Volume 1,Issue-1,December-2011

International Journal of Advanced Research in Computer Science and Software Engineering

A Monthly Scientific Journal of Computer Science

www.ijarcsse.com

Research paper

Available online at www.ijarcsse.com

Measurement Based Performance of Reactive and Proactive Routing Protocols in WMN

Shivlal Mewada*
Institute of Computer Science
Vikram University,
Ujjain-INDIA

Umesh Kumar Singh
Institute of Computer Science
Vikram University,
Ujjain-INDIA

***Abstract*— Wireless mesh network is an advanced form of wireless network. Wireless Mesh networks is the key technology for represent an emerging wireless networking technology that promises wider coverage than traditional wireless LANs and lower development and operation cost than 3G cellular networks. Wireless mesh networks can be implemented with various wireless technologies including IEEE 802.11. Routing is a key factor for transfer of packets from source to destination. That is Routing is a process of determining a path between source and destination upon request of data transmission. We have discussed the related issues and advantages and disadvantages of Reactive and Proactive routing protocol in WMNs. In this paper we mainly presented measurement based performance of reactive protocols and Proactive Protocols in wireless mesh networks.**

***Keywords*— WMNs, Reactive protocols, Proactive protocols.**

I. INTRODUCTION

Wireless Mesh Networks have emerged as a key technology for next-generation wireless networking. WMNs is the key technology for represent an emerging wireless networking technology that promises wider coverage than traditional wireless LANs and lower development and operation cost than 3G cellular networks. The most commonly used technology in day to day life is desktops, laptops, PDA's, Pocket PC's, Phones. WMNs can also be used in other applications such as broadband, networking, enterprise networking building automation, and neighbourhood networks. Although by definition a WMN is any wireless network having a network topology of either a partial or full mesh topology, practical WMNs are characterized by static wireless relay nodes providing a distributed infrastructure for mobile client nodes over a partial mesh topology. WMNs are multi-radio, multi-hop network with the ability of dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (an ad-hoc network) [1, 2]. WMNs standard is defined as IEEE 802.11; it is one such solution to provide wire free network communication. The field of Wireless Networking has been experiencing an explosive growth proportional to the Internet. Since, the users and service providers enjoy the flexibility and accessibility of network any-where, any-time. Wireless Networks have many advantages, which come bundled along with lot of security issues. The major risk involved is that the information is transmitted through air [3]. The Routing protocols in WMN are divided into reactive and proactive & hybrid protocols. In reactive protocols, a route path is established only when a node has data packets to send that is Reactive routing that means discovers the route when needed. Proactive routing that means route available immediately and Hybrid routing that means combination of both, such as proactive for neighbourhood, reactive for far away. The common routing needs of any routing protocol are scalability, reliability, throughput, load balancing, and congestion control. The unique routing metrics of WMN protocols are classified into Expected number of Transmissions, Expected Transmission time, Weighted Cumulative ETT (WCETT) [4]. In the early stages, WMN used many of the Ad-hoc protocols for routing. But these protocols does not follow routing metrics, so it unsuccessful to achieve reliability, scalability, throughput, load balancing, congestion control over WMN.

II. CLASSIFICATION OF ROUTING PROTOCOLS

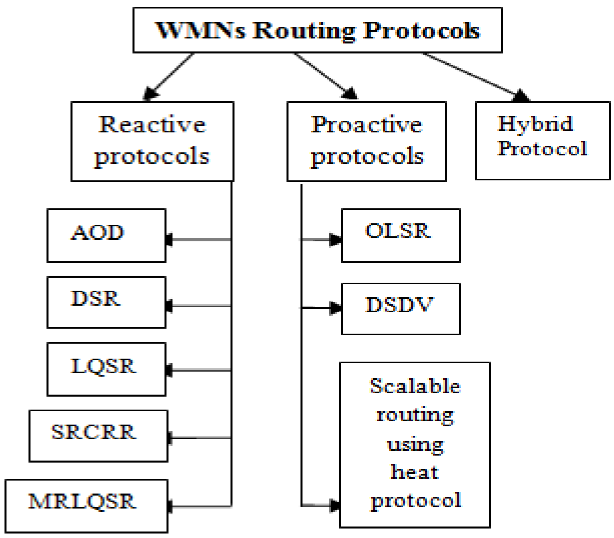

Figure: 1 Classification of Routing protocols in WMNs

There exists a large number of wireless mesh network routing protocols. They can be broadly classified into three categories as shown in Figure 1. In this study, we focus on two types of protocols: Proactive and Reactive Routing Protocols.

III. Analysis of Reactive Routing Protocols

In reactive routing protocols, the route is calculated only when a node needs to send data to an unknown destination. Thus, route discovery is initiated only when needed. This saves overhead in maintaining unused routes. However, this may lead to larger initial delays. During route discovery, the query is flooded into the entire network and the reply from the destination (or intermediate nodes) sets up the path between the source and destination. The Reactive protocols are classified into Ad-hoc on Demand Distance Vector, Dynamic Source Routing, SRCRR, Link Quality Source Routing, and Multi radio Link Quality Source Routing.

A. DSR Routing Protocol

Dynamic source routing protocol (DSR) is a reactive protocol (on demand routing protocol) that is known as simple and efficient, specially designed for the multi-wireless mesh network. Often called "on-demand" routing protocol as it involves determining the routing on demand unlike the pro- active routing protocols that has periodic network information. This means that it discovers the route from source to the destination if required. DSR was designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks, by eliminating the periodic table-update messages used in proactive protocols. DSR protocol is based on two mechanisms: route discovery and route maintenance.

Route Discovery: Route discovery is the process of DSR uses to find the route and to transmit the data from a source to destination where the source node is unaware of the destination route. For example [5]

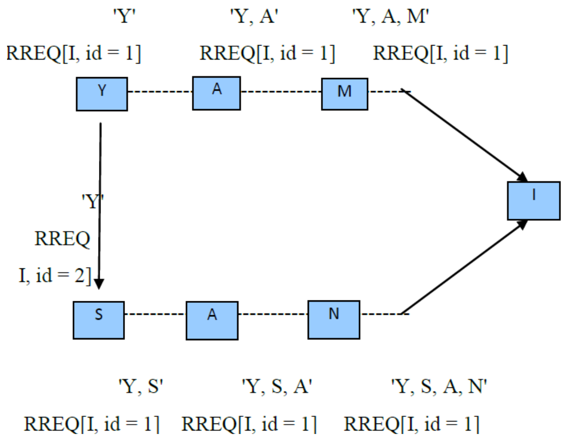

Figure: 2 Route Discovery Process

Let us assume node 'Y' wants to establish a route to node 'I'.

- Initially node 'Y' transmits 'RREQ' (Route Request) will usually be received by all the participating nodes in the network.
- This Route request contains information about the source and the destination along with unique request identification (id = 1 and id = 2 respectively in the considered figure).
- RREQ even maintains the information about all the intermediate nodes passed by while reaching the destination.
- Once the destination receives the RREQ packet then it will send the 'RREP' (Reply Route) to the source node 'Y'.
- "RREP" contains a copy of the route information of the RREQ then the source cache information to use in further communication process.

Route Maintenance: DSR protocol implements the route maintenance mechanism while communicating the packets from source to destination. But when the communication link between the source and the destination is broken or else a change in network topology is noticed. It will lead to failure of the communication between source node and destination node. In this scenario DSR protocols uses the route mechanism, to detect any other possible known route towards the destination to transmit data. If the route maintenance fails to find an alternative known route to establish the communication then it will invoke the route discovery to find the new route to destination [5].

Advantage: The DSR protocol are: guaranteed loop-free routing, Nodes can store multiple paths to destination., support for use in networks containing unidirectional links, use of only "soft state" in routing, and rapid recovery when routes in the network change.

Disadvantage: One of the major disadvantages of DSR protocol is in implementing the route discovery process. Source will transmit the RREQ messages to all the neighbouring nodes to find the route to destination. It is fair and good when there are few nodes in the network, it will easily find a route and it can receive a RREP message from the desired destination. But if in case the network size is very high and participating nodes are numerous, then there will be a possibility to have so many routes to the destination. It may result in the reply storms this may cause collision of packets and it may increase the congestion at the nodes while sending reply [6]. Another disadvantage of it is not scalable for the WMN, it is not suitable for the large networks, When the traffic load is high congestion will occur and it has poor mechanisms for controlling congestion, When network size, node mobility, network load increases then delay rate increases more when compared to other protocols.

B. Ad-hoc on Demand Distance Vector

Ad-hoc on Demand Distance Vector routing protocol is developed as an improvement to DSDV routing algorithm. The purpose of DSDV is to reduce the number of broadcast messages sent throughout the network and reduces the routing overhead, but introduces some initial latency due to the on demand route setup. This is achieved by discovering routes on-demand instead of keeping complete up-to-date route information. AODV uses a simple request–reply mechanism for the discovery of routes. AODV protocol mainly involves 3 packets. They are [7]:

1. The route request (RREQ) is mainly used for the establishment of packets from source to destination.
2. The route reply (RREP) is sent by the destination to the source after the establishment of route.
3. The route error (RERR) is sent by intermediate node or destination in 2 conditions.

- When there is no path to the destination.

- When the link breaks in the valid path to the destination.

The source will first broadcast the RREQ packet by keeping the source and destination IP address in the RREQ packet.

The packet will be received by the intermediate node and the intermediate node will check whether there is a valid route to the destination or not. If it has, then the RREQ is again rebroadcasted otherwise route error will be sent to the source. The duplicates of route request packets can be discarded by route request id present in the RREQ packets. When the destination gets the route request packets in different paths it considers only one path as a valid path i.e. the path along which it receives the route request first, other paths are discarded. Destination sends the RREP packet back to the source with the path details from source to destination [8].

Advantages: This protocol is reliable for the wireless mesh networks. AODV is loop free and does not require any cartelized system to handle routing process for wireless mesh networks.

Disadvantages: Shortest path may be lost due to traffic during the path discovery process [8]. AODV do not utilize any congestion control or avoidance mechanism to balance traffic load [8]. The delivery ratio of AODV drops dramatically from more than 90% to about 28% when the number of connections increases from 10 to 50 [9].

C. SrcRR Protocol

SrcRR protocol is similar to DSR with link caches: SrcRR is a reactive routing protocol with source routed data traffic. SrcRR protocol mainly functions with the ETX metric, transmission bit-rate and transient bursts.

Every node running SrcRR maintains a link cache, which tracks the ETX metric values for links it has heard about recently [8, 10]. Whenever a change is made to the link cache, the node locally runs Dijkstra's weighted shortest path algorithm on this database to find the current, minimum-metric routes to all other nodes in the network. To ensure only fresh information is used for routing, if a link metric has not been updated within 30 seconds it is dropped from the link cache [8, 10]. When a node wants to send data to a node to which it does not have a route, it floods a route request. When a node receives a route request, it appends its own node ID, as well as the current ETX metric from the node from which it received the request, and rebroadcasts it. A node will always forward a given route request the first time it receives it. If it receives the same route request again over a different route, it will forward it again if the accumulated route metric is better than the best metric it has forwarded so far. This ensures that the target of the route request will receive the best routes. When a node receives a route request for which it is the target, it reverses the accumulated route and uses this as the source-route for a route reply. When the original source node receives this reply, it adds each of the links to its link cache, and then source-routes data over the minimum-metric path to the destination. When a SrcRR node forwards a source-routed data packet, it updates its entry in the source route to contain the latest ETX metric for the link on which it received the packet. This allows the source and destination to maintain up-to date link caches, and discover when a route's quality has declined enough that an alternate route would be better.

Advantages: This protocol is reliable for the WMN, it is Increases throughput for the WMN, it is manage traffic balancing and control congestion control.

Disadvantages: This protocol is not scalable for wireless mesh networks. SrcRR is not likely to scale to more than a few hundred nodes.

D. Link Quality Source Routing

Link Quality Source Routing is a modified version of DSR and LQSR aims to select a routing path according to link quality metrics that is aims to select a better route using link quality metrics in single-radio, single-channel wireless networks. LQSR implements the basic functionalities of DSR including route discovery and route maintenance. The protocol was developed by Microsoft for use with their Mesh Connectivity Layer (MCL) technology, which facilitates the interconnection of computers into a mesh network using WiFi or WiMax wireless service. It is located between layer 2 (link layer) and layer 3 (network layer) of the standard ISO/OSI model. Three performance metrics, i.e., the expected transmission count (ETX) [11], per-hop RTT, and per-hop packet pair are implemented separately in LQSR.

The performance of the routing protocol with these three performance metrics is also compared with the method using the minimum hop-count. For stationary nodes in WMNs, ETX achieves the best performance, while the minimum hop-count method outperforms the three link quality metrics when nodes are mobile. The reason is that, as the sender moves, the ETX metric cannot quickly track the change in the link quality. This result illustrates that the link quality metrics used in [12] are still not enough for WMNs when mobility is concerned. Better performance metrics need to be developed, and routing protocols integrating multiple performance metrics are necessary for wireless mesh networks.

Advantages: Increases throughput as it considers the ETX metric for routing. It is managing the congestion control and traffic balance.

Disadvantages: ETX, RTT, only considers loss rates on the links and not their data rate. Scalability is not provided for wireless mesh networks. ETX is designed to give preference to shorter paths over longer paths, as long as loss rates on the shorter paths are not significantly higher.

E. Multi radio Link Quality Source Routing

A new routing protocol for multi-radio multi-channel WMNs called Multi-Radio Link Quality Source Routing. Multi radio Link Quality Source Routing also a reactive routing protocol for wireless mesh networks. MR-LQSR is a combination of the LQSR protocol [13] with a new metric that we call WCETT. LQSR is a source-routed link-state protocol derived from DSR [14]. A link-state protocol consists of four components:

1. A component that discovers the neighbours of a node.
2. A component that assigns weights to the links a node has with its neighbours.
3. A component to propagate this information to other nodes in the network.
4. A component that uses the link weights to find a good path for a given destination. In other words, the link weights are combined to form a path metric.

The first and the third components of MR-LQSR are similar to the corresponding components in DSR. We will not discuss them further except to briefly point out some implementation- related issues later in the paper.

The second and the fourth components of MR-LQSR are very different from DSR. DSR assigns equal weight to all links in the network. The path metric is simply the sum of link weights along the path. Thus, DSR implements shortest-path routing. Instead of shortest-path, MR-LQSR uses the WCETT metric. WCETT can be calculated as follows:

$$WCETT_p = (1-\alpha) \times \sum_{i \in p} ETT_i + \alpha \times \max_{1 \le j \le k} X_j$$

Where β is a tunable parameter subject to 0≤β≤ 1. Xj is the sum of transmission times of hops on channel j. The MAX1≤j≤ k Xj component in the equation counts the maximum number of times.

Advantages: This protocol is more reliable for the WMN, it is Increases throughput for the WMN, and it is handle traffic balancing and control congestion control.

Disadvantages: Scalability is not provided because adding a new node in a path will increase the weight of the link as extra hope is needed to reach the destination.

IV. Analysis of Proactive Routing Protocols

In these types of routing protocols, each node maintains a table of routes to all destination nodes in the network at all times. This requires periodic exchange of control messages between nodes. Since the route to every destination already exists, there is little or no initial delay when first sending data. However, periodic control traffic competes with data transfer to gain access to the channel. The Proactive protocols are classified into Destination Sequence Distance Vector, Optimized Link State Routing, Scalable routing using heat protocols.

A. Destination Sequence Distance Vector:

DSDV is a proactive type of routing protocol. DSDV table-driven DV routing scheme for MANET, DSDV based on the Bellman-Ford algorithm with adaptations that are specifically targeted for mobile networks. The Bellman-Ford algorithm uses the distance vector approach, where every node maintains a routing table that records the "next hop" for every reachable destination along the shortest route and the minimum distance (number of hops). Whenever there is any change in this minimum distance, the information is reported to neighbouring nodes and the tables are updated as required [15] To make this algorithm adequate for mobile ad hoc networks, DSDV added a sequence number with each distance entry to indicate the freshness of that entry. A sequence number is originated at the destination node and is incremented by each node that sends an update to its neighbours. Thus, a newer routing table update for the same destination will have a higher sequence number. Routing table updates are periodically transmitted throughout the network, with each node updating its routing table entries based on the latest sequence number corresponding to that entry. If two updates for the same destination have identical sequence numbers but different distances, then the shorter distance is recorded. The addition of sequence numbers removes the possibility of long-lived loops and also the "counting-to-infinity" problem, where it takes a large number of update messages to ascertain that a node is not reachable [15].

- It solved the routing loop problem
  1. Each entry in the routing table contains a (sequence no) to measure the freshness of a route
  2. The number is generated by the destination, and the emitter has to send out the next update with this number
  3. Routing info is distributed between nodes by sending full dumps
  4. Infrequently and smaller incremental updates more frequently.
  5. If a router receives new information, then it uses the latest sequence no.
- Old routes are deleted automatically.

Advantages

- Suitable for small number of nodes,
- Other protocols have borrowed similar techniques (e.g. AODV).
- It also loop free path.

Disadvantages:

- No formal specification, no significant commercial implementation
- But many improved forms of this algorithm have been suggested and used
- Need regular update of its routing tables, (battery power problem)
- Congestion control is bad
- not suitable for highly dynamic networks

B. Optimized Link State Routing

OLSR protocol is a proactive routing protocol. The Optimized Link State Routing (OLSR) protocol was first introduced in [16]. The current OLSR Version 11 is the definitive RFC 3626. It provides optimization of a pure link state algorithm tailored to the requirements of a mobile wireless LAN (OLSR protocol optimized for MANET but can also be used in WMNs). The concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique provides two key optimizations [16]. First, it reduces the size of the control packets, that is, instead of all links, it declares only a subset of neighbouring links designated as the MPRs. Secondly, flooding of the control traffic is minimized by using only the selected nodes to propagate its messages in the network. Only the MPRs of a node retransmit its broadcast messages. Such procedures substantially reduce the message overhead as compared to pure flooding mechanisms where every node re-transmits each message when it receives the first copy of the packet.

Advantages:

- Proactive -> no route discovery delay associated with finding a new route.
- Throughput; Better when compared to DSDV.
- Routing overhead is greater than that of a reactive protocol, but does not increase with the number of routes being used.
- Default and network routes can be injected into the system.

- Timeout values and validity information are used

Disadvantages:

- It is not scalable for wireless mesh networks.
- Requires sufficient CPU power to compute optimal paths in the network.
- In the typical networks where OLSR is used.

C. Scalable routing protocols

Scalable routing is a proactive (table-driven) type of routing protocol for WMNs. In case of scalable routing protocol the gateways are modelled as heat sources which create a temperature field in the network. The higher the temperature of a node, the closer it is to an access point. Using these fields, packet forwarding is fairly simple: packets are forwarded along the nodes with the highest temperature until they eventually reach any heat source (an Internet gateway). It means that every node calculates its own temperature by only evaluating the temperature of its direct neighbours. This makes protocol particularly scalable since no flooding of messages is required. Whenever an entry is added, removed, or changed, the temperature value is re-computed [8].

The key idea of HEAT is to provide scalability (with regard to protocol overhead) and robustness (with regard to link and node failures). Due to the local message exchanges, this method scales with the number of neighbours per node. Robustness is achieved by assigning the temperature values such that routes through network areas with high redundancy (in terms of node and link redundancy) are preferred. The more neighbours with high temperatures, the higher is the temperature of a given node [17].

The algorithm calculates the temperature tfinal of a node as follows: In a first step, the node sorts its neighbours based on their temperatures Θ_i, $i \in \{0, ..., n\}$ in ascending order (line 1) into an array a. Then, it iterates over a accumulating the temperature of the next neighbour to the sum of the temperatures of the previous neighbours tj until the temperature of the next neighbour is less than the accumulated temperature (line 4). In each step j, the value tj+1 is calculated as follows (line 5): The difference between the temperature of the currently considered neighbour, denoted by a[j], and the temperature accumulated so far, tj, is calculated. Then, this difference is multiplied by the conductivity parameter k, and the result is added to the temperature accumulated so far, denoted by tj.

Algorithm Temperature Field Calculation Function:

```
1: α = sortascending’ (Θ0, ..., Θn)
2: j = 0
3: tj = 0
4: while tj < α[j] do
5:        tj+1 = tj + (α[j] − tj) · k
6:        j = j + 1
7: end while
8: tfinal = tj
```

Advantages:

- This protocol is reliable for the WMN, it is Increases throughput for the WMN
- Provides scalability with less resource consumption.
- Packets can be easily routed by considering the heat of the nodes near to gateways.

Disadvantages:

- Scalable routing does not utilize any congestion control or avoidance mechanism to balance traffic load.

External environment heat can effect the gate which provides gate ways.

Protocol	DSR	AODV	SrcRR	LQSR
Scalability	No	No	No	No
Reliability	Yes	Yes	Yes	Yes
Throughput	Decreases as mobility increases	Poor for more than 20 mobile nodes	Yes	Yes
Load balancing	No	No	Yes	Yes
Congestion control	No	No	Yes	Yes

Protocol	MR-LQSR	DSDV	OLSR	Scalable Routing
Scalability	No	No	No	Yes
Reliability	Yes	Yes	Yes	Yes
Throughput	Yes	Decreases with mobility	Better when compared to DSDV	Yes
Load balancing	Yes	No	No	No
Congestion control	Yes	No	No	No

Figure: 3 Analysis Results of Reactive and Proactive Protocols in Wireless Mesh Networks.

V. Recommendation

A network will get a better performance if these factors are considered accurately the Scalability is most challenging factor that has to be considered in all the protocols that have been used till now. The recommendations mentioned above would help improve performance of the system for wireless mesh networks.

VI. Conclusion

Every reactive and proactive routing protocol has its own advantages and disadvantages. This paper effectively classifies different protocols by considering different factors. We have analysed that among all the protocols Scalability is the most challenging factor that has to be considered. In these various protocols we can select an effective protocol to our network by looking the behaviour of the protocol at various conditions and if more emphasis is given on the improvement of scalability factor we can help in enhancing the overall performance of the entire network.

REFERENCES

[1]. I. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks," IEEE Communications Magazine, vol. 43, No. 9, pp. 23–30, 2005.
[2]. Ian F. Akyildiz a, Xudong Wang b,*, Weilin Wang" Wireless Mesh Networks: a survey",@- IEEE, 1 jan-2007.
[3]. Olatunde O. Abiona , Yu Cheng " Mobile Agent based Authentication for Wireless Network Security",© IEEE 2008
[4]. Wireless mesh networks architectures and protocols by Yan Zhang.
[5]. D. Johnson, Y. Hu, D. Maltz "The Dynamic Sorce Routing Protocol (DSR) for Mobile Adhoc Networks for Ipv4" NWG, 2007.
[6]. S. Ahmad, I. Awan, A. Waqqas, B. Ahmad. "Performance Analysis of DSR and Extended DSR protocols" ICON-AICMS, pp.191-196, 2008.
[7]. Multi-Linked AODV Routing Protocol for Wireless Mesh Networks, IEEE GLOBECOM 2007.
[8]. V.Srikanth, A.Chenchu Jeevan, B.Avinash, T.Sai kiran, S.Suresh Babu, "A Review of Routing Protocols in Wireless Mesh Networks (WMN)", IJCA (0975–8887) Volume 1 – No. 11, pp.47-51, ©2010.
[9]. Study of Distance Vector Routing Protocols for Mobile Ad Hoc Networks IEEE International Conference on Pervasive Computing and Comm. (PerCom'2003)
[10]. Tropos networks technology whitepaper, May 2003
[11]. D.S.J. De Couto, D. Aguayo, J. Bicket, R. Morris, A high-throughput path metric for multi-hop wireless routing, in: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), 2003, pp. 134–146.
[12]. R. Draves, J. Padhye, B. Zill, Comparisons of routing metrics for static multi-hop wireless networks, in: ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM), pp. 133–144, August 2004.
[13]. R. Draves, J. Padhye, and B. Zill. The architecture of the Link Quality Source Routing Protocol. Technical Report MSR-TR-2004-57, Microsoft Research, 2004.
[14]. D. B. Johnson and D. A. Maltz. Dynamic source routing in ad-hoc wireless networks. In Mobile Computing. Kluwer Academic Publishers, 1996.
[15]. http://web2.blogtells.com/2008/09/17/proactive-routing-protocols-destination-sequenced-distance/
[16]. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "OLSR Protocol for Ad Hoc Networks", IEEE INMIC, pp. 62–68, Dec 2001, last accessed on Oct 2005.
[17]. Rainer Baumann, Simon Heimlicher, Vincent Lenders†, Martin May," HEAT: Scalable Routing in Wireless Mesh Networks Using Temperature Fields" last accessed on august 2011.