sukhatme [4] maximize the area coverage of sensor network with the constraint that each of nodes has at least K neighbors, where K is a user specified parameter. When nodes are dropped in a field, each sensor tries to cover at least k number of nodes by using two types of energies, namely, attraction and repulsion. When a sensor has less than the required number of nodes, it attracts the other nodes and when it has more than K-number, it uses the repulsion force to balance the number of nodes in its coverage area.

Srisathapornphat et.al.[5] Presents the variable history based sleeping time for passive nodes to save energy. This approach is similar to the approach used in 802.11.It concentrates on maximizing the energy for the whole network by maximizing the lifetime for a single node. By giving the measured values for transmitter, receiver, idle and

sleeping modes for each node with separate energy level for each mode, it presents better ways to keep a node in active or passive state. It proposes three algorithms for choosing coordinators based on their history of sleeping and other constraints.

In ad hoc routing protocols after a link is broken, a new route is reconstructed during which packets can be dropped, causing significant throughput degradation. Shen [6] utilizes location information on table-driven protocols to reduce the message overhead and to provide link prediction to increase packet delivery. The proposed Location-Triggered Routing protocol only exchanges routing messages when a node changes its location and impacts at least one network route.

Distributed Sensor Networks are ad-hoc mobile net-works that include sensor nodes with limited computation and communication capabilities. [7] Presents a key-management scheme designed to satisfy both operational and security requirements of Distributed Sensor Networks. This scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery and path-key establishment, and for key revocation, Re-keying, and incremental addition of nodes.

Tracy, et. al. [8] survey mobility models used for mobile ad hoc network to test protocol performance under realistic scenarios.. The models includes random waypoint mobility model, random walk mobility model, random direction mobility model, boundless simulation mobility model, gauss-markov mobility model, probabilistic version of mobility model and city section mobility model.

Jie, et. al. [9] proposes reducing energy consumption by constructing the connected dominating set, which reduces the route and complexity of the network. The paper explains the possible scenarios that play a key role in determining the energy consumption of active node and passive node separately. By consuming less energy per unit time, this approach outperforms the other existing approaches.

Royer et.al [10] and Haas et.al [11] gives the overall review on routing protocols in mobile ad hoc networks. These papers present the basic idea and comparison between the table driven, on-demand and zone routing protocols.

CHAPTER III

PROBLEM DOMAIN

The existing approaches ([1], [9]) on dominating set based mechanism are mainly concentrated on routing (dominating set construction) and energy conservation. It is important to answer the following questions for dominating set based approaches.

A Dominating set improves network life by keeping only the nodes in the dominating set as active. Since all nodes are not used in the network, in other words, only the nodes in the dominating set are used, the overall energy consumed for the network will be low.

A question that arises is what happens when the energy of a particular node in the dominating set is fully consumed? If a particular node of the dominating set doesn't work, it cannot be used for transmission. This affects the efficiency and coverage of the network and keeps the network life low.

The best way to alleviate the above problem and to improve the network life is to use a mobile Dominating set. A mobile dominating set can be defined as the set of dominating nodes that keep on changing based on certain criteria. The criteria for mobile dominating set depends on change of network topology, nodes mobility, energy remaining for dominating set nodes and the full energy consumption of active node.

The other question that arises is how to provide security without consuming excessive energy. This plays important role when pair of nodes are not willing to share information.

The approaches proposed to-date consider security and energy conservation as separate issues. In this thesis we provide a simple security mechanism while providing energy optimization. This is accomplished by considering security as a part of the dominating set. Hence, the dominating set will contain secured nodes instead of unsecured nodes. In our approach the mobile dominating set includes security along with the maximum energy remaining as part of the constraints used while choosing a dominating set node.

Our proposed approach mechanism also aims to minimize energy consumption by reducing computations required for the reconstruction of dominating set due to the mobility of nodes.

CHAPTER IV

CHARECTARISTICS OF PROPOSED APPROACH

Our proposed approach is different from existing approaches in two very distinct characteristics.

4.1. Mobile dominating sets:-

Dominating sets are applied in areas such as routing and energy optimization. In our approach, it used for energy optimization. Dominating set reduces the number of nodes that consume energy, thereby reducing the overall energy consumption. In fixed dominating sets, the dominating nodes are kept constant until the nodes that are serving are fully utilized. But when a dominating set node is unable to run, the network cannot be used further. This implies that we need to look for another dominating set formation, which can cover the whole network. However, in some cases this may not be possible due to insufficient number of nodes to form a complete dominating set to cover the network.

By using the concept of mobile dominating set, we change the dominating set at a constant time period based on two factors:

- o   The nodes with maximum energy remaining

- o   The current topology of the network.

This criterion helps to choose nodes which have consumed minimum energy to form a dominating set. We therefore maximize the network life by maximizing the utilization of energy of each node of the network.

4.2. Security:-

We further extend the dominating set to include security. The proposed approach thus provides a secure, energy optimized network. Hence, only the nodes that are secured are able to communicate with each other. Unsecured communications are eliminated.

In our proposed approach, the dominating set is therefore defined by the mobility of the nodes, the energy remaining, security and other network topology constraints (maximum degree etc).

CHAPTER V

PROPOSED SOLUTION

As outlined in the previous chapter, we are proposing a different mobile dominating set using secured and reliable communication between active nodes of the network. The proposed solution consist of four phases,

1) Calculation of dominating set

2) Checking of the connection between nodes by calculating the relocation of the mobile nodes.

3) Optimizing the energy based on the backbone (dominating set) of the network.

4) Securing communication while minimizing energy consumption.

The above phases are explained below.

The dominating set calculation will be repeated depending on the change in the network topology and change in node energy levels to maximize network life.

5.1. Dominating set construction:-

5.1.1. Dominating set:

From a network point of view, a dominating set is defined as a set of hops such that each hop in the original network is either present in the dominating set or it is with in reachable distance (the distance in which nodes can communicate with each other) of the node or nodes present in the dominating set.

A dominating set is said to be connected, if the resultant graph formed by the hops of the dominating set are connected.

A dominating set is said to be minimum, if the number of hops in it are minimum when compared with all other possible dominating sets that can be constructed on the original graph.

The formation of a dominating set is NP-Hard [1].

A simple way to construct a minimum connected dominating set is to start with the highest degree hop and then proceeding with the next lowest or equal degree until the hops in dominating set cover all nodes of the network either directly or indirectly.

Another approach proposed in [1] uses a marking process to calculate the dominating set. Some Other Approaches use minimum spanning tree technique to construct dominating set.

5.1.2. Construction of Dominating sets in small network:

In one cluster or small network,
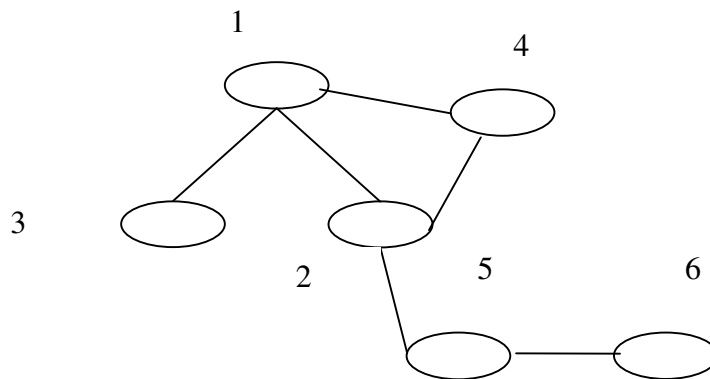
5.1. Small ad hoc network

In figure 5.1, the dominating set formation includes,

(1, 5) because 1 can communicate with 2, 3, 4 and 5 can communicate with 2 and 6.

Thus using (1, 5), the whole network is covered.

Similarly the other possible dominating sets are (2,6,3),(4,3,5),(6,1),(3,4,6) etc.

The minimum dominating set is (1, 5) or (1, 6) with size 2.

5.1.3. Construction of dominating set for large network:

Consider the following network (figure 5.2),
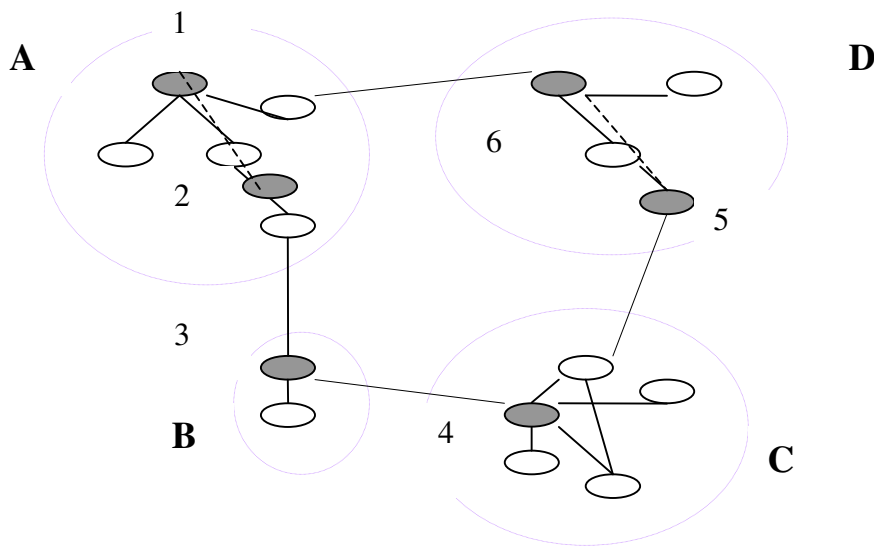
5.2. Big ad hoc network

The dashed lines represent the connection between dominating sets.

Solid lines represent the actual connection between nodes of the network.

In the above network, there are four clusters {A, B, C, D}.

Cluster A contains dominating set as {1, 2}.

Cluster B contains dominating set as {3}.

Cluster C contains dominating set as {4}.

Cluster D contains dominating set as {5, 6}.

Every node has information of its neighbors

In cluster A, 1 contains the information of all the three nodes that are represented in white. Similarly node 2 contains the information of nodes that are indicated in white adjacent to it.

This applies to all clusters (B, C, D) in the network.

Passive nodes do not communicate directly. All communication will be carried out through dominating set nodes only.

That implies the above network with dominating set nodes is as shown below (figure 5.3).
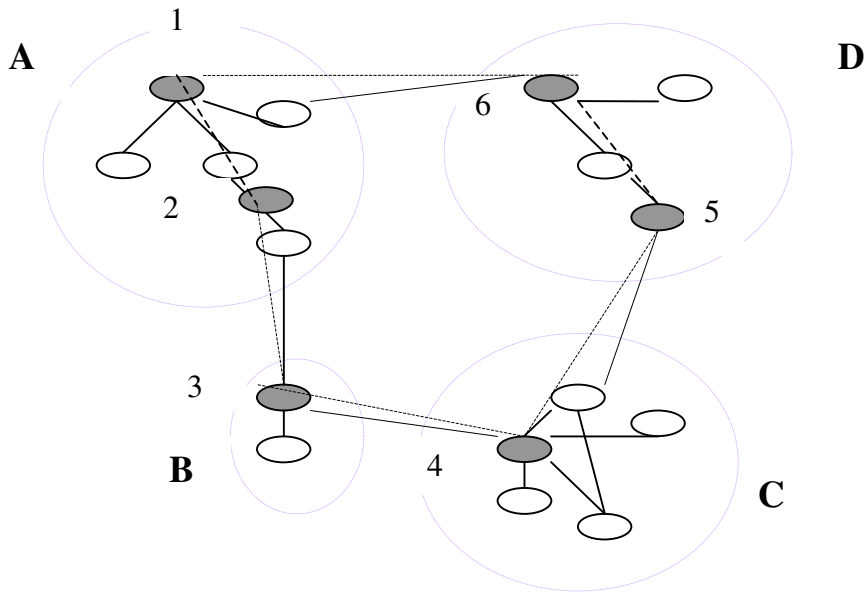
5.3. Big network with dominating sets

Construct the new graph with the nodes as 1, 2, 3, 4, 5, 6 as indicated by the dashed lines in the above diagram, which form a simple dominating set as shown below (figure 5.4).
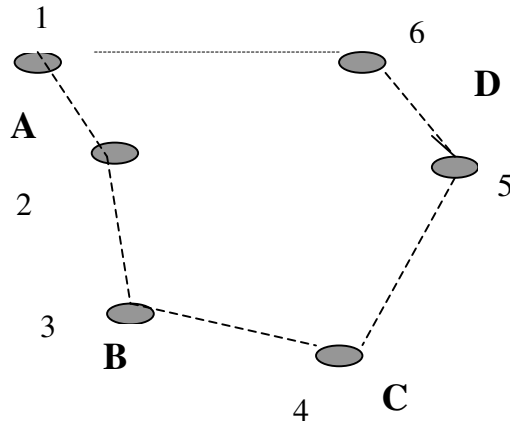
5.4. Dominating set

Hence node 1 contains the information about node 2 and node 6 including the nodes indicated in fig 5.2. In this manner a dominating set is formed for large networks.

5.2. Connectivity

The dominating set of the network should be changed as needed according to changes in the network topology caused by the mobility of the nodes.

5.2.1. Checking for disconnection:

Due to mobility when a node moves to a new location, there may be change in the network topology. In order to obtain the new network topology check the connectivity using the procedure described below.

Each node is assigned a unique number (Id), in order to distinguish it from the other nodes in network. Each node in this mobile ad-hoc network has a list of nodes adjacent to it in the network. The connectivity of nodes is regularly determined at certain intervals by sending a 'Hello Id' message to all its neighbors, where Id is the unique number assigned to it at the start of the network.

When a node receives a 'Hello Id' message from its neighbors, it responds as follows,

- If the message is received, it sends back the 'ack Id', where 'ack' is used to say that it received and 'Id' is the unique number assigned to the receiver node.

- When the sender receives the above message, it adds the Id that came with ack message to its neighbor list.

If an 'ack Id' message is not received within a certain interval 'Tg', the message is retransmitted to that neighbor and if no reply comes back it is assumed the node is disconnected.

Due to mobility, if no node is disconnected from the network, then dominating set is not re-constructed.

5.2.2. Re-Construction of Dominating set:

- Due to mobility, if the resulting node is disconnected from its neighbor, then the dominating set is reconstructed using the above described procedure. In our approach, the dominating set is only reconstructed as needed, in other words, it is not necessary to reconstruct the entire dominating set when the network topology changes due to node movement. This results in reduced energy expenditure.

- If the node is not disconnected from its neighbor even after the node has moved to a new location, then there is no need to reconstruct the dominating set.

- When there exist nodes with more energy remaining than those nodes that form part of dominating set, these nodes with the higher energy can be used as part of the dominating set by reconstructing the dominating set based on energy remaining criteria. This action will be performed at regular intervals of time. This time period can be either user defined or chosen at randomly. Energy remaining for each node is calculated as

    Energy remaining = total energy - energy spent.

5.2.2.1. Key Points in Re-construction of Dominating set:

<u>Type-1:-</u>

Suppose a node moves to a new location from a previous location where it was being covered by a dominating set node. Due to its movement, now it is disconnected from the neighborhood of its original dominating set node, but the new location is still covered by

another dominating set node. In this situation there is no need to reconstruct all or part of dominating set. In other words,

as long as the moved node is covered by one or more dominating set nodes, there is no need for recalculation. The overall coverage of nodes is important while constructing the dominating set as explained below.

Example1:-

Suppose the dominating set for the network with 8 nodes, numbered from 1 to 8, is (2,5).

Let the neighbor set for dominating node 2 be {1,4,7} and 5 be {3,6,8}.

Due to mobility of node 4, it is disconnected from the neighborhood of node 2 and moved to a new location, where it is now covered by dominating set node 5.

In this situation, there is no need to re-calculate the dominating set because the new neighbor set for dominating set 2 is {1, 7} and for 5 is {3, 4, 6, 8}.

The nodes covered by dominating set nodes in the current situation is therefore

= {1, 7} U {3, 4, 6, 8}

= {1, 3, 4, 6, 7, 8}. This is same as the overall nodes covered by the dominating

set before node 4's movement. That is, node set covered before 4's movement is

= {1, 4, 7} U {3, 6, 8}

= {1, 3, 4, 6, 7, 8}

Since there is no change in the overall coverage of the dominating set even though there is a change in the node movement, there is no need to recalculate the dominating set as long as there is no change in the overall coverage of the network.

Type-2:-

When there is a change in a particular cluster of the network, how do we construct the dominating set?

One way to deal with this kind of problem is to reconstruct the whole dominating set. However, the construction of whole dominating set will require more computations and time resulting in increased energy expenditure.

For this we propose a simple solution as follows:

Since every node in a dominating set has a neighbor set associated with it, whenever there is a change in the neighborhood of a dominating set node, this implies that there is a change in the neighbor set of the dominating set node –

The moved node can be in one of the two situations:

- If the node has moved to a different dominating set node's neighborhood, then there is no need to reconstruct the dominating set – this is Type 1 movement as described above.

- If the node is not moved to another dominating set node's neighborhood, then we need to reconstruct the dominating set for the moved node's dominating set node cluster.

Example2:-

Suppose the dominating set for the network with 8 nodes, numbered from 1 to 8, is (2, 5). Let the neighbor set for dominating node 2 be {1, 4, 7} and 5 be {3, 6, 8}. Due to mobility node 4, gets disconnected from the neighborhood of node 2 and moves to a new location, where it is not covered (node A is said to be covered by node B if node B is able to communicate with node A.) by any other dominating set nodes.

In other words, node 4 has moved closer to node 1 and is not within range of dominating set node 5. Now we need to reconstruct the dominating set for cluster {1,2,4,7}.This results in new node 1 being chosen as the dominating set node (assume 7 is within range of 1).

Type-3: -

Suppose a node in the dominating set itself moves. This dominating is moved to new location due to mobility. But if the neighbor set of it is still unchanged, then don't make any changes. Otherwise, re-construct the dominating set for the cluster of this dominating set node (similar to type 1).

Example3:-

Suppose the dominating set for the network with 8 nodes, numbered from 1 to 8, is (2, 5). Let the neighbor set for dominating node 2 be {1, 4, 7} and 5 be {3, 6, 8}. Suppose node 2 moves.

If it has the same neighbor set {1, 4, 7} (possible when all are moving in the same direction with the same speed), there is no need to reconstruct the dominating set. However, if 2 moves away from its neighbors and has a new neighbor set as{1,7}, then follow the steps for ., type 1 or type 2 depending on the other dominating set node's neighborhood. The dominating set of the neighbor set that node 2 left also needs to be recalculated.

To summarize, due to mobility of nodes, if there is a change in the neighbor set of the dominating set node:

- If the overall coverage by the dominating set is the same, then no changes are made to the network.
- Else,

o If the node has moved is non dominating set node, then recalculate the dominating set for the cluster to which the node has joined if the current dominating set node does not cover the newly arrived node

o If the node that has moved is a dominating set node, then recalculate the dominating set for the cluster from which the dominating set node has moved

5.3. Optimizing energy based on dominating set

The dominating set is constructed as explained above. The optimizing of energy works as follows:

Only the nodes in the dominating set function as active nodes. All others remain as passive nodes. The transfer of messages is possible only within active nodes or nodes that are part of the dominating set.

If a node has to send a message to an inactive node, then the message is sent to the nearest (neighbor) active node of that passive node. The communication between passive nodes is done through their active neighbors. Every active node consumes much more energy than passive nodes.

Example 4:-

Suppose a given network with 'N' number of nodes consumes 'E' energy per node. Let the dominating set of the network constructed as described above contain N/3 (this number can vary anything from 1 to N) nodes.

The energy consumed for the network without using dominating set will be approximately equal to N*E, whereas the energy consumed for the same network in the

same amount of time by the use of the dominating set will be approximately Equal to N*E/ 3(because only the N/3 nodes are used in the network run).

According to example 4 above, this energy consumption is reduced, hence increasing the network life by applying mobile dominating sets. These dominating sets are dynamic, that is, they change with network topology and energy levels of nodes, resulting in an even usage of energy of all the nodes in the network resulting in increased survivability of the network.

Always choose a node with maximum energy remaining as a part of dominating set from the list of neighboring nodes associated with their energy levels.

5.4. Secured Networking:-

The secured communication between nodes of dominating set can be achieved by the use of keys based on the work reported in [7]. Each node in the network is assigned a set of keys associated with it. Two nodes can communicate if they share a key. The keys involved in secured communication between pair of nodes need not be the keys of their own; they can be part of the other node's key set, which are part of communication path. The communication between nodes that do not share a key is not secured.

Since each node has a certain number of keys, there might be some common keys which can be present in two node sets.
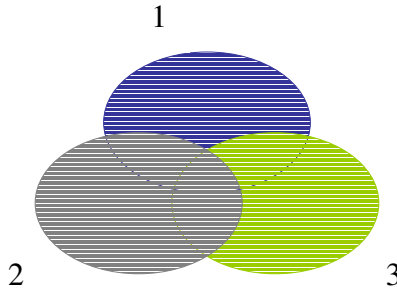
5.5. Security key management diagram

Figure 5.5 shows a network with three nodes sharing a common set of keys. The intersection part of each node region with other represents the set of keys that are common to each other thus permitting secure communication between them. If key set of 1 contains keys {2,3} and set of node 2 contains {3,1},there exist the communication between 1 and 3 (assume 3 does not have any keys) secured through 2 .Always give priority for secure communication links to be used as a link in the dominating set instead of insecure link

5.5 seurity and energy optimization

The optimization of energy using secured communication may not be possible all the time due to the fact that nodes that are part of secured communication may not be the nodes that are part of minimum network energy consumption. The objective of this proposal is to provide secured communication between nodes using the concept of dominating set by maximizing energy optimization.

Always choose a secured node, a node that is part of secured communication, with better energy remaining will be chosen.

25

When constructing the dominating set, a secure node (a node with which secure communication is possible) is give priority over a node with more energy remaining. The aim is to provide secure communication as much as possible by utilizing the available resources. When secure communication is not possible, we will construct the dominating set based on energy optimization criteria only.

Our approach to dominating set will include this security issue along with energy optimization.

5.6. Key points in construction of mobile secured dominating set

1. Construct the dominating set as explained above.

   While forming a dominating set, perform the following to keep uniform secured energy utilization.

   i.   Always give priority for secured nodes to be used as active nodes instead of unsecured nodes. i.e. choose a secured node as apart of dominating set when there is competition between secured and unsecured nodes

   ii.   Always choose a node with maximum energy remaining as a part of dominating set from the list of neighboring nodes associated with their energy levels. Energy remaining for node=total energy-energy spent (This step should be chosen after performing step i.).

   Now all nodes in the dominating set are secured nodes and have maximum energy remaining.

2. Check the connection between neighbors: Send messages (as explained in section 5.2.1) between the neighbor nodes.
   Two nodes 'A' and 'B' are said to be neighbors if 'A' is with in reachable distance of node 'B', that is, they can communicate directly. Two nodes 'A'

and 'B' are said to be disconnected if 'A' is not with in reachable distance of node 'B'

- When node 'A' of disconnected set of nodes, is unable to send/receive messages from its neighboring nodes, go to step 3.
- If no node is disconnected, do nothing, that is, leave the dominating set as it is; go to step 6.

3. Perform the calculation of finding neighbor set for each node in the network to find the network topology.

4. If there is no change in the neighbor set for the node that is a part of dominating set, don't recalculate the dominating set.

5. If there is a change in the neighbor set of dominating set node,

- If the overall coverage by the dominating is the same, then don't make any changes in the network (as explained in type 1, section 5.2.2.1).
- Else, go to step 2 to recalculate the dominating set for this dominating set node's cluster of the network based on new network topology without disturbing the other clusters dominating set nodes(as explained in type 2,section 5.2.2.1).

6. When there is chance of forming a less energy consuming secured dominating set from the existing network by considering the energy remaining, security, maximum node degree etc, redo the process of dominating set construction by going to step2.

Keep doing the above six steps until the energy remaining for nodes is insufficient for the network to survive or there is no more use of the network.

This algorithm represents the basic steps in simulation design. It clearly analyzed in the following chapters.

5.7. Example of Algorithm

Consider a mobile ad hoc network with undirected graph G_m (V_m, E_m), where $V_m =$ {1,2,3,4,5,6,7,8,9} and E_m={(1,2),(1,8),(1,9),(2,1),(2,3),(2,4),(2,9),(3,2),(3,5),(4,2), (4,8),(5,3),(5,6),(5,8),(6,5),(6,7),(7,6),(7,8),(7,9),(8,1),(8,4),(8,5),(8,7),(9,1),(9,2),(9,7)}.

The graph G_m is shown below.
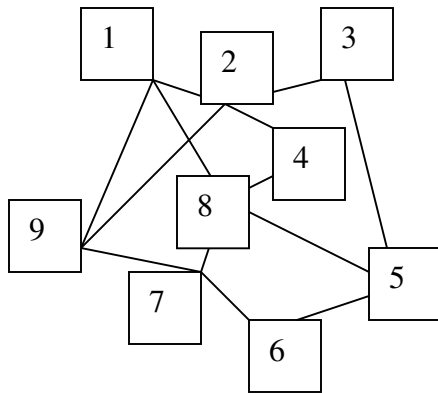
5.6. Mobile ad hoc network

The network in the fig 5.6 contains the following set of neighbors for each node.

The adjacency list of node 1 contains {2, 8, 9}

The adjacency list of node 2 contains {1, 3, 4, 9}

The adjacency list of node 3 contains {2, 5}

The adjacency list of node 4 contains {2, 8}

The adjacency list of node 5 contains {3, 6, 8}

The adjacency list of node 6 contains {5, 7}

The adjacency list of node 7 contains {6, 8, 9}

The adjacency list of node 8 contains {1, 4, 5, 7}

The adjacency list of node 9 contains {1, 2, 7}

Consider a security key network ,with undirected graph (V_s, E_s), where $V_s =$

{1,2,3,4,5,6,7,8,9} and E_s={(1,2),(1,4),(1,9),(2,1),(2,5),(2,7),(3,4),(3,6),(4,1),(4,3),(4,8),

(4,9),(5,2),(5,6),(5,8),(6,3),(6,5),(7,2),(7,5),(8,4),(8,5),(9,1),(9,4)}.

The above key network is shown below.
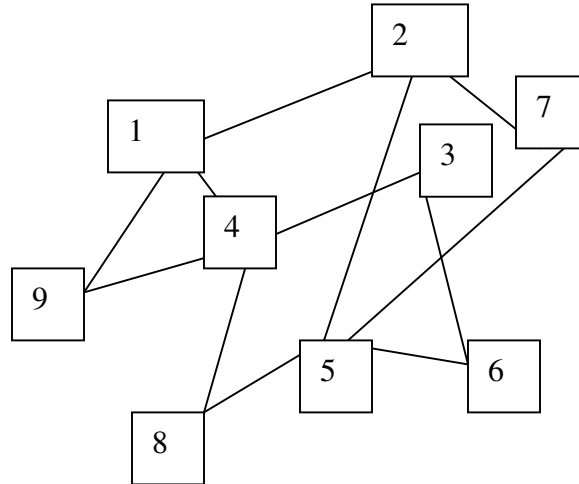
5.7. Security key network

The network in fig 5.7 represents the keys for each node through which secured

communication is possible. That is

Node 1 securely communicates with its neighbors {2, 4, 9}.

Node 2 securely communicates with its neighbors {1, 5, 7}

Node 3 securely communicates with its neighbors {4, 6}

Node 4 securely communicates with its neighbors {1, 3, 8, 9}

Node 5 securely communicates with its neighbors {2, 6, 7, 8}

Node 6 securely communicates with its neighbors {3, 5}

Node 7 securely communicates with its neighbors {2, 7}

Node 8 securely communicates with its neighbors {4, 5}

Node 9 securely communicates with its neighbors {1, 4}

The result is stored in secure dominating set network, with undirected graph (V_{ds}, E_{ds}), where $|V_{ds}| \leq |V_m|$} and $E_{ds} = \{(x,y)| x \in V_{ds}$ and $y \in E_m \cap E_s, \forall x\}$ with the constraints of maximum possible degree (to minimize the dominating set size) and energy remaining per node.

Working steps in simulation part for the above network:-

1. Choose any node 'x' such that $x \in V_m$ and x has maximum possible degree of un-covered nodes. That is $x_{Max\_deg} = \{x \mid x \in V_m \wedge x$ has maximum degree in $V_m\}$

   - In this case it is node 8 with maximum possible degree of 4 (fig 5.6).

2. Choose any node 'y' from x's security key network adjacency list, which has the highest number of uncovered nodes in mobile ad hoc network graph.

   i.e $y_{ds\_node} = \{y \mid y \in V_s \wedge (x_{Max\_deg}, y) \in E_s \wedge y$ has maximum degree in $V_m\}$

   - In this example, choose any node from the security key set of node 8 with highest degree of uncovered nodes in mobile ad hoc network.

   - In this case, the key set V_{ss} (defined as set of security keys for the current dominating set) for secure dominating set (SDS, defined as the set of nodes representing the secure dominating set) 8 is {4, 5}.

     - Pick any node from the above set to be the next node in the dominating set. Here node 8 is covering (1, 4, 5, 7). The node selected for the dominating set should cover other uncovered nodes. Node 5 covers 3 and 6 whereas node 4 covers only 2. Therefore node 5 is chosen as part of dominating set.

- Now the key set for 5 from security key network graph (fig 5.7) is (2, 6, 7, 8).So new security key graph V_{ss} will be the union of two dominating set node's key sets.

  V_{ss}= {key set of x_{Max_deg}} $\cup$ {key set of y_{ds_node} }

  i.e V_{ss}= {key set of 8} $\cup$ {key set of 5}

  V_{ss}= {4, 5} $\cup$ {2, 6, 7, 8}

  V_{ss}= {2, 4, 5, 6, 7, 8}

  The dominating set is union of previous dominating nodes and dominating node chosen in this step.

  i.e SDS = SDS $\cup$ {node 5}

  SDS = {8} $\cup$ {5}

  SDS = {5, 8}

3. Since we have chosen nodes 8 and 5 already as part of dominating set, the new key set to choose next dominating node, should not contain dominating set nodes 5 and 8. Ie V_{ss} = V_{ss}-dominating set

   V_{ss} = {2, 4, 5, 6, 7, 8}-{5, 8}

   V_{ss} = {2, 4, 6, 7}

4. Node 4 can be chosen as part of dominating set using the same rules that we applied in step 2.The updated dominating set in this step is {4,5,8}.

   The new key set V_{ss}=V_{ss} $\cup$ {key set of 4}

   V_{ss} = {2, 4, 6, 7} $\cup$ {1, 3, 8, 9}

   V_{ss} = {1, 2, 3, 6, 7, 9}

   and SDS =SDS $\cup$ {node chosen in this step}

$$\text{SDS} = \{5, 8\} \cup \{4\}$$

$$\text{SDS} = \{4, 5, 8\}$$

5. Now choose any node from the above key set V_{ss}, and that covers the remaining nodes. Node chosen in this step is 9.

The security set $V_{ss} = V_{ss} \cup \{9 \text{ key set}\}$

$$V_{ss} = \{1, 2, 3, 6, 7, 9\} \cup \{1,4\}$$

$$V_{ss} = \{1, 2, 3, 4, 6, 7, 9\}$$

And $\text{SDS} = \{4, 5, 8\} \cup \{9\}$

$$\text{SDS} = \{4, 5, 8, 9\}$$

But removing SDS repeated nodes (nodes that are present both in V_{ss} and SDS) from V_{ss}, I.e. $V_{ss} = V_{ss} - \{\text{SDS repeated nodes}\}$

$$V_{ss} = \{1, 2, 3, 4, 6, 7, 9\}-\{4, 9\}$$

$$V_{ss} = \{1, 2, 3, 6, 7\}$$

6. Since the dominating set nodes covers all the nodes in the network, the set construction stops. The final dominating set is {4, 5, 8, 9} which forms a secured dominating set network is shown in below fig 5.8.
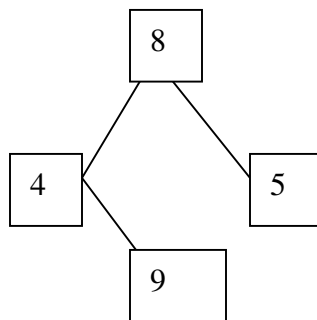
5.8. Secured dominating set

CHAPTER VI

SIMULATION

We developed our own simulation framework to evaluate energy optimization. The

simulator was developed using VC++.Net 2003 on windows XP operating system.

Our proposed simulation simulates the network in the form of a graph. The random walk

model [8] was used to model mobility. The dominating set was be re-calculated based on

network topology characteristics such as nodes mobility and energy levels, as a part of

the simulation. We also developed a graphical interface to view and analyze the

algorithm.

Each node's security key set is either taken as a user input or chosen randomly from the

nodes available in the network. Each node is assigned a random (or user defined) number

of keys and each key is assigned randomly. The Energy levels for the dominating set

nodes and for the nodes that are passive is input by the user or input as a simulation

program. The comparison of the normal network along with our proposed network

characteristics and results are shown at the end of the simulation.

The characteristics of the simulation results include

- Energy consumption variation along with security.

- Dominating set formation.

- Complexity of the simulation.

- Energy utilized per node.

6.1. Complexity

The complexity of the algorithm depends on the number of statements to be executed.

The proposed algorithm includes

  a) The time complexity of the marking and unmarking process at each vertex is
     $O(\Delta*\Delta)$, where $\Delta(G) = \max\{M(v), v\varepsilon V\}$, where $M(v)$ represents the
     neighborhood of vertex v in a graph G with vertices V.

  b) The process of checking whether the node is secured or not takes an $O(K)$,
     where K represents the length of the key set (number of keys) for that node.

  c) To calculate the energy remaining per each node of the graph requires $O(N)$,
     where N represents the number of nodes in a graph.

  d) For checking the connectivity of the each node with its neighbor set of K keys
     requires $O(N*K)$.

The overall Complexity of constraints

$$= O(K) + O(N) + O(N*K)$$

$$\approx O(N) + O(N*N) \qquad\qquad \text{(since } K<N)$$

$$\approx O(N*N) \qquad\qquad \text{(since } N<<N2.\text{when } N \text{ is large.)}$$

The total complexity of the simulation including dominating set calculation is

$$\text{Total complexity} = O(\Delta*\Delta) + O(N*N)$$

$$\approx O(N*N) + O(N*N) \qquad \text{(since } \Delta<N)$$

$$\approx O(2N*N)$$

$$\approx O(N*N)$$

6.2. Complexity Comparison with other Approaches

The proposed algorithm includes additional complexity for computing the

repeated check to form a better dominating set based on energy remaining at regular

intervals(O(N*N) added)

It includes the complexity of O (K); where k is the size of secure key set, for checking

security when compared with normal algorithms.

However, the overall complexity when it is applied to a large network equals O (N*N),

which is a common complexity incurred in energy optimization [1].

CHAPTER VII

RESULTS

The simulation for the proposed approach was developed based on the key points

discussed in chapter 5 to include object oriented features and a user interface. The

simulation part mainly deals with the construction of secured dominating set network

with constraints on security, maximum energy remaining, and connection between nodes.

This chapter looks at:

- Construction of security key network.

- Construction of mobile ad hoc network, random walk model.

- Dominating set based energy calculation.

- Simulation results and graphs.

Security key network is constructed only once for a simulation run. This network is fixed

and it is the same for the whole simulation run, whereas the mobile ad hoc network is

constructed repeatedly depending on the links obtained according to the random walk

model. The assumption made in construction of security key network is that, the total

number of keys that each node can securely communicate is taken randomly between 0 to

totalNodes /5,where 'totalNodes' represents the size of the network. The number

totalNodes/5 gives the simulation at max a node can have $1/5^{th}$ of the total number of

nodes in the network, which makes the simulation close to real time application.

7.1 Random walk model

The Random walk model is used in our simulation to model the mobility of the nodes in the network in two dimensional planes. It is implemented as follows.

All nodes in the network start at the same point at the beginning of the simulation. Each node moves in a random direction, chosen between direction lower limit (directionMin) and upper limit (directionMax), with a random speed, chosen between speed lower limit (speedMin) and upper limit (speedMax) . When a node reaches the boundary line, it bounces back with the same speed with which it came. The nodes within a particular distance range are considered as adjacent nodes.

Simulation assumptions made in this model are

- The starting point for all nodes in the beginning of the simulation is (0, 0).

- The random direction can be any value between directionMin=0 to directionMax = 360 degrees.

- The random speed can be any value between speedMin=2 pixels/sec to speedMax = 6 pixels/sec.

- The range for adjacent nodes is taken as 3.5 pixels.

- The network bound assumed for the network is 1280 by 800 pixels computer screen.

- When the node reaches a boundary line, it bounces back with same speed with which it came.

- The simulation is repeated for different network sizes 20,30,40,50.

7.2. Energy calculation

The energy consumption for the network is based on two types of nodes, the nodes that are part of the dominating set (active or serving node) and nodes that are passive. A passive node is the one which just transmits or receives messages through its nearest dominating set node. It is not involved in routing etc. An active node is a node in the dominating set.

The energy calculations for active node and passive node are therefore calculated separately.

The energy calculation of a passive node is

$E_{passive} = E_{send} + E_{recv}$.

Where,

$E_{passive}$ represents the energy spent for each passive node.

E_{send} represents the energy spent in transmitting a packet of node

E_{recv} represents the energy spent in receiving a packet.

The energy involved in the transmission of 'N' packets in the network is

$$E_{passive} = N*(E_{send} + E_{recv}) \qquad (1)$$

In this above equation, (1), E_{recv} is assumed a constant. The energy involved in sending can be taken either as constant or calculated based on the distance between source and destination.

To calculate the energy for transmitting a packet based on the distance between sender and receiver,

$E_{send} = k*distance^{\gamma}$.

Where

'k' and 'γ' are constants. The distance is calculated based on the distance between nodes in the two dimensional space using the random walk model.

Let A(x1,y1) and B(x2,y2) be two nodes in a network. The distance between A and B is the distance between two points in two dimentional space.

i.e. distance between A and B is $= \sqrt{(x2-x1)^2 + (y2-y1)^2}$ (2)

The dominating set nodes (active nodes) consume more energy when compared to non dominating (passive) nodes because they are involved in two extra tasks.

- Routing information gathering and updating,

- Packet relay.

For routing, consider routing energy spent in updating a path for every 'm' packets and each updating process includes a flooding among all dominating nodes.

The energy involved in the above scenario for each dominating node is

$E_{routing} = (N*totaN \, odes/m) *(E_{send}+avgdegree*E_{recv})$

Where

$E_{routing}$ is the energy spent for routing for a dominating set node as part of routing between any two neighborsin the dominating set.

'totalNodes' is the total number of nodes in the network

'avgDegree' represents the average degree corresponding to each dominating set node.

'm' is the number of packets

For packet relay, consider the task of relaying is evenly distributed among all dominating nodes,

$E_{relay} = ((L-1)*N*totalNodes/Dominatingnodes)*(E_{send}+E_{recv})$

Where,

E_{relay} is the energy spent for relay between neighbors in the dominating set.

L is the average path length.

L is the average path length.

Dominatingnodes represents the number of nodes that are part of the dominating set.

Therefore the overall energy spent for each active node is

$E_{active}= E_{passive}+E_{routing} +E_{relay}$

$E_{active} = E_{passive}+(N*Totalnodes/m)*(E_{send}+avgdegree*E_{recv}) +$

$\qquad (L-1)*N*toatlNodes/domiatingnodes)*(E_{send}+E_{recv})$

$E_{active} = (1+ alpha*totalnodes+beta*(totalnodes/dominating nodes))E_{passive}.$ \qquad (3)

Where,

'alpha' is routing overhead , alpha $= (K+avgDegree)/(m*(K+1))$

'beta' is the average number of relays for each packet (beta $=$ L-1).

Assumptions made in this part of simulation are

- The energy involved in 'receiving' is 0.1.

- The energy involved in sending a packet is calculated in both cases, that is, constant and distance based.

    o The assumed value of constant sending is E_{send} is 10 times the E_{recv}. That is the value of constant 'K' is 10.

    o The value of 'k' =1 and gamma=2 when sending energy is calculated based on the distance.

- The number of packets transferred between each pair of nodes in the network are 2.That is N=2.

- The route is updated for each 10 packets. That is m=10.

All the above constants are taken after several sample executions of simulation.

7.3. Formal Algorithm

The following formal description of algorithm explains the main steps involved in the simulation part of secured dominating set energy calculation network.

#Procedure secure_graph, accepts input from the user and calls the main modules of #the simulation for further calculation and then prints the output.

Algorithm secure_graph

   Begin

   Var *networkEnergy* **array [0..N]** of **integers**

      Input: Accept user input for number of nodes, 'N' and uniform energy of

         network per node, 'E'.

      for every node, *I* of *networkEnergy[I]=E*

      #create security key network.

      Call createSecurityKeyNetwork

      #create mobile network and perform other main functions.

      Call untilFinish.

      Output: Print energy consumption.

   End

#this creates the security key networks based on the random number of adjacent #links

and random node selection based on rand ().

Algorithm createSecurityKeyNetwork

Begin

    Var *secureLinks* **array [0..N]** of **integers**

    Var *I, j, key:* **integer**

    For all elements 'x' of *secureLinks*, *securĿinks[x]* → 0

    I → 0

    j → 0

    Repeat until *I < N*

    Choose random number, *r* → rand()%5.

    Repeat until j < *r*

    Choose random *key* from 0 to N, *key* → rand()%N.

    If *key* is not in *secureLinks* **then**

        secureLinks[i] → key

        j → j +1

    end if

   end loop # j loop

   end loop # I loop

End

Procedure untilFinish constructs the mobile network,, constructs the dominating set

and finally calculates the energy spent in the network.

Algorithm untilFinish

Begin

Var *isPossible***: Boolean.**

Var *I* **:integer**

Var *location* **array [0..N]** of **integers**

I $\rightarrow$ 0

For every node 'x' of *location*, *location[x]* $\rightarrow$(0,0)

Repeat without condition,

Begin loop

isPossible $\rightarrow$ **true**

#to create the mobile ad hoc network based on random way point model.

Call createMobileNetwork

to construct dominating set.

Call constructDS

#to check for the completeness of dominating set.

Call checkForCompleteDS and assign it to *isPossible.*

to calculate the energy consumed in the network.

Call calculateEnergy

For every node 'n' in network, *consumption* $\rightarrow$ *consumption + networkEnergy[n]*

If *isPossible* = **false or** *consumption* > 50% of total energy **then**

break

end if.

End.

#This procedure calculates the mobile ad hoc network links based on the random walk

 #model described earlier. The range and random speed bounds can be chosen according to

the simulation requirements.

Algorithm createMobileNetwork

Begin

Var *random_speed, random_direction, range :* **double**

Var *I ,j :***integer**

    Initialize *smin,smax***.**

    random_speed =smin + rand() % (smax-smin)

    random_direction=rand()%360

    Initialize *range*.

    after certain **time,** T,

        Calculate new location for all nodes in the network, based *random_speed,*

            random_direction and old location.

        I → 0

        Repeat until *I<N*

       begin

            Repeat until j<N

            begin

            Find *distance* between *I* and *j.*

            If *distance < Range* **then**

                mobileLinks[I] → j

            end if

            end loop

end loop

End.

\# Procedure constructDS constructs the dominating set based on the dominating

\#node chosen. It updates the security key set in order to choose the next dominating node

\#from the available security keys.

Algorithm constructDS

Begin

    Var *possible***: Boolean**

    Var *index,temp,:***integer**

    Var *DS* **array [0..20] of integers**. \#to hold the dominating set variables

    Var *DSPrev* **array [0..20] of integers**. \#to hold the previous dominating set nodes.

    Var *securitySet* **array [0..50] of integers.** \# to hold the security keys.

    possible→**true**

    index→*0*   \#this is the index of dominating set, that is used for current chose DS node

    Initialize *DS, DSPrev* and *securitySet*

    Repeat until *possible* = **false**

    Begin loop

        \#to check the previous dominating set

        Call checkPreviousDS   \#pass variable *temp* and *index*.

        If *temp* = -1 **then**

        begin

            possible → **false**

        end if

else

begin

DS[index] →temp

index->index+1.

End else-if.

Update the *securitySet* to include the extra *temp* node's *secuirtyLinks.*

DSPrev[index] → DS[index]

DSPrevAdj[index] →MobileLinks[DS[index]]

end loop

End

\# checks for the need of new dominating set construction. Depending on the type change

\# in the neighborhood of dominating set nodes, the dominating is constructed (type1,2,3

\# of chapter 5).

Algorithm checkPreviousDS

Var *j,temp* **: integer**

Var *diffNodes[0..20] ,otherDiffNodes[0..20]***:integer**

Begin

   \#checks the completeness of the DSPrev dominating nodes with new mobile network

   links.

   \#It will not be called first time, since there is no previous DS

   Call checkForCompleteDS and assign it to *temp.*

   \#type 2 is failed.

   If *temp == -1* **then**   \#need to construct new DS

   Begin

If *MobileLinks[index] !=DSPrevAdj[index]* **Then**

Begin

   diffNodes→|MolbileLinks[index]-DSPrevAdj[index]|

   For all elements *j* of *DSPrev*

   If *j!=index* **then**

   begin

      otherDiffNodes→otherDiffNodes+| MolbileLinks[j]-DSPrevAdj[j]|

   end

      #new dominating node is required for this cluster, type#1 failed

   if *DiffNodes* is **Not In** *OtherDiffnodes* **then**

   Begin

      Call chooseNode and assign it to *temp. #for the cluster DSPrevAdj[index]*

   End if

 End if

End

#this procedure chooseNode helps in choosing the dominating set node. The criteria

#chosen are maximum energy left, maximum adjacent nodes, secured communication

etc.

Algorithm chooseNode

Var *I, max, count, node***:integer**

   Begin

   Initialize *I, max, count* Initialize *node* to -1.

   Repeat until *I* < **size** of *securitySet*

   Begin loop

For All *mobileLinks [I]*

    Assign *count* to total **uncovered** nodes.

If *count >max* **and** *securitySet[I]* **Not In** *DS* **then**

Begin

max →count

node → securitySet[I]

end if

if *count =max* **and** *Energy[securitySet [I]]>Energy[node]* **then** ,

begin

    max→count

    node →securitySet[I]

end if

End loop.

Return *node*

 End

#this procedure is to check the completeness of the dominating set constructed. It helps in

#deciding when to stop the construction of the dominating set.

Algorithm checkForCompleteDS

Var *I, j:* **integer**

Var *Occur:* **boolean**

  Begin

  j→0

  Repeat until *j<N,*

Begin

    Occur → **false**

    I →*0*

    Repeat until *I* < **size** of *DS* ,

    begin

        If *j=mobileLink[DS[i]]* **then**

            occur →**true**

        end if

    end loop

    if *occur* =**false, then**

    begin

        return false

    end if

  end loop.

  return true

End

#This is the main procedure to calculate the energy spent for the network. The calculation

#of energy spent for each node, active/passive is calculated separately as explained in the

#previous section.

Algorithm calcEnergy

  Begin

  Var *I*: **Integer**

    I→*0*

  Repeat until *I* < *N*

If *I* **is in** *DS,* **then**,

       Energy[I] →*Energy[I]-Eactive* #(from equation (3) of section 7.2.).

end if

If *I* **is not in** *DS*, **then**

    Energy[i] →*Energy[i]-Epassive* #(from equation (1) of section 7.1.).

end if

  End loop

End

The variables declared in one procedure are used in other procedures with the assumption

that they are passed as a parameter list.

The above algorithm presents the main steps in the simulation process.

7.4. Results and graphs

The simulation process is run until 50% of the whole network energy is consumed.

The simulation is repeated for network sizes of 20,30,40,50 respectively.

The results of secured key dominating set network are compared with unsecured dominating set network and general mobile ad hoc network with and with out security.

Simulation results are drawn for these three types of networks in different scenarios namely:

- constant path based energy calculation

- distance based maximum path energy calculation

- Nodes surviving after simulation (more 50% of energy consumed).

The path between source and destination for packet transfer in the general mobile ad hoc network is calculated as shown below.

- Pick any node from the adjacency list of the source and establish this node as part of path. Make this node as source and proceed until destination node is found or no path exists (adjacency list is empty).

- If adjacency list is empty then repeat the process by picking another adjacent node of the previous node in the path.

- If destination is found, stop the process and confirm the path.

7.4.1. Average Path Comparison

The average path length traveled for each packet to reach its destination is calculated for each secured dominating set network, unsecured dominating set network, secured manet and unsecured manet. The path length is one of the important factors that play a role in calculating the energy spent for each dominating set node in the simulation

Average path length for a network is defined as the average number of hops a packet will travel for each possible source and destination pair.

These results are drawn for each network with sizes 20, 30, 40 and 50.

The results are shown below.

Number of nodes	Secured Dominating set network	Unsecured Dominating set network	Secured Mobile Ad hoc network	Unsecured mobile ad hoc network
20	3.30556	2.61111	2.69472	2.44444
30	3.31034	2.86207	2.73358	2.51379
40	3.34783	3	2.85652	2.75652
50	3.41176	3.05882	2.96521	2.89294

7.1. Average path comparison

The values in table 7.1 are drawn in the graph below by comparing secured and un secured dominating set approaches average path length.
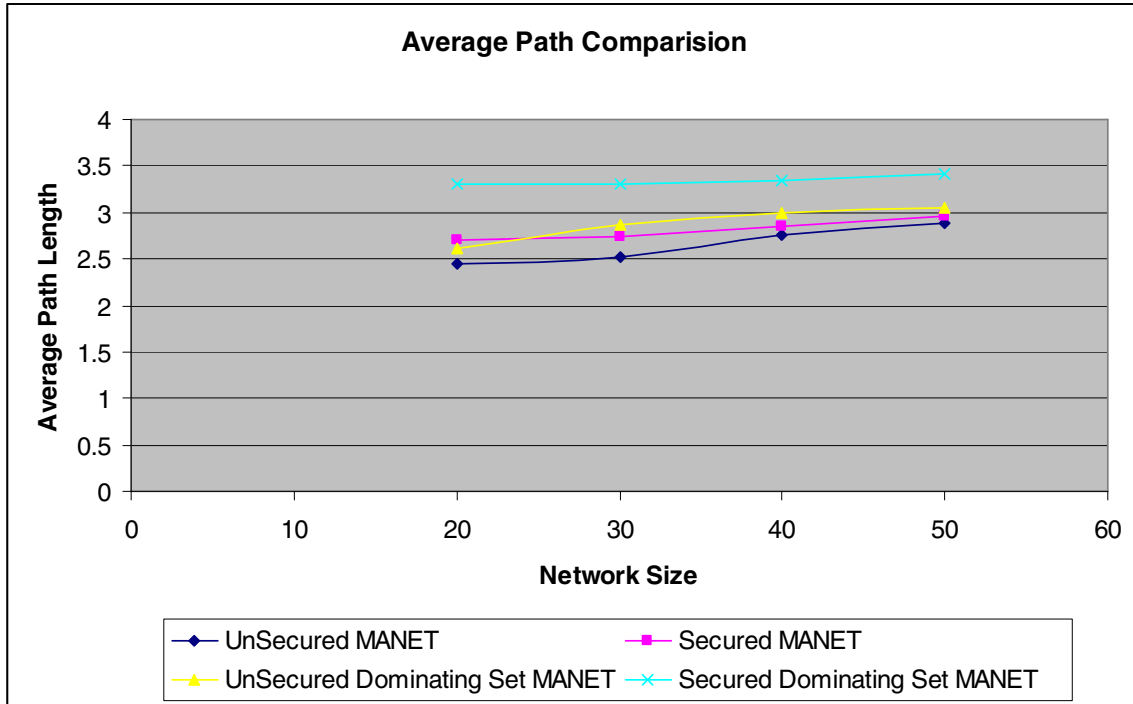
7.1. Average path comparison

Discussions and conclusions:-

From the above results we can see that:

- The average path length in the secure dominating set network is greater than the average path length of the unsecured dominating set network.

- The average path length in the secured manet is greater than the average path length of the unsecured manet.

- The average path length increases as the network size increase but not proportionally

- The difference between average path length decreases as the network size increases, but at a slower pace. This is due to the fact that the security key set becomes richer as the network size increases. In other words, there is a higher probability of obtaining a key with a neighbor.

53

7.4.2. Distance based energy comparison

The energy spent in transferring a packet between source and destination is calculated based on the path taken between them. Between source S and destination D, energy is calculated as follows.

1. The S and D are taken as the source and destination of the longest path from all pair of nodes in the network.

2. The energy is calculated for the shortest path between pair of S and D.

The energy spent in the transferring a packet between source and destination is the total energy spent for transferring packet from source to destination through the intermediate dominating set nodes.

The energy is calculated based on distance between source and destinations, which are represented as (x, y) coordinates in a two dimensional field using a random walk mobility model.

Distance based send energy for each network is calculated as follows.

- Distance between pair of nodes is calculated based on equation (2) in section 7.2.

- The energy spent for each dominating set node and non dominating set node is calculated using equations (1) and (3) in section 7.2.

- The energy spent for the whole network is the sum of energies of all individual nodes

The results of secure dominating set network are compared with unsecured dominating set network and mobile ad hoc network with and without security.

The results are obtained for different network sizes of 20,30,40,50 nodes based on shortest path between pair of nodes as described above.

The results are shown in table below.

Network size	Secured dominating set network	Un secured dominating set network	Secured mobile ad hoc network	General mobile ad hoc network
20	3266	2423	12212	10500
30	3472	2883	18332	15229
40	3919	3108	25367	21243
50	4931	4215	32809	27519

7.2. Distance based energy consumption

The Results shown in the table 7.2 are shown in the graph below.
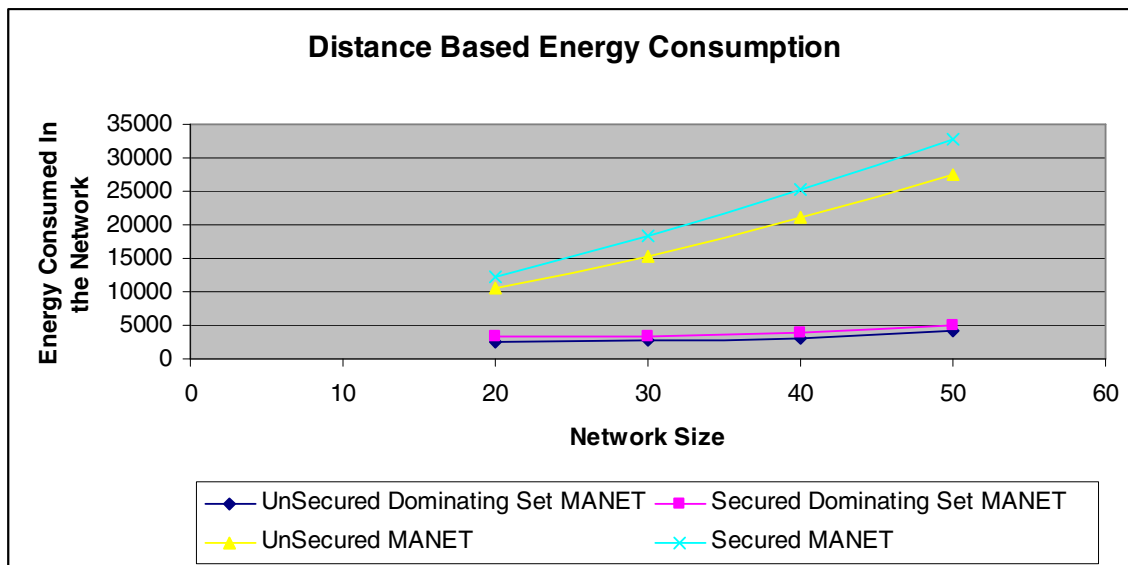
7.2. Distance based energy consumption

These results show that

- The unsecured dominating set network consumes the least energy while the secured mobile ad hoc network consumes the maximum.

- The energy levels for manets with and without security increases as the network size increase at a rapid rate.

- The energy consumed for secured network is close to the unsecured dominating set network

- The results can be interpreted due to the result of longer average (maximum) path resulting for a secured dominating set network when compared to unsecured dominating set network as shown in table 7.1.

- The difference between the secured energy level and unsecured energy level decreases at a slower pace as the network size increases.

7.4.3. Constant send energy based comparison

The energy consumed in transferring a packet between source and destination is assumed to be a constant. These results are obtained independent of the path taken by the packet transmission. All paths are assumed to have the same length.

The energy consumed in sending a packet is assumed to be 10 times the energy spent for receiving.

Constant send energy for each network is calculated as follows.

- The path for packet transmission is taken as constant. So the sender energy is taken as 10 times the receiver.

- The energy for spent for each dominating set node and non dominating set node is calculated using equations (1) and (3) of section 7.2.

- The energy spent for the whole network is the sum of energies of all individual nodes.

The results are compared between secured dominating set network, unsecured dominating set network and general mobile ad hoc network.

The simulation results are drawn for different network sizes 20,30,40,50.

The results obtained are shown below.

Network size	Secured dominating set network	Un secured dominating set network	Secured mobile ad hoc network	General mobile ad hoc network
20	6043	4798	11114	10208
30	7368	6376	17432	15147
40	7924	7097	23432	20152

| 50 | 7449 | 6697 | 23854 | 20295 |

7.3. Constant path energy consumption

The above simulation results are compared with help of graph as shown below.

Constant Path Energy Consumption
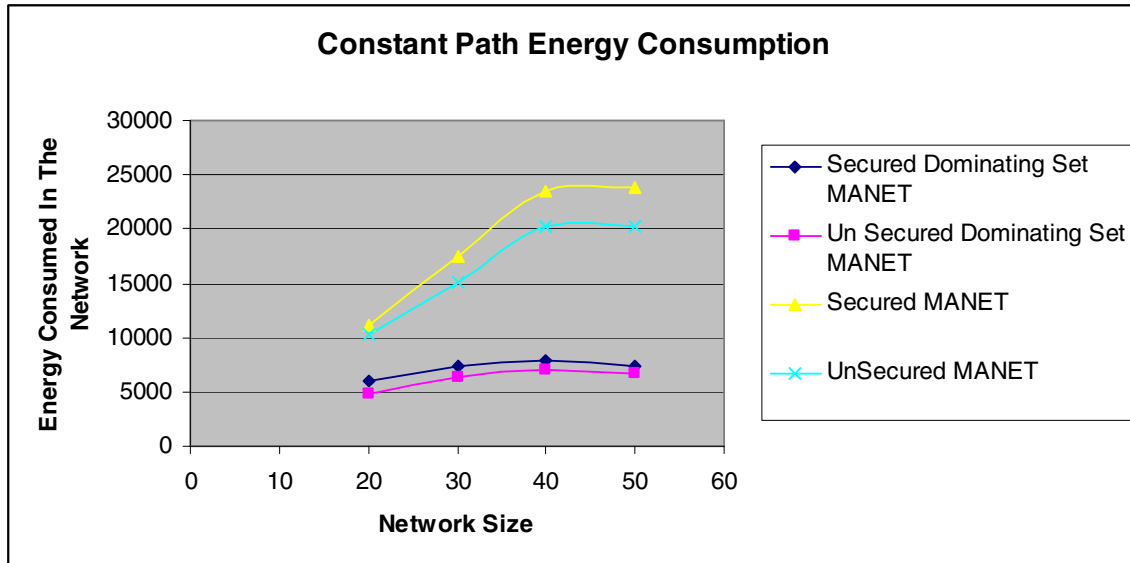
7.3. Constant path energy consumption

Discussions and conclusions from the fig 7.3: -

The conclusions that can be drawn based on the graph shown between secured dominating set network, unsecured dominating set network and general mobile ad hoc network with different network sizes are

- The energy consumed for unsecured dominating set network is smaller than all other networks.

- The energy spent for general mobile ad hoc network (with or without security) is nearly 4 times the energy spent for secured or unsecured dominating set network.

- The result also shows that as the size of the network increases, the energy level difference between secured and unsecured networks decreases.

- These results are similar to the results shown in fig 7.2.

58

7.4.4. Nodes Survived

Results are obtained for the number of nodes that survive after the simulation run based on the constant path energy calculation criteria. The results are shown for network sizes of 30 and 50 after the simulation runs till 50% of the whole network energy is consumed. The results are shown for both secured and unsecured dominating set networks.

The node surviving is calculated based on the energy left for that particular node after the simulation run. If the energy left for a node is less than a threshold value, it is taken as a dead node (did not survive), otherwise it is taken as survived node. The threshold value is taken as zero. The results of survived nodes for network size 30 are shown below.

Time Unit	Unsecured dominating set network nodes survived	Secured dominating set network nodes survived
10	30	30
20	30	29
30	30	29
40	30	29
50	30	29
60	30	27
70	30	27
80	28	27
90	24	21
100	24	19

110	24	18

7.4. Nodes survived in network size 30

The results in table 7.4 are drawn in the form of graph as shown below.

Nodes survived in Network Size 30
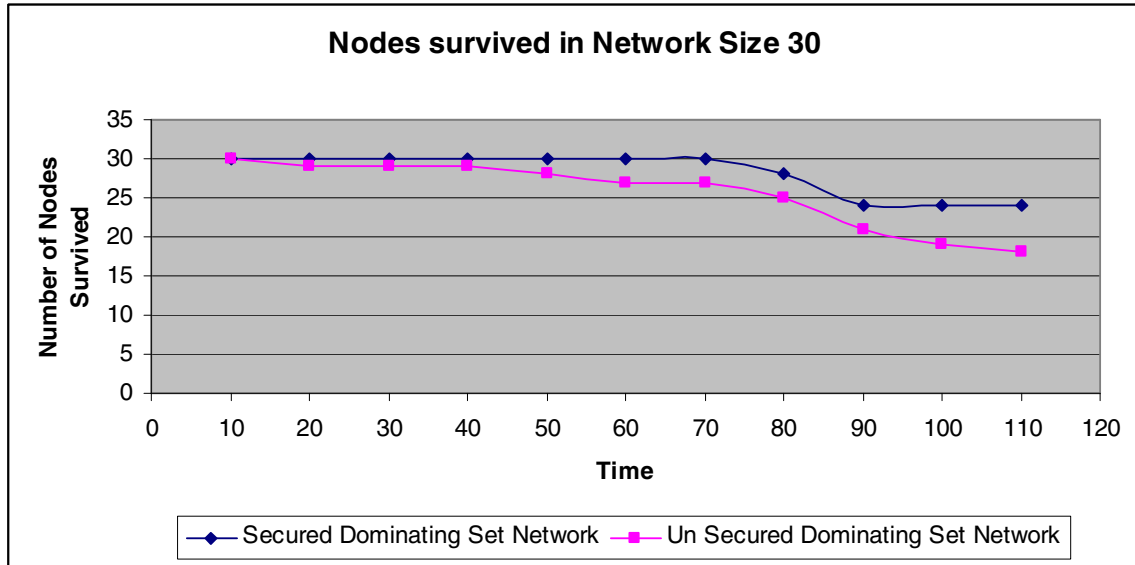
7.4. Nodes survived in network size 30

The results of survived nodes for network size 50 are shown below.

Time Unit	Unsecured dominating set network nodes survived	Secured dominating set network nodes survived
10	50	50
20	50	50
30	50	49
40	46	45

50	46	45
60	46	45
70	46	45
80	41	26
90	38	21
100	38	18
110	38	18

7.5.Nodes survived in network size 50

The results in table 7.5 are drawn in the form of graph as shown below.
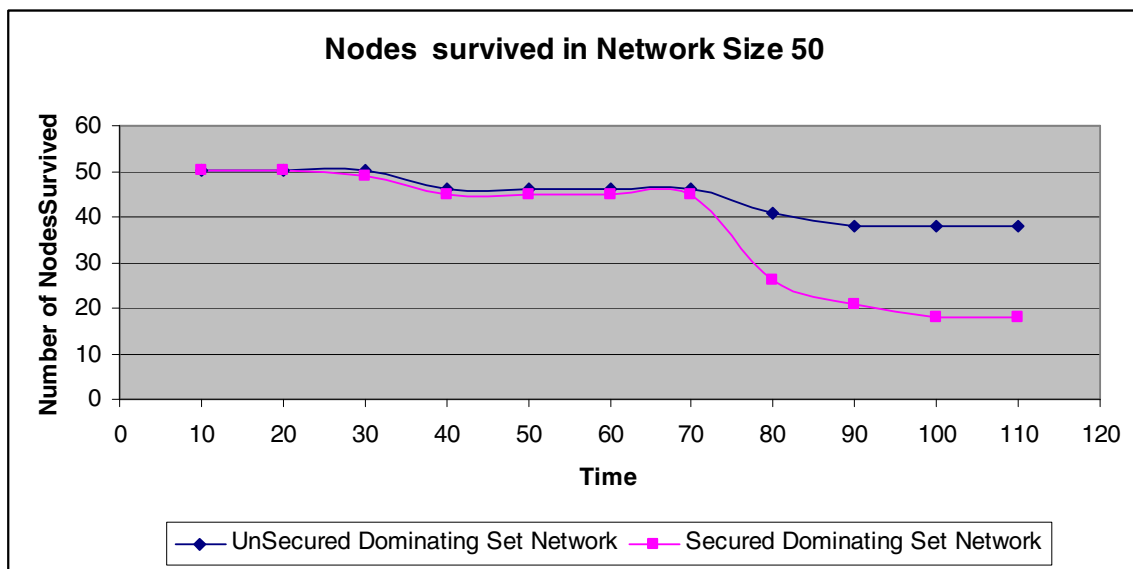

7.5. Nodes survived in network size 50

Discussions and conclusions from the fig 7.4 and Fig 7.5: -

- The Number of nodes surviving decreases as the network period increases.

- The nodes dying for unsecured dominating set network is greater than the secured dominating set network. This is due to the fact that a secured node is chosen as part of dominating set, every time the dominating set is constructed.

- The number of nodes surviving decreases very slowly at the beginning of the
  simulation and decrease rapidly as the simulation period progresses. This is due to
  the fact that almost each node in the network serves as part of the dominating set
  at different time periods during the simulation run.

CHAPTER VIII

FUTURE WORK

In this thesis we have proposed a mechanism for energy conservation while achieving security in a mobile ad hoc network using dominating sets. Simulation results show that the proposed approach results in energy being saved while achieving security. The proposed approach was compared to an non-dominating set approach. Our approach results in increased survivability of the network. Simulation results furthermore show that energy is saved even in a network where a node can control its signal range based on distance.

Future work may investigate prioritizing nodes in the dominating set or including additional constraints when calculating the dominating set. The incorporation of different security mechanisms with the dominating set approach may also be considered.

REFERENCES

[1]. Jie Wu and Hailan Li: "On Calculating Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks", *Proc. Third Int'l Workshop Discrete Algorithms and Methods for Mobile Computing and Comm*, pp. 7- 14, 1999.

[2]. Fei Dai, Jie Wu: "An extended localized algorithm for connected dominating set formation in ad hoc wireless networks". *IEEE Transaction on Parallel and Distributed Systems*, 15 pp. 908–920. 2004

[3] Jamil A. Shaikh, Julio Solano, Ivan Stojmenović, and Jie Wu: "New metrics for dominating set based energy efficient activity scheduling in ad hoc networks". In *Proceedings of the International Workshop on Wireless Local Networks* (WLN 2003), Bonn, Germany, October 2003.

[4]. Sameera Poduri and Gaurav S.Sukhatme: "Constrained coverage for mobile sensor networks". *In Proceedings of IEEE International Conference on Robotics and Automation,* 2004.

[5]. Chavalit Srisathapornphat, Chien-Chung Shen: "Coordinated Energy Conservation for Ad hoc Networks*",. Proceedings of IEEE International Conference on Communication*s, ICC 2002 Volume: 5, 2002.

[6]. Zhengming Shen, Johnson Thomas:" Location-Triggered Routing Protocol in Mobile Ad Hoc Networks". *Proceedings of IEEE International Symposium on Network Computing Applications,* pp. 261-268, 2004

[7]. Laurent Eschenauer and Virgil D.Gilgor, V.D: "A key-management scheme for distributed sensor networks", *Proceedings of the ACM conference on Computer and Communication Security*, 2002.

[8]. Tracy Camp,Jeff Boleng and Vanessa Davies: "A Survey Of Mobility Models For Ad Hoc Network Research", *Wireless Communication and MobileC omputing(WCMC)*, special issue on Mobile ad hoc Networking Research, vol. 2, no. 5, pp. 483-502, 2002.

[9]. Jie Wu, Fei Dai, Ming Gao, and Ivan Stojmenovic: "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks", *Journal of Communication and Networks*, March 2002.

[10].Elizabeth Royer and Choy Keong Toh: "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", *IEEE Personal Communications Magazine*, April 1999, pp.46-55.

[11].Zygmunt J Hass and Marc R Pearlman,"The Performance of Zone Routing Protocol in Reconfigurable Wireless Networks", *IEEE JSAC Issue on Ad Hoc Networks,* June 1999.

VITA

Madhusudhan Jakkidi

Candidate for the Degree of

Master of Science

Thesis: SECURED ENERGY OPTIMIZATION IN MOBILE AD HOC NETWORKS

Major Field: Computer Science

Biographical:

Personal Data

Education: Bachelor of Science, Computer Science, JNTU, India, May 2003.

Completed the Requirements for the Master of Science degree at Oklahoma State University in December, 2005.

Experience: Graduate Assistant, December 2003 – August 2005.

Professional Memberships: ACM

Research Interests: Sensor/Wireless Networks, Compiler Design.

Name: Madhusudhan Jakkidi   Date of Degree: December, 2005

Institution: Oklahoma State University   Location: Stillwater, Oklahoma

Title of Study: SECURED ENERGY OPTIMIZATION IN MOBILE AD HOC
                NETWORKS

Pages in Study: 65   Candidate for the Degree of Master of Science

Major Field: Computer Science

Scope and Method of Study:
Due to limited resources, it is essential to optimize energy consumption in mobile ad hoc networks. There exist different ways to optimize energy usage for mobile ad hoc network. Our thesis proposes usage of secured mobile dominating sets for efficient optimized use of energy in a mobile ad hoc network. Existing approaches for energy optimization use different techniques. Some of them include techniques such as dominating sets, communication reduction between nodes and concept of balanced forces. Energy optimization in dominating set based approaches is carried out by the use of some special nodes, which are the only working nodes in the network. The dominating set based approach can be modified to improve network life by improving energy consumption per node. Further more these approaches do not provide security.

Approach, Findings and Conclusions:
In this thesis we propose the concept of mobile dominating set, which updates the dominating set nodes at regular intervals based on the nodes mobility and the network topology constraints. This further improves the network life by utilizing the maximum energy per node. Furthermore, we propose a secure dominating set mechanism, which provides security with minimum energy expenditure for mobile dominating sets. Our approach starts by constructing the dominating set based on the initial composition between two networks, security key network and mobile ad hoc network, and then depending on the nodes mobility, decrease in energy levels of dominating set nodes, network topology constraints; it recalculates the dominating set with new mobile network links to include secured communication between the dominating set nodes. The results are compared with unsecured dominating set networks, secured mobile ad hoc networks and general mobile ad hoc networks. The results show that the energy consumed for each network in increasing order as unsecured dominating set networks, secured dominating set networks, general mobile ad hoc networks and secured mobile ad hoc networks. It also shows that the narrow difference in energy levels for unsecured dominating set network and secured dominating set network decreases as the network size increases. It also shows that there is very small difference of average path lengths between secured dominating set network and unsecured dominating set network. The results also show that the number of nodes survived decreases as the network period increases with improved network life per each node.

ADVISER'S APPROVAL: Dr. Johnson P Thomas