Active Service Routing Protocol for Mobile Networking

M.V Mamesh Babu [1], D.Rammohanreddy[2]
[1]*PursuingM.Tech (software engineering), Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*
[2]*Associate Professor, Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*

***Abstract*- An ad-hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. LAR is an on-demand protocol who is based on the DSR(Dynamic Source Routing). The Location Aided Routing protocol uses location information to reduce routing overhead of the ad-hoc network! Normally the LAR protocol uses the GPS(Global Positioning System) to get these location information's. With the availability of GPS, the mobile hosts knows there physical location.**

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as

I. INTRODUCTION

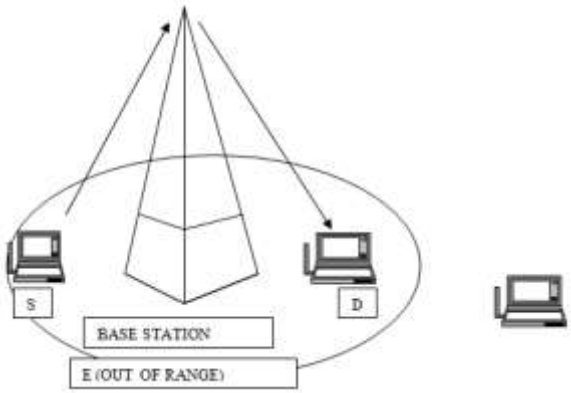
An location based routing is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The primary goal of this routing is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. LAR is an on-demand protocol who is based on the DSR(Dynamic Source Routing). The Location Aided Routing protocol uses location information to reduce routing overhead of the ad-hoc network! Normally the LAR protocol uses the GPS(Gloal Positioning System) to get these location information's. With the availability of GPS, the mobile hosts knows there physical location.

Unlike traditional distance networks, networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.

II. LITERATURE SURVEY

2.1 EXISTING SYSTEM:
Infra-structured Networks

The first one is to introduce a third fixed party (a base station) that will hand over the offered traffic from a station to another, as illustrated in Figure 1. The same entity will regulate the attribution of radio resources, for instance. When a node S wishes to communicate to a node D, the former notifies the base station, which eventually establishes a communication with the destination node. At this point, the communicating nodes do not need to know of a route for one to each other. All that matters is that both nodes source and destination are within the transmission range of the base station. If one of them fails to fulfil this condition, the communication will abort.



Here the base station's range is illustrated by the oval. The two nodes S and D which want to communicate are in the range of the base station. S send the message to the base station which in turn forwards it to destination node D. Thus communication is carried out with help of a base station. All messages have to pass through the base station. Node E is out of the range of the base station this prevents it from communicating to other nodes in the network. When node E wants to communicate to any node in the network it has to contact the base station. Since it is out of range communication is not possible.

That happens if the base station is unavailable? Or what happens if we are in a situation where such an infrastructure does not exist at the first place?

The answer is that we simply do not communicate! This is where the second approach is useful. JNote however that this form of centralized administration is very popular among wide cellular networks such as GSM etc.

2.2 Limitations

The following are the limitations of the existing system.

- Maintenance of information is done manually
- Data collection is not uniform and is stored in different forms
- Locating the appropriate server and client profile and updating it whenever required becomes cumbersome.
- Enforcement of data integrity not possible.
- Unavailable of prominent security measures for data collection.

2.3 PROPOSED SYSTEM:

Location Based Routing

The concept behind these infrastructure less networks is the collaboration between its participating members, i.e, instead of making data transit through a fixed base station, nodes consequentially forward data packets from one to another until a destination node is finally reached. Typically, a packet may travel through a number of network points before arriving at its destination.

Gateways to and interface with a fixed network.

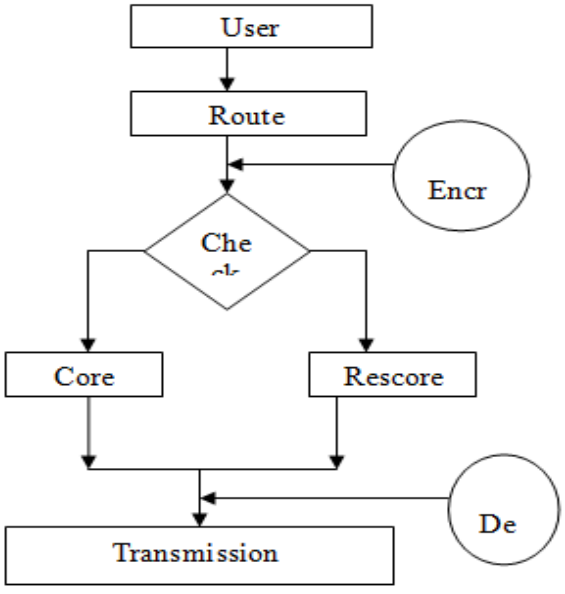
Infra-structure less Network

Here the node S wants to communicate to node D. The oval indicates the communication range of the node.

SYSTEM DESIGN

3.1DATA FLOW DIAGRAM

The data flow diagrams are very helpful in determining the flow of data in an application.



III.SYSTEM TESTING

The purpose of testing is to discover errors.
Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide a systematic demonstration that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.
Functional testing is centered on the following items:
Valid Input: identified classes of valid input Must be accepted.
Invalid Input: identified classes of invalid input must be rejected.
Functions: identified functions must be exercised.
Output: identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested . Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

4.1 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach
Field testing will be performed manually and functional tests will be written in detail.

Test objectives
- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.
- Features to be tested
- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

4.2 Integration Testing
Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.
The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Integration testing for Database Synchronization:
- Testing the links that call the Change Username & password, Migration and Synchronization screens etc.
- The username should be retained throughout the application in the form of hidden variables or by using cookies.
- If the login user does not have enough privileges to invoke a screen, the link should be disabled.
- Any modification in the Master server should be reflected in the Slave server.
- The XML file should retrieve only the records, which have been modified.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

4.3 Acceptance Testing
User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Acceptance testing for Data Synchronization:
- Users have separate roles to modify the database tables.

The timestamp for all insertions and updating should be maintained.

IV. CONCLUSION

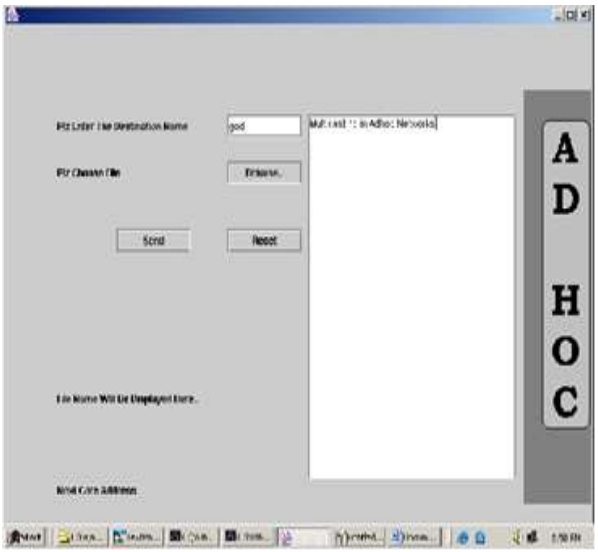
Terminate routing aims to support location-based routing on irregular topologies with mobile nodes. It achieves its goal by combining a location-based routing method with a link state-based mechanism. Further, it introduces the concept of anchors, which are geographical points imagined by sources for routing to specific destinations, and proposes low overhead methods for computing anchors. Last, a special form of restricted search mode (Restricted Local Flooding, RLF), solves problems due to the inaccuracy of location information, in particular for control packets. The performance analysis shows that, in large mobile ad hoc networks, terminate routing performs better than MANET-like, or existing location-based routing protocols. It does so by maintaining its routing overhead low and by efficiently solving location inaccuracies.

V. FUTURE ENHANCEMENT

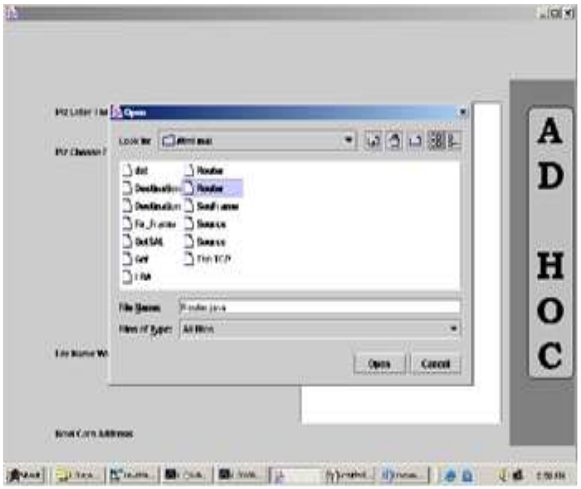
A Mobile Gateway has been developed that uses a cellular network for the connection. It handles the challenges that had to be solved to realize this interconnection and describes a way how to connect two IPv6 networks over an IPv4 infrastructure. Different levels of mobility are described. Mobility within the ad hoc domain and between different Mobile Gateways of this ad hoc domain is handled using an enhanced AODV routing protocol. Mobility of the whole ad hoc network is handled by the mobility mechanisms of the cellular network and finally the seamless mobility of single ad hoc nodes is realized using two interfaces and a modified MobileIPv6 implementation.

VI. SAMPLE SCREENS

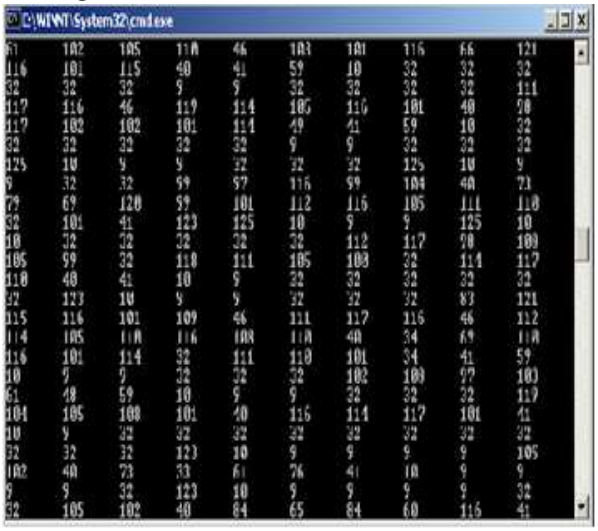
Front-end snapshot of the source node

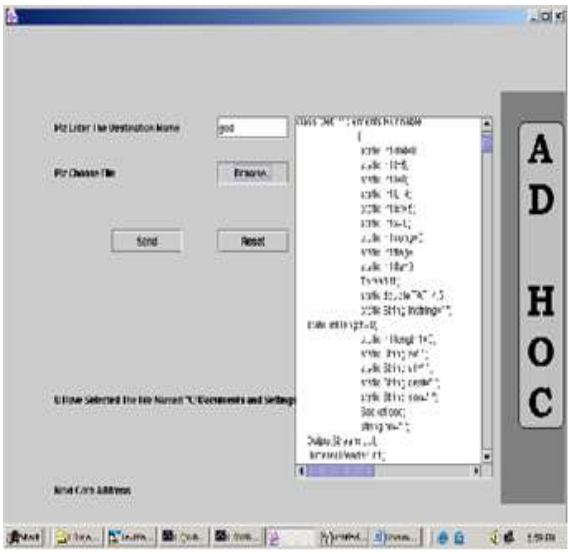


Browsing the file to be sent to destination



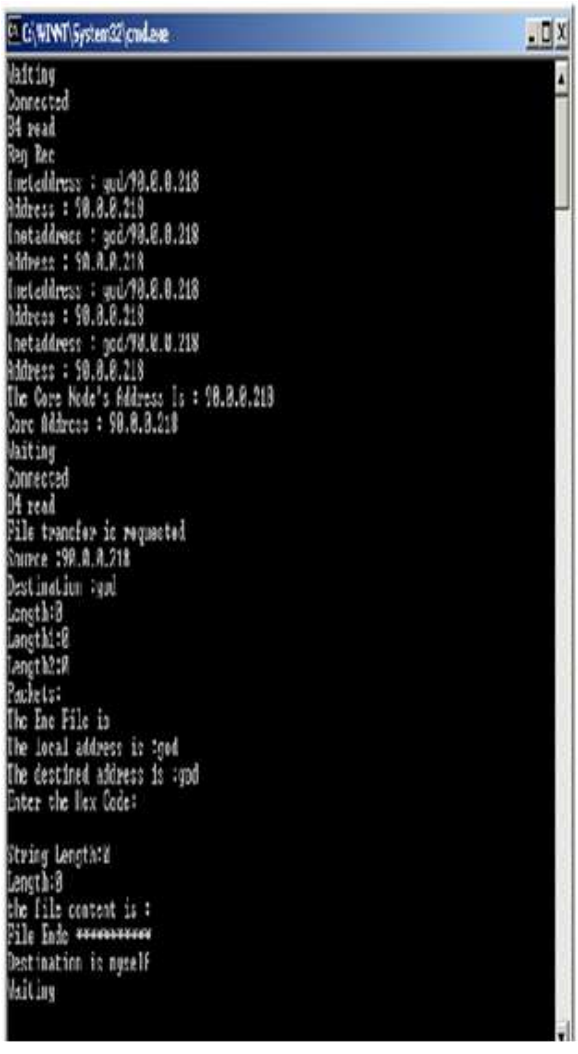
Sending selected file to destination



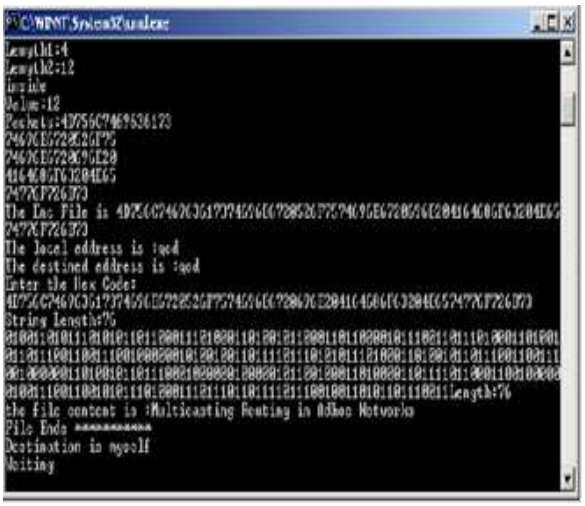


Encrypted form of the file

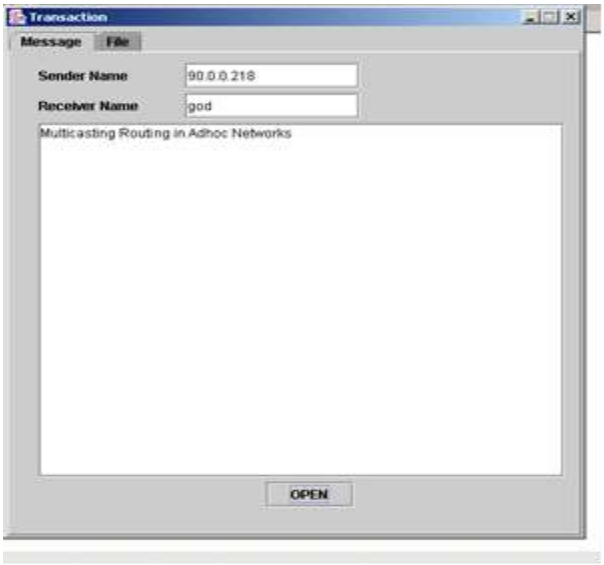
Finding the core node to send data



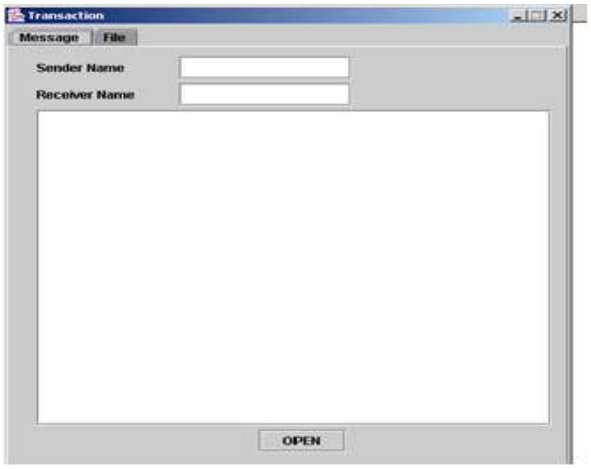
Decrypted form of the file Front-end



Snapshot of destination node



Receiving data at destination node for Mobile Ad Hoc Networks,



REFARENCESS

[1] in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan. 27-31, 2002.

[2] P. Papadimitratos, Z.J. Haas, and P. Samar, ―The Secure Routing Protocol (SRP) for Ad Hoc Networks,‖ Internet Draft, draftpapadimitratos-secure-routing-protocol-00.txt, Dec. 2002.

[3] M.O. Rabin, ―Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance,‖ Journal of ACM, Vol. 36, No. 2, pp. 335-348, Apr. 1989.

[4] H. Krawczyk, M. Bellare, and R. Canetti, ―HMAC: Keyed- Hashing for Message Authentication,‖ RFC 2104, Feb. 1997.

[5] P. Papadimitratos and Z.J. Haas, ―Secure Link State Routing for Mobile Ad Hoc Networks,‖ in Proceedings of the IEEE CS Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, Jan. 2003.