Mobile Ad-Hoc Service Grid – MASGRID

Imran Ihsan, Muhammad Abdul Qadir, and Nadeem Iftikhar

***Abstract*—** Mobile devices, which are progressively surrounded in our everyday life, have created a new paradigm where they interconnect, interact and collaborate with each other. This network can be used for flexible and secure coordinated sharing. On the other hand Grid computing provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities. In this paper, efforts are made to map the concepts of Grid on Ad-Hoc networks because both exhibit similar kind of characteristics like Scalability, Dynamism and Heterogeneity. In this context we propose "Mobile Ad-Hoc Services Grid – MASGRID".

***Keywords*—**Mobile Ad-Hoc Networks, Grid Computing, Resource Discovery, Routing

I. Introduction

GRID is a flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources—what is being referred as *"Virtual Organizations"* [1]. Grid uses Globus Architecture for its proper functioning. Globus APIs use high computational power machines and require lot of free space for their installation. Due to limited abilities of mobile devices in term of computational power and storage, it is not possible to use the Globus Architecture on every type of mobile devices. Therefore there is need of a light weight Globus that we may call as Mini-GT or Mobile-GT, so that Ad-Hoc networks can be used as Grid. Through MASGRID, we can create a small scale resource sharing Grid, without involving the overheads of Globus. It uses the underlying connectivity and routing protocols defined by MANET, in order to perform resource discovery and access.

II. Mobile Ad-Hoc Network

MANET is an autonomous collection of mobile users (nodes) that communicate over relatively bandwidth-constrained wireless links. Due to mobility, the network topology may change rapidly and unpredictably over time. [2] The network is decentralized, where network organization and message delivery must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

A. *Characteristics of MANET*

The mobility of small, wireless devices creates tremendous opportunities to utilize the grid, and to enhance the services available on the grid. These mobile devices differ from typical grid servers and clients in terms of communication and computation abilities, limited power constraints, small screen, and the transitive nature of their connection to network infrastructures but they share common characteristics like;

Heterogeneity: Heterogeneity in mobile devices exists both in hardware and software form as there are number of different wireless devices like Mobile Phone, Laptops, PDAs etc. Wireless networks are also heterogeneous in terms of administrative policies. Since the network will be owned by different organizations. [3]

Dynamism: Mobile networks exhibit several kinds of dynamism such as adding a new node to the network without human involvement beyond placing the new node within the radio range of the existing node and afterwards its automatic configuration, no reliance on network infrastructure, free node mobility and ease of interaction with the changing set of nearby resources. The underlying protocols of these networks should also provide APIs that use algorithms to take advantage of rich and changing network topologies. [3]

Scalable: Scalability means; to group nodes into an addressing and routing hierarchy that inhibits movement. But the existing MANET routing systems use flooding system to find a destination. Thus Global Flooding allows node to attach to the network anywhere but it scales badly beyond few hundred nodes. [3]

B. *Secure Connectivity in MANET*

Ad-hoc network is as a community of autonomous devices that collaborate with each other. The control and authentication aspects are required for the establishment of ad-hoc communities. A policy-based approach can be used to establish ad-hoc communities by regulating and governing the membership of the community. The concept of certification authorities (CAs), and attribute authorities (AAs) is not feasible due to non-availability of high computational devices at all times. Therefore Ad-Hoc networks rely on the concept of "Peer Trust" [4] where devices rely on peers to relay or provide security information in the form of assertions.

Manuscript received April 7, 2005.

Imran Ihsan is with Muhammad Ali Jinnah University, Islamabad Campus, Jinnah Avenue (Blue Area) Islamabad, Pakistan (phone: 92-333-5118897; e-mail: iimranihsan@gmail.com).

Muhammad Abdul Qadir is with Muhammad Ali Jinnah University, Islamabad Campus, Jinnah Avenue (Blue Area) Islamabad, Pakistan (phone: 92-300-5011600; e-mail: aqadir @ jinnah.edu.pk).

Nadeem Iftikhar is with Muhammad Ali Jinnah University, Islamabad Campus, Jinnah Avenue (Blue Area) Islamabad, Pakistan (phone: 92-300-5164815; e-mail: nadeem @ jinnah.edu.pk).

C. *Routing in MANET*

A MANET uses multiple hops where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host [5]. Due to frequently change in node locations, topology in is highly dynamic. Therefore traditional routing protocols can no longer be used in such an environment. New routing protocols that can handle the dynamic topology by facilitating fresh route discoveries are developed and are differentiated into three main groups namely Proactive, Reactive and Hybrid.

Proactive Routing Protocols are traditional distributed shortest-path protocols that maintain routes between every host pair at all times. Examples are DSDV (Destination Sequenced Distance Vector) [6], OLSR (Optimized Link State Routing) [7]

Reactive Routing Protocols determine route if and when needed. Route discovery is initiated by the Source in order to discover the destination. Some of reactive protocols include DSR (Dynamic Source Routing) [8], AODV (Ad Hoc On-Demand Distance Vector Routing) [9], PAR (Power-Aware Routing) [10], SSA (Signal Stability Based Adaptive Routing) [11] and many more.

Hybrid Routing Protocols are the combination of both Proactive and Reactive protocols. In these protocols, Proactive protocols are used up to certain hops and beyond that Reactive protocols are used. Examples are ZRP (Zone Routing Protocol) [12, 13, 14] etc.

III. Mobile Grid Services

Grid service is a Web service that provides a set of well-defined interface and that follows specific conventions. The interfaces address discovery, dynamic service creation, lifetime management, notification, and manageability; the conventions address naming and upgradeability [12]. Two other important issues, authentication and reliable invocation, are viewed as service protocol bindings that must be addressed.

When we take the Grid Services on mobile devices, it becomes a real challenge to deploy such kind of core Grid services and their requirements in terms of space and computational power, especially in case of hand-held devices. Therefore, there is a need of altering this Grid Service concept a bit, when we map the Grid on Ad-Hoc networks. We need to use the under-laying connectivity and routing protocols that exist on Ad-Hoc networks in order to develop Mobile Ad-Hoc Services Grid – MASGRID. Thus MASGRID is a dynamic, secure, coordinated resource sharing among mobile devices and can be referred as "*Mobile Virtual Organizations*

IV. Mobile Ad-Hoc Services Grid Architecture

MASGRID Architecture as shown in Fig 1 uses mobile network underlying protocols to provide resource discovery and its access. Thus the architecture uses two services known as Resource Discovery Service – RDS and Resource Access Service – RAS (as explained later). It also contains a Resource Look-Up Table – RLT that is similar to a routing table (explained later).

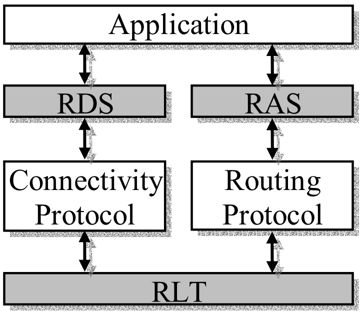

Fig 1: MASGRID Architecture

A. *Node Authentication*

Each mobile node gets authenticated using the concept of "Peer Trust" [4] to establish link. An ad-hoc community specification, namely "*doctrine*" [4], is used to define the roles of participants, the rules (or policies) governing their behavior in terms of authorizations, obligations, etc. and constraints. Doctrines are specified by some issuers. The doctrine can be used to instantiate several communities with different participants provided that all of them trust issuer to issue the doctrine.

B. *Node Service*

Each mobile device that enters the Trusted Mobile Grid becomes a Node Service. Node service publishes itself on the Grid, by making a packet containing the Node Service in particular format and broadcasting this packet to its peer (one hop) devices using the underlying routing protocol.

The packet is <servicedata> that comprises **<N, SN, SD, SDD, PTYPE, [GSR], [GSH]>** as shown in Fig 2.

- **N:** <Node> Name
- **SN:** <Service> Name
- **SD:** <Service> Data
- **SDD:** <Service> Data Description
- **PTYPE:** <Port> type
- **GSR:** Grid <Service> Reference
- **GSH:** Grid <Service> Handler

[ ] ➔Optional

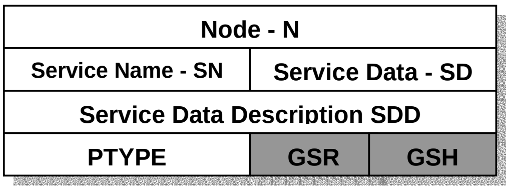

Fig 2: <servicedata> packet

C. *Resource Look Up Table*

Every node maintains a Lookup table which contains all the fields that are defined in Node service <servicedata> format. Every node not only has its own <servicedata> but also the <servicedata> of all the nodes that are present in the Trusted Mobile Grid. Thus the format is shown by Table 1.

TABLE 1: RESOURCE LOOK-UP TABLE

N	SN	SD	SDD	PTYPE	GSR	GSH
1						
2						
3						
4						

D. Resource Discovery Service

Resource Discovery Service – RDS is a service that is used to find a particular resource node using RLT. Functions provide by RDS that use underlying routing algorithm are explained below and are shown in Fig 3.

- **Authenticate –** To authenticate using doctrine.
- **CreateRLT –** Creates RLT and places its own service.
- **NodeCheck –** Talks with underlying protocol to find out whether its peer nodes are active or not.
- **SendRLT –** Sends complete RLT to its peers (one hop).
- **DaleteNode –** Deletes the Node entry from RLT.
- **UpdateRLT –** Updates RLT on getting <servicedata> packets from other nodes.
- **BCDeletedNode –** Broadcasts the deleted node entry on to Trusted Mobile Grid.
- **SearchRLT –** Scans and searches RLT to find a particular service.
- **QoS –** Provides Quality of Service
- **CheckRLT –** Whether there is a change in Resource Lookup Table or not.

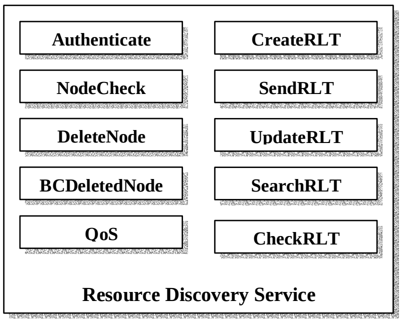

Fig 3: Resource Discovery Service

E. Resource Access Service

Resource Access Service – RAS is published in Trusted Mobile Grid and performs following functions (Fig 4).

- **GetResourceInfo –** Calls the RDS SearchRLT function to find the information about a resource service.
- **SendData –** Send the data to a particular node.
- **ConnectNode –** Calls the underlying routing protocol to bind itself with the requested Node.
- **Receive Data –** Receives the data from a particular node.
- **ExecuteProgram –** Makes the program run.
- **Cache Data –** Caches the received data.
- **SaveLifeCycle –** Maintains the states of the program, thus makes it state-full
- **QoS –** Provides Quality of Service

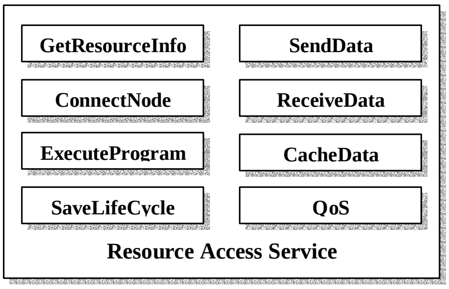

Fig 4: Resource Access Service

V. RESOURCE DISCOVERY

Resource discovery in Trusted Mobile Grid is a function of by the RDS – Resource Discover Service. RDS maintains the RLT – Resource Lookup Table which contains the information about the services provided by each node. But the creation of this Resource Lookup Table requires a procedure in which an RDS send and receives its Table entries to and from their peer nodes. The Resource Discovery Algorithm can be stated as (shown in Fig 5).

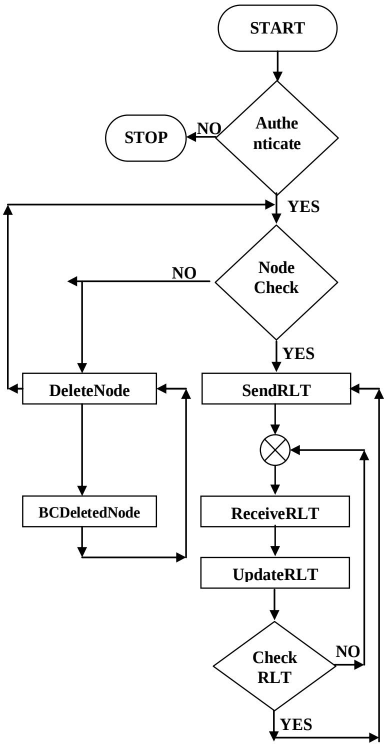

Fig 5: Resource Discovery Algorithm

A. Algorithm

1: Authenticate: Yes → Go to Step 2, No → Go to Step 9
2: Node Check: Yes → Go to Step 3, No → Go to Step 7
3: SendRLT
4: ReceiveRLT
5: UpodateRLT
6: CheckRLT: Yes → Go to Step 4, No → Go to Step 3
7: DeleteNode: Go to Step 8 and 2

8: BCDeletedNode: Go to Step 7
9: Stop

In order to explain Resource Discovery Algorithm, we discuss a certain scenario where nodes enter or leave from a Trusted Mobile Grid. One very important part of the algorithm is to understand that the device only sends its RLT – Resource Lookup Table only when there is change in RLT (as described in algorithm) or when a new node gets authenticated and becomes a part of Trusted Mobile Grid.

B. Scenario: A Node enters a Mobile Grid

This scenario is based on a two node mobile grid. When a third node enters the trusted community it requires to get authenticated and becomes a part of the grid. The complete scenario is explained using Fig 6.

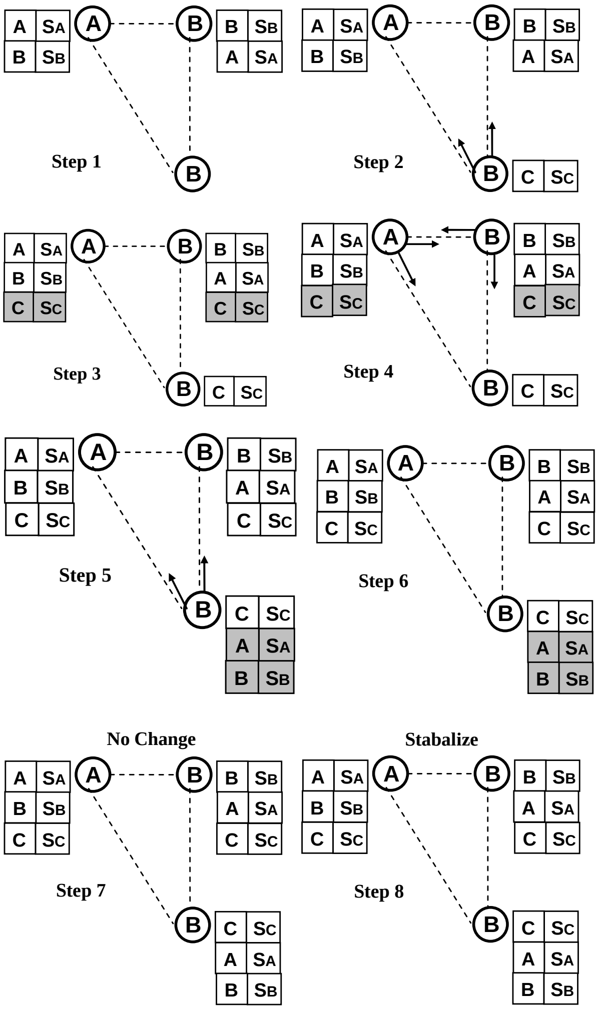

Fig 6: Scenario: Step 1 – 8

Step 1: Node C: Authenticate and get connected.
Step 2: Node C: CreateRLT, SendRLT
Step 3: Node A & B: ReceiveRLT, UpdateRLT, CheckRLT
Step 4: Node A & B: SendRLT
Step 5: Node A, B & C: ReceiveRLT,UpdateRLT,CheckRLT
Step 6: Node A & B: Stable; **Node C:** SendRLT
Step 7: Node A & B: ReceiveRLT, UpdateRLT, CheckRLT
Step 8: No change at any Node: Stabilize

CONCLUSION

This paper has defined an architecture that can perform similar functions that are available in Globus for the establishment and utilization of Grid and on the other hand has simplified these functions so that they can be used on Mobile Ad-Hoc Networks – MANET because both Grid and MANET exhibit similar characteristics like dynamism, heterogeneity and scalability. We have also defined the Resource Discovery and Resource Access mechanism that can be used on light weight mobile grids thus making it MASGRID – Mobile Ad-Hoc Services Grid.

REFERENCES

[1] Ian Foster, etc., "The Physiology of the Grid-An Open Grid Services Architecture for Distributed Systems Integration" Globus Project, 2002

[2] M. W. Subbarao. "Performance of Routing Protocols for Mobile Ad-Hoc Networks," (white paper), (undated). Available: http://w3.antd.nist.gov/wctg/manet/docs/ perf_routing_protocols.pdf

[3] Robert Morris, John Jannoti, Frans Kaashoek, Jinyang Li, Douglas Decouto, "Carnet: A Scalable Ad Hoc Wireless Network System", In the Proceedings of the 9th ACM SIGOPS European workshop: Beyond the PC: New Challenges for the Operating System, Kolding, Denmark, September 2000.

[4] Sye Loong Keoh and Emil Lupu, "Peer Trust in Mobile Ad-hoc Communities" , In the Proceedings of the 11th HP-OVUA Annual Planetary Workshop, Paris, June 20 - 23, 2004.

[5] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network", Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Aug 15, 1999.

[6] Charles E. Perkins, Pavin Bhagwat, "Highly Dynamic Destination-Sequenced Distance- Vector Routing (DSDV) for Mobile Computers", ACM SIGCOMM, pp.234-244, Oct. 1994

[7] Philippe Jacquet, Paul Muhlethaler, Amir Qayyum, Anis Laouiti, Laurent Viennot, Thomas Clausen, "Optimized Link State Routing Protocol", IEEE INMIC Pakistan, 2001.

[8] David B. Johnson, David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", In Mobile Computing, T. Imielinski and H. F. Korth,Eds. Kluwer Academic Publishers, Dordrecht, The Netherlands, ch. 5, pp. 153-181. February 1996.

[9] Charles E. Perkins, Elizabeth M. Royer, "Ad- hoc On-Demand Distance Vector Routing", Second IEEE Workshop on Mobile Computer Systems and Applications, New Orleans, Louisiana, pp.90, February 25 - 26, 1999.

[10] Erol Gelenbe Ricardo Lent, "A Power-Aware Routing Algorithm", International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'03), Montreal, Canada, July 2003.

[11] Rohit Dube, Cynthia D Rais, Kuang-Yeh Wang, Satish K. Tripathi, "Signal Stability Based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks", IEEE Personal Communications Magazine, vol. 4, no. 1, pp. 36--45, Feb. 1997.

[12] Z.J. Haas & M.R. Pearlman, "The Performance of a New Routing Protocol for the Reconfigurable Wireless Networks," ICC'98, Jun. 8-11, 1998

[13] Z.J. Haas and M.R. Pearlman, "Evaluation of the Ad-Hoc Connectivity with the Reconfigurable Wireless Networks," Virginia Tech's Eighth Symposium on Wireless Personal Communications, Jun. 10-12, 1998

[14] Z.J. Haas and M.R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," SIGCOMM'98, Sept. 2 –4, 1998