

## **Integrated Approach to Provide Data Security by Using Pre-Existing Routing Approaches in Manets**

**P. Varun Kumar**

Department of Computer Science & Engineering,  
NS Raju Institute of Technology,  
Visakhapatnam, Andhra Pradesh-531173, India.

**A.Sravani**

Department of Computer Science & Engineering,  
NS Raju Institute of Technology,  
Visakhapatnam, Andhra Pradesh-531173, India.

**P. Supriya**

Department of Computer Science & Engineering,  
NS Raju Institute of Technology,  
Visakhapatnam, Andhra Pradesh-531173, India.

**K. Shankar**

Department of Computer Science & Engineering,  
NS Raju Institute of Technology,  
Visakhapatnam, Andhra Pradesh-531173, India.

### **Abstract**

The flexibility and mobility of Mobile Ad hoc Networks (MANETs) have made them increasing popular in a wide range of use cases. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full protection. The use of communication security protocols originally developed for wire line and Wi-Fi networks can also place a heavy burden on the limited network resources of a MANET. To address these issues, a novel secure framework (SUPERMAN) is proposed. The framework is designed to allow existing network and routing protocols to perform their functions, whilst providing node authentication, access control, and communication security mechanisms. This paper presents a novel security framework for MANETs, SUPERMAN. Simulation results comparing SUPERMAN with IPSec, SAODV and SOLSR are provided to demonstrate the proposed frameworks suitability for wireless communication security.

### **Index Terms:**

Access control, authentication, communication system security, mobile ad hoc networks.

### **1. Introduction**

Mobile computing is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away. Otherwise **Mobile computing** is a generic term used to refer to a variety of devices that allow people to access data and information from where ever they are.

- ❖ In existing system, Reactive protocols such as Ad hoc On-demand Distance Vector (AODV), plan routes when messages need to be sent, polling nearby nodes in an attempt to find the shortest route to the destination node.
- ❖ Another system i.e. Optimized Link State Routing (OLSR) takes a proactive approach, periodically flooding the network to generate routing table

**Cite this article as:** P. Varun Kumar, A.Sravani, P. Supriya & K. Shankar, "Integrated Approach to Provide Data Security by Using Pre-Existing Routing Approaches in Manets", International Journal of Research in Advanced Computer Science Engineering, Volume 4, Issue 10, 2019, Page 58-65.

entries that persist until the next update. Both approaches are motion-tolerant and have been implemented in UAV MANETS.

- ❖ Motion-tolerance and co-operative communication characteristics make these protocols ideal for use in UAVs.

To this end, we provide the following contributions:

- ❖ This paper proposes a novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols.
- ❖ SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network.
- ❖ SUPERMAN is a framework that operates at the network layer (layer 3) of the OSI model. It is designed to provide a fully secured communication framework for MANETs, without requiring modification of the routing protocol which process packets and provide confidentiality and integrity.
- ❖ SUPERMAN also provides node authentication.

## 2. Implementation modules

The Application is mainly divided into 4 Modules. They are as follows:

- 1) System Configuration Module
- 2) Node Monitoring Module
- 3) Identify the attack node inside the router
- 4) End to End path measurements

### 2.1 System Configuration Module

In this module, the system construction is mainly done by initializing the sender, receiver and router and all these node details are updated inside the database. Here in this module we can see single sender window, single router window and multiple destination windows.

### 2.2 Node Monitoring Module

Node monitoring is a collaborative detection strategy where a node monitors the traffic going in and out of its neighbors. In the router we try to apply prim's algorithm for generating the shortest path for transferring the data and once the shortest path is found then the data will be send according to that best path. So based on the path choose at the time of sending packets, these nodes try to exchange the information from sender to receiver node.

### 2.3 Identify the attack node inside the router

Here in this level we try to identify those nodes which are attacked by the intruder. Here if any intruder or attacker tries to create any attack for the intermediate nodes inside the router then such a nodes should be immediately identified by the SUPERMAN protocol which is their inside the network layer. And once the superman detects the attacker node immediately it will try to create an alternate path from the POA (point of attack) to reach the data safely to the destination.

### 2.4 End to End path measurements Module:

Here in this module the Superman will try to find out the end to end path measurements for the data which is send from valid source node to destination node. The measurements include the throughput, delay time, travelling path and energy loss .All these measurements are calculated and reported for the sender and receiver.

### 2.5 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay,

avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

## 2.6 Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

## 3. Overview

In this section, we discuss the data, define the problem, and then briefly sketch the proposed solution.

### 3.1 System Design

#### 3.1.1 System Architecture:

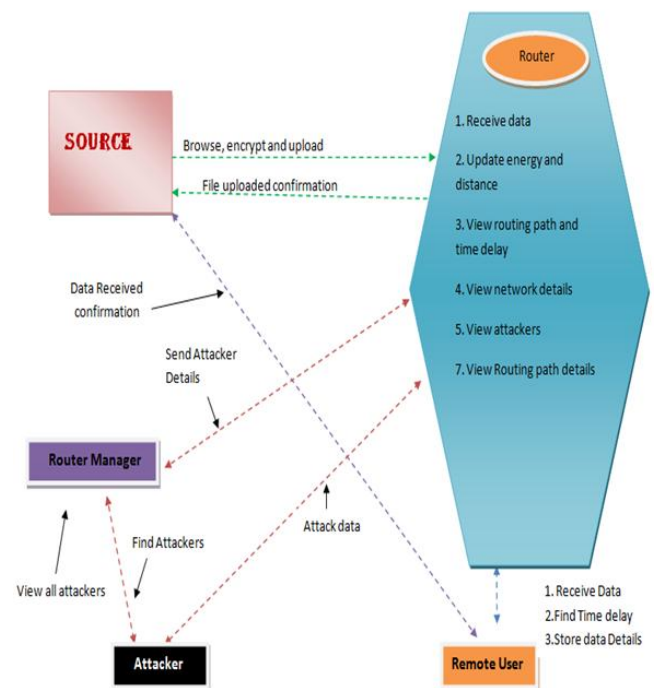


Fig. 1 System architecture

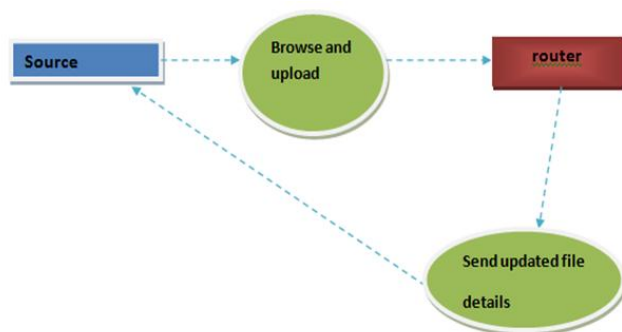
#### 3.2. Data Flow Diagram:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations

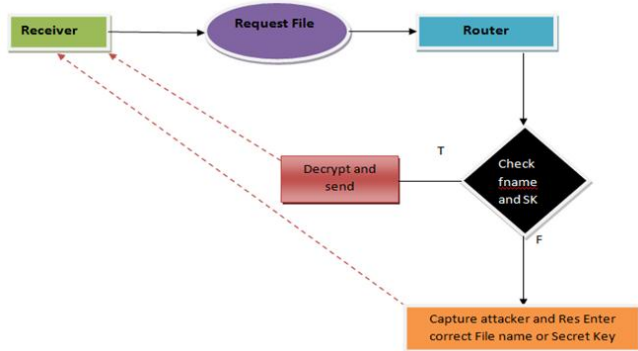
that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

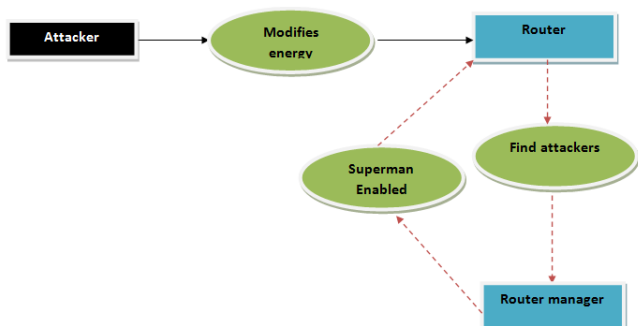
## Level 0:



## Level 1:



## Level 2:



## 3.3 Sequence Diagram:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

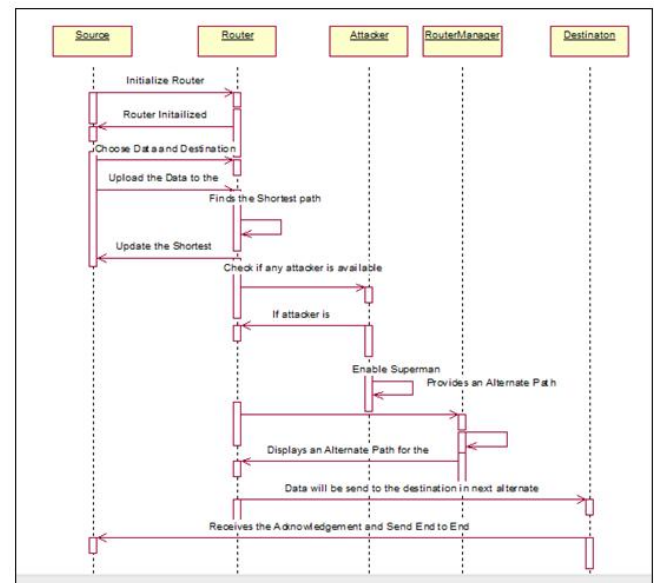


Fig. 3 Sequential diagrams are graphical representations

## 3.4 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.

### 3.4.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid



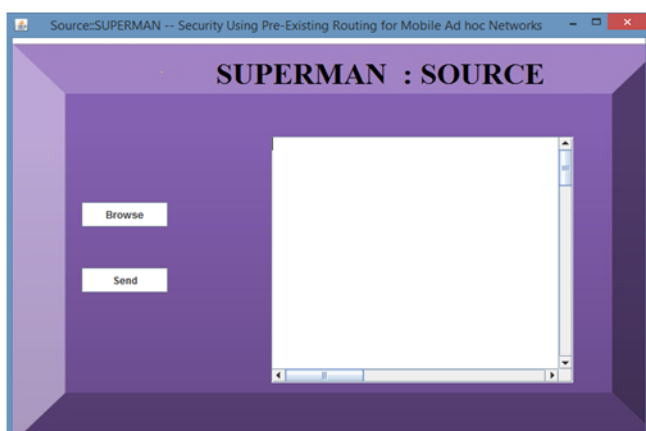
outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. 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.

### 3.4.2 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.

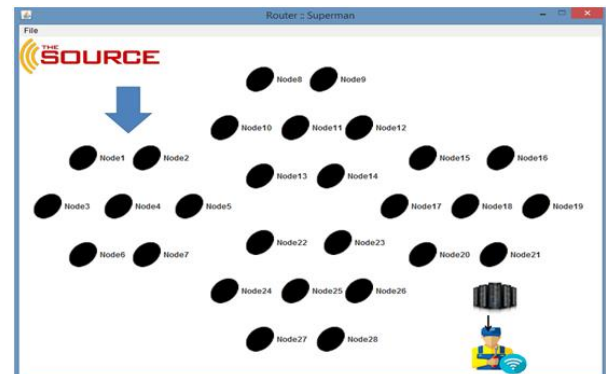
## 4. Result and Discussions

### 4.1 SEND INFORMATION THROUGH SOURCE WINDOW:



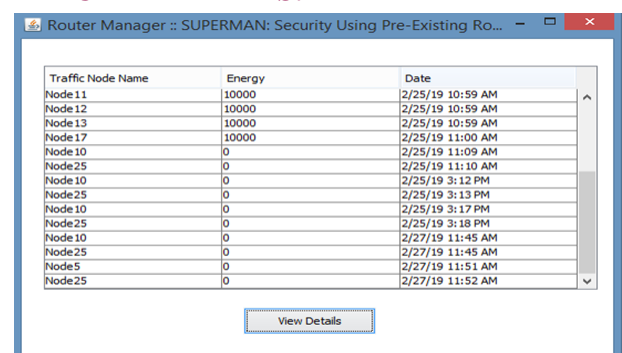
**Fig 4 : Source window for sending data**

### 4.2 SELECT SHORTEST PATH AND SEND DATA TO DESTINATION EVEN ATTACKS OCCUR:



**Fig 5 : Select shortest path and send data to destination even attacks occur**

### 4.3 CHECK FOR ATTACKS AND STORE ATTACKER DETAILS:



Traffic Node Name	Energy	Date
Node11	10000	2/25/19 10:59 AM
Node12	10000	2/25/19 10:59 AM
Node13	10000	2/25/19 10:59 AM
Node17	10000	2/25/19 11:00 AM
Node10	0	2/25/19 11:09 AM
Node25	0	2/25/19 11:10 AM
Node10	0	2/25/19 3:12 PM
Node25	0	2/25/19 3:13 PM
Node10	0	2/25/19 3:17 PM
Node25	0	2/25/19 3:18 PM
Node10	0	2/27/19 11:45 AM
Node25	0	2/27/19 11:45 AM
Node5	0	2/27/19 11:51 AM
Node25	0	2/27/19 11:52 AM

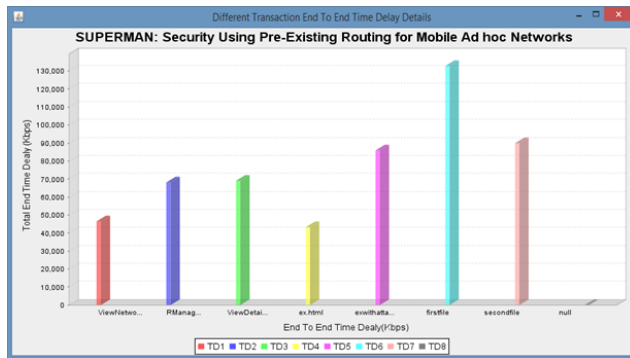
**Fig. 6 Check for attacks and store attacker details**

### 4.4 DESTINATION WINDOW TO RECEIVE THE DATA AND TO SAVE DATA:



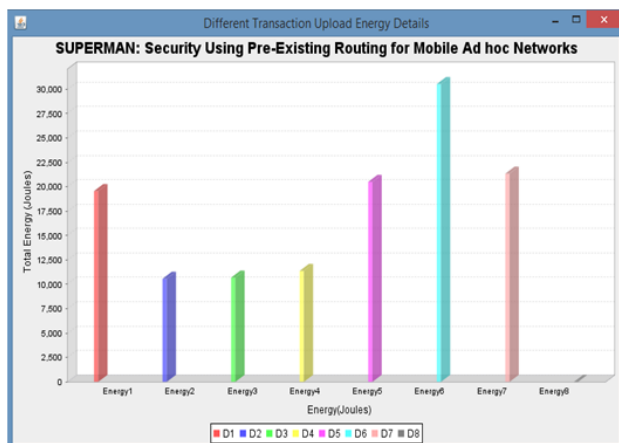
**Fig. 7 Destination window to receive the data and to save data**

#### 4.5 DIFFERENT TRANSACTIONS END TO END TIME DELAY DETAILS:



**Fig. 8 Different transactions end to end time delay details**

#### 4.6 DIFFERENT TRANSACTIONS UPLOAD ENERGY DETAILS:



**Fig. 9 Different transactions upload energy details**

### 5. Conclusions

SUPERMAN is a novel security framework that protects the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services. SUPERMAN addresses all eight security dimensions outlined in X.805. Thus, SUPERMAN can be said to implement a full suite of security services for autonomous MANETs. It fulfils more of the core services outlined in X.805 than IPSec, due to being network focused instead of end-to end

oriented. IPSec is intended to provide secure environment between two end-points regardless of route, and has been suggested by some researchers to be a viable candidate for MANET security. However, it does not extend protection to routing services. Nor does it provide low-cost security, requiring a lengthy set-up and teardown process, usually on a session basis. Simulation has been undertaken and the results are reported and analyzed to determine the relative cost of security for SUPERMAN, compared against IPSec, SAODV and SOLSR where relevant. SUPERMAN provides a VCN, in which the foundation block of security is provided by authenticating nodes with the network. This enables further benefits, such as the security association referral and network merging.

It also provides a relatively light-weight encapsulation packet and variable length tag. Under both CBBA and CF-CBBA, the security overheads of SUPERMAN have been demonstrated to be lower than those of IPSec. Both DTA algorithms represent how a MANET can be made autonomous, by allowing problem solving without human intervention to occur on the network. Securing the communication required to facilitate this functionality is a critical consideration when providing a fully secured network. By providing lower cost security than existing alternatives, while providing security across all eight security dimensions, SUPERMAN proves it is a viable and competitive approach to securing the communication required by autonomous MANETs.

SUPERMAN has been shown to provide lower-cost security than SAODV and SOLSR for their respective routing protocols. By establishing a secure, closed network; one can assume a certain level of trust within that network. This reduces the need for costly secure routing behaviors designed to mitigate the effects of an un-trusted environment (and un-trusted nodes) on the routing process. By preventing the entry of potentially untrustworthy nodes to the network, and thus the

routing process, a MANET may be protected from subversion of its routing services at a lower cost, as malicious nodes are barred from the process entirely. SUPERMAN provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

Future work includes the implementation of SUPERMAN on a simple mobile node platform to allow experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing SUPERMAN services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on SUPERMAN to better understand the role of the credential referral mechanism on overhead mitigation in SUPERMAN networks.

## 6. References

- [1] P. S. Kiran, "Protocol architecture for mobile ad-hoc networks," 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.
- [2] A. Chandra, "Ontology for manet security threats," PROC. NCON, Krishnankoil, TamilNadu, pp. 171–17, 2005.
- [3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
- [4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster-based approach to consensus based distributed task allocation," in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euro micro International Conference on. IEEE, 2014, pp. 428–431.
- [5] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004, pp. 698–703.
- [6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot et al., "Optimized link state routing protocol (olsr)," 2003.
- [7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.
- [8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.
- [9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.
- [10] N. Garg and R. Mahapatra, "Manet security issues," IJCSNS, vol. 9, no. 8, p. 241, 2009.



[11] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch,  
“An evaluation of protocols for uav science  
applications,”2011.

[12] A. R. McGee, U. Chandrashekhar, and S. H.  
Richman,“Using itu-t x. 805 for comprehensive  
network security assessment and planning,” in Tele  
communications Network Strategy and Planning  
Symposium. NETWORKS2004, 11th International.  
IEEE, 2004, pp. 273–278.