Int. J. Advanced Networking and Applications
Volume: 02 Issue: 01 Pages: 464-469 (2010)

Dynamic Key-Scheduling and Authentication Scheme for Distributed Wireless Network

T.Surya Prakash Reddy
Associate Professor, Department of Computer Science, Madina Engineering College, INDIA
Email: surya.prakash12@rediffmail.com

T. Sunil Kumar Reddy
Assistant Professor, Department of Computer Science, Madina Engineering College, INDIA
Email: sunil_reddy1982@yahoo.co.in

ABSTRACT

A self-protection technique is suggested for adhoc network fall short of the objective of data privacy, data integrity, and authentication. Various security standards such as IEEE 802.11i, WPA, IEEE 802.1X were suggested to enhance the security issues in 802.11.Despite their efficiency, these standards does not provide any security approach for monitoring of these authentication in a distributed architecture. For the efficient monitoring of the authentication issue in adhoc network, in this paper we present a self monitored security approach for self-monitoring of key authentication for security protocol in adhoc networks. The processing overhead for the suggested approach is evaluated for a threshold based cryptographic approach.

Keywords – adhoc network, key stream, MANET, quality of service, self secure.

Date of Submission: March 10, 2010 Date of Acceptance: April 30, 2010

I. INTRODUCTION

Wireless technology has advanced tremendously over the past decade, introducing a wide range of devices with networking abilities. Wireless connectivity is certainly available for many devices, but it is limited to few hotspots, and requires subscription to specific services. Furthermore, the quality of connection is rarely adequate[4] for any high-bandwidth applications, which are expected to drive the market for these devices. These are formed by a group of wireless enabled devices that connect together and form a network, without the assistance of a pre-existing infrastructure, like a base station. The commonly used 802.11b MAC[1] protocol includes support for an ad-hoc mode of operation. Such networks are often used in cases of rapid deployment,[5] in places lacking adequate infrastructure, or to facilitate direct communication between nodes when the base station becomes the bottleneck. Ad hoc networking is an attractive concept and has various possibilities for different kinds of applications. In some application environments, such as battlefield communications, disaster recovery etc., the wired network is not available and multi-hop wireless networks provide the only feasible means for communication and information access [7]. This kind of network is called Mobile Ad hoc network (MANET). It is also expected to play an important role in civilian forums such as campus recreation, conferences, and electronic classrooms etc. A MANET can be seen as an autonomous system or a multi-hop wireless extension to the Internet. As an autonomous system, it has its own routing protocols and network management mechanisms. As a multi-hop wireless extension, it should provide a flexible and seamless access to the Internet. Recently, because of the rising popularity of multimedia applications and potential commercial usage of MANETs, QoS support in MANETs has become an unavoidable task. By definition, a mobile ad hoc network does not rely on any fixed infrastructure; instead, all networking functions (e.g. routing, mobility management, etc) are performed by the nodes themselves in a self-organizing [2] manner. For this reason, securing mobile ad hoc networks is challenging and in some applications this requires modifications with respect to the traditional security solutions for wire line networks. Mobile ad hoc networks do not provide any online access to communicating nodes. As they exhibit frequent partitioning due to link and node failures [8] and due to node mobility maintenance of a centralized security system is not possible. Hence traditional security solutions that require centralized authorities [6] are not well suited for securing ad hoc networks. There are two extreme ways to introduce security in mobile ad hoc networks: 1) through a single authority domain, where certificates and/or keys are issued by a single authority, typically in the system setup phase or 2) through full self-organization, where security does not rely on any trusted authority or fixed server, not even in the system initialization phase. In contrast with conventional networks, mobile ad hoc networks usually do not provide on-line access to trusted authorities or to centralize servers and they

Volume: 02 Issue: 01 Pages: 464-469 (2010)

exhibit frequent partitioning [3] due to link and node failures and to node mobility. For these reasons, traditional security solutions that require on-line trusted authorities or certificate repositories are not well suited for securing ad hoc networks. For the authentication of adhoc network

In this paper, we propose a fully self-monitored key management system that allows users to generate their key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. A self organizing key management system that allows users to create, store, distribute and revoke their keys without the help of any trusted authority or fixed server.

II. SECURITY IN ADHOC NETWORK

Security is a fundamental issue that needs resolution before ad hoc networks will experience large-scale deployment. Vehicular ad hoc networking is a good example of a MANET application with some serious security implications. Failure of the security mechanisms may result in the loss of human life. The characteristics of mobile ad hoc networks, pose numerous challenges in achieving conventional security goals. Since the nodes are responsible for basic network functions, like packet forwarding and routing, network operations can be easily jeopardize if countermeasures are not integrated into these network functions at the early stages of design. For example, some existing routing protocols for mobile ad hoc networks may be able to manage the dynamic network topology of mobile ad hoc networks, but none of these protocols incorporate mechanisms to prevent, tolerate or defend against attacks from malicious adversaries. Due to the close relationship between security and the characteristics of ad hoc networks these protocols will have to be fundamentally altered or re-designed to effectively incorporate security mechanisms. Researchers in the ad hoc network security field initially focused on secure routing protocols. The focus of these protocols is:

1. To provide a robust routing mechanism against the dynamic topology of MANETs.
2. To provide a robust routing mechanism against malicious nodes.

Routing protocols use various security mechanisms to ensure robustness of the routing scheme. Some of these mechanisms are listed below:

1. Redundancy exploitation.
2. Diversity coding.
3. Authenticated route discovery and network nodes.
4. Guaranteed route discovery.
5. Route maintenance techniques.
6. Fault or intrusion tolerant mechanisms.
7. Cryptographic techniques, procedures, schemes, tools or mechanism.

It is widely acknowledged that cryptographic techniques can provide some of the strongest mechanisms to ensure the authenticity, integrity and confidentiality of routing information. Secure key management with a high availability feature is at the center of providing network security. However, all routing schemes neglect the crucial task of secure key management and assume pre-existence and pre-sharing of secret key pairs. This leaves key management considerations as an open research area.

III. SECURITY APPROACH

In a security concept, typically striving for goals like authenticity, integrity, confidentiality, non-repudiation and availability, authentication of communicating entities is of particular importance as it forms the basis for achieving the other security goals: e.g., encryption is worthless if the communication partners have not verified their identities before. Various methods were suggested before to provide these security approaches.

i) Threshold cryptography: Several methods of authentication have been proposed for ad hoc networks. The threshold cryptographic method is found to be the most commonly used current method. In threshold based cryptographic method, authentication and communication including data transfer is based on centralized node concept.

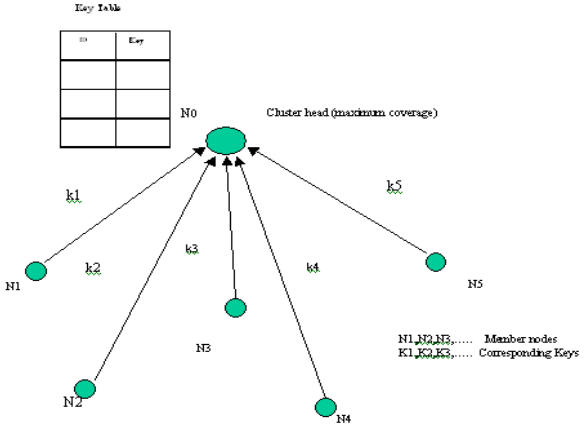


Figure 1: Threshold cryptographic method

For the above illustrated network considered, node with id N0 is chosen as the centralized server node or the cluster head. All the other nodes N1 to N5 send their corresponding keys (K1 to K5) to the centralized node i.e.N0. Node N0 forms the repository table.

If any node needs to send a message or communicate with any other node in the network, the network performs route establishment. All the possible routes from source node to destination node are found out. This is carried out using a routing protocol Dynamic Source Routing (DSR) that gives all the possible routes that go from source node to destination node.

Threshold based cryptography method is based on the centralized node for monitoring the keys .The key distribution and Authentication is completely relied on centralized node. Any failure in key generation may result in wrong authentication. All nodes depend on the centralized node for authentication.

Volume: 02 Issue: 01 Pages: 464-469 (2010)

TABLE 1 : REPOSITORY TABLE AT NODE N0

ID	KEY
N1	K1
N2	K2
N3	K3
N4	K4
N5	K5

IV. SELF MONITORING APPROACH

The main problem of any key based security system is to make each user's key available to others in such a way that its authenticity is verifiable. In mobile ad hoc networks, this problem becomes even more difficult to solve because of the absence of centralized services and possible network partitions. More precisely, two users willing to authenticate each other are likely to have access only to a subset of nodes of the network (possibly those in their geographic neighborhood). The best-known approach to the key management problem is based on key certificates. A key certificate is a data structure in which a key is bound to an identity (and possibly to some other attributes) by the digital signature of the issuer of the certificate. In this system, the users themselves create users' keys. For simplicity, it is assumed that each honest user owns a single mobile node. Hence, same identifier is used for the user and her node (i.e., both user *u* and her node will be denoted by *u*). Unlike in the previous method, where certificates are mainly stored in centralized certificate repositories, certificates in our system are stored and distributed by the nodes in a fully self-monitored manner. Each certificate is issued with a limited validity period and therefore contains its issuing and expiration times. Before a certificate expires, its issuer issues an updated version of the same certificate, which contains an extended expiration time. Each node periodically issues certificate updates, as long as its owner considers that the user-key bindings contained in these certificates are correct.

The self-organizing concept includes two stages
1) Key Distribution /Initialization
2) Authentication

In an ad hoc network, in order for the nodes to communicate, it is essential that each node have the information about the rest of the nodes in the network. In particular, the keys of the nodes that are in its communication range are the most important parameter.
In self-organization method, key distribution is the first phase. It is the initial phase for an ad hoc network to perform any task within the network.

Initialization Phase: The initial phase of the system is executed in three steps: each node creates a key pair; each node creates a self-certificate, issues certificates to other nodes and constructs an non updated certificate repository; nodes exchange certificates; and create updated certificate repositories. Each of these steps is illustrated in Figure.

Step-1: Creation of Key Pairs: Users locally create their own private key and corresponding key.
Step-2: Key distribution: Communication range of each user depends on the power level of each user. Depending up on the communication range of the nodes, they find out their nearest neighbors or the nodes that can be reached in one-hop. Once the nodes generate their keys, key distribution takes place. During broadcast period, each user broadcasts its key to all its nearest neighbors or one-hop neighbors. This is a synchronous process i.e. every node does this simultaneously. Now all the users in the network are aware of the keys of their neighbors.

Distribution of keys to neighbors
Step-3: issuing of Key Certificates/Certificate exchange
Every node receives a set of keys from all its neighbors. A node up on receiving a key from a particular neighbor, issues a certificate comprising the sending node id, key along with its own key. This indicates that the node believes in the sender's identity. That is each node acknowledge back to the sender node with the certificate for the received node key. All the nodes in the network do this simultaneously.

Issuing of key certificates:
Certificate issued is of the following form. It consists of id's and keys of the two nodes involved in exchange of certificates.

Authentication:
Each node collects the certificates from all its one-hop neighbors. The Exchanged certificates are saved in the form of a repository table at each node. Consider node n issued a certificate to node m. The certificate includes node m's id and key Pm along with node n's id and key Pn. The exchanged certificate gives the authentication of the key received (Pm) by presenting the key of node-m which it received, with it' s own key (Pn). The authentication of the key is done by the node m by checking the second field of the certificate i.e. it's own key(Pm)as received by node-n. That means that node m believes that node n has its valid key and communication can be carried out. The certificate exchange process has a low communication cost since certificate exchanges are only performed locally in a one-hop fashion.

Every node will store the repository table in its memory. The form of the non-updated repository table is given in the figure below:
The Figure 2 shows the formation of repository tables by the nodes in the network

Construction of Updated Certificate Repositories:
Every network has a work cycle period during which network operations are carried out. This work cycle is known as a beacon period. This beacon period includes the time taken for initialization of the network as well as communication. Initialization phase is nothing but the time taken by the nodes to know about all the other nodes in the network. This period is called the broadcast period or setup period

Since the mobile ad hoc networks are open, any number of the existing nodes may leave the network or new nodes may join the network. The nodes or the users may keep on changing their location even. So the network is dynamic in nature. The changes that may occur to the network during any beacon period are not taken in to consideration till the completion of beacon period. That is these changes do not effect the communication that is being carried out. Once the beacon period is completed, what ever the repository table each node has is taken as a back up. Then each and every node again tries to find out their neighbors. These neighbors may be same as those, which the node encountered, in the previous beacon period or the node may encounter some new nodes The process of broadcasting the keys and certificate exchange again begins. When a node starts receiving the new certificates, it checks whether its back up repository table contains the similar certificate or not. If it already has similar certificate in its back up non-updated repository table, the newly received certificate is ignored. Like this every new certificate is verified. Scenario when one new node is added to the network after a beacon period is shown in the Figure 3.

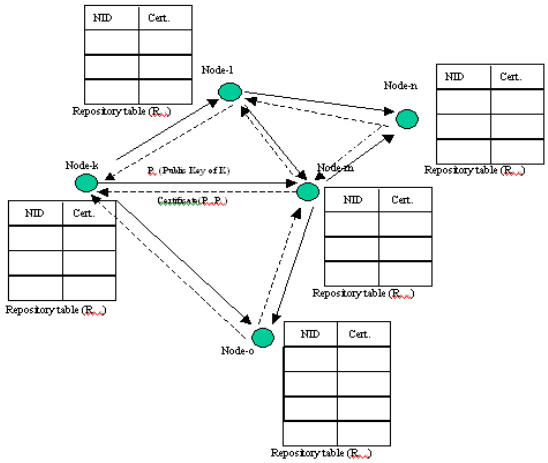


Figure 2: Formation of repository tables

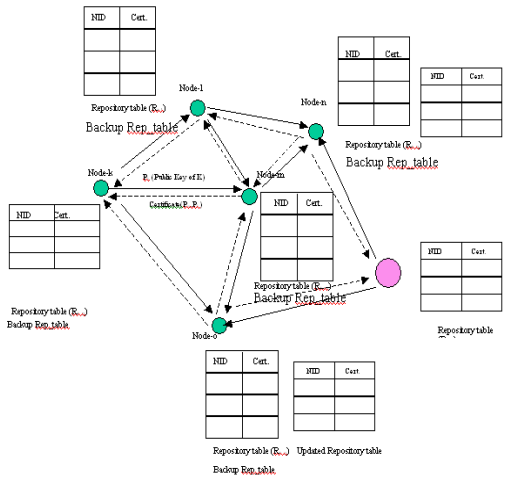


Figure 3: certificate exchange with newly added node

Finally certificates are saved in the new repository table are the certificates given by the nodes that entered the network lately. Users can revoke any issued certificate to other users in the instance of distrust in the key binding. Similarly users can also revoke their own certificate if they believe that their private key has been compromised. This new repository table is known as the updated repository table. Clearly the size of the updated repository table becomes less as time goes on. In the similar way, further communication will be carried out. After more and more beacon periods the trustiness among the nodes increases. The proposed self-monitored key management system is completely independent in operation. Does not rely on any centralized node for key. The method performs certificate exchange so the authentication is most secure without involving any third party or central server. The approaches described were compared using various analysis factors. 1) Propagation delay, 2) Average packet delivery,3) Repository updation factor as shown.

V. SIMULATION RESULTS

The proposed self-monitored key management scheme is implemented on an ad hoc network. The network is created with randomly distributed nodes. Network is considered with the following properties:

No of nodes (n): 20
Network area: 200 x 200
Band width: Random
Routing Algorithm: DSR
Optimizing algorithm: SWP
Network distribution: random
Neighbor Discovery: Range factor
Communication: non-interfering
Head discovery**:** coverage

Several ad hoc networks are tested for various cases of network load. Even variable number of nodes is taken into account. Performance of both threshold based cryptography and self-monitored approach are tested. The three analysis factors mentioned in the previous section are evaluated in both the cases.

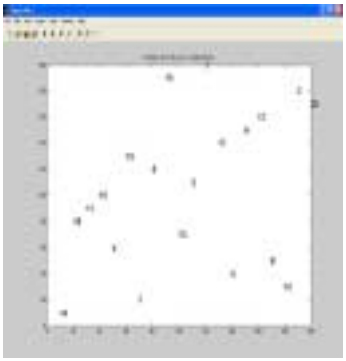
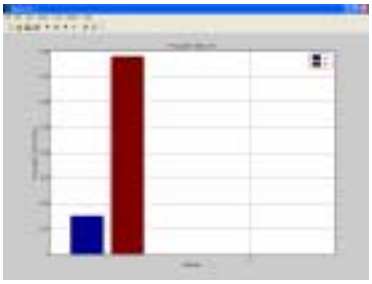


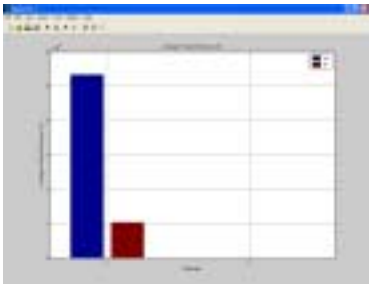
Figure 4: Simulated network with the stated specifications

Volume: 02 Issue: 01 Pages: 464-469 (2010)

Case 1: With No Add-on nodes ,Source node:18 Destination node:12, Route taken for communication from source to destination: 18 → 4→ 6 → 17→ 12



(a)

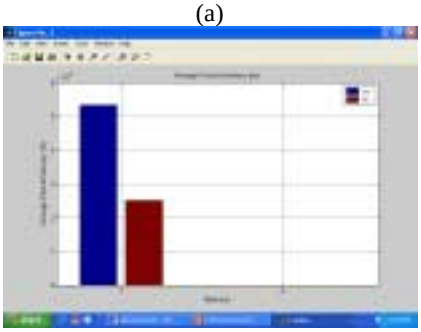


(b)

Figure 5:(a) Average Packet Delivery & (b) Propagation delay plot

Case 2: Source node:14,Destination node:20,With No Add-on nodes,Route taken for communication from source to destination: 14 → 4 → 6 → 3 → 9 → 20

(a)

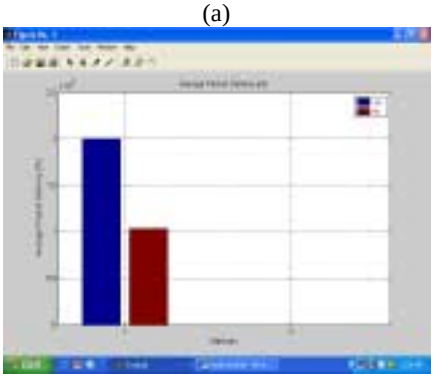


(b)

Figure 6:(a) Average Packet Delivery & (b) Propagation delay plot

Case 3: Source node:14, Destination node:20, Generated load: four bytes, With no add on nodes, Route taken for communication from source to destination: 14 → 4 → 6 → 3 → 9 → 20

(a)

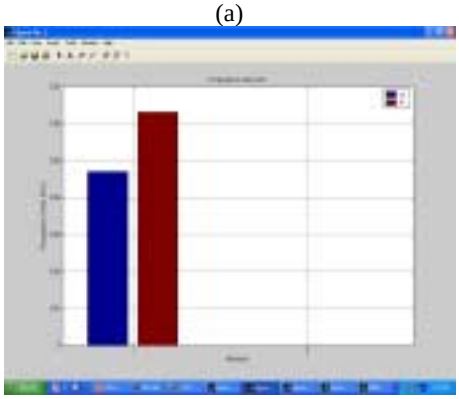


(b)

Figure 7: Average Packet Delivery plot

Case 4: Source node:14, Destination node:20, Generated load: four bytes, With 2 add on nodes, Route taken for communication from source to destination: 14 → 4 → 6 → 3 → 9 → 20

(a)



(b)

Figure 8: a) Average Packet Delivery & (b) Propagation delay plot

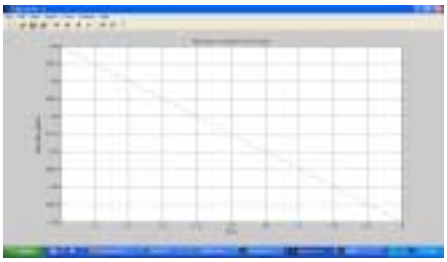
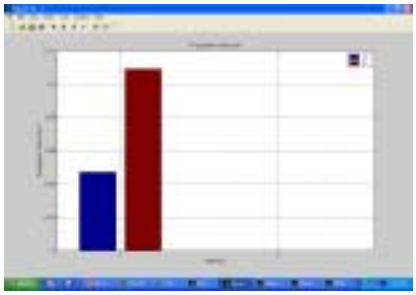
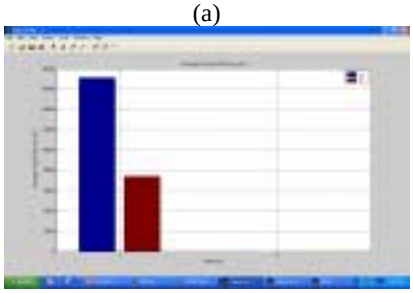


Figure 9: Repository Updation plot

Case 5: Source node:14, Destination node:20, Generated load: four bytes, With 2 add on nodes and 1 remove node Route taken for communication from source to destination: 14 → 4 → 6 → 3 → 9 → 20



(a)



(b)

Figure 10: (a) Average Packet Delivery & (b) Propagation delay plot

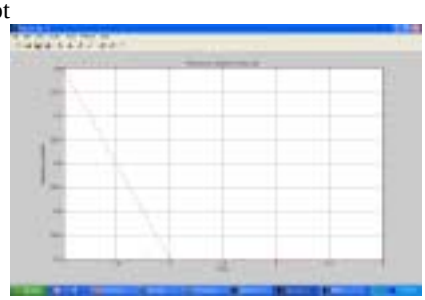


Figure 11: Repository Updation plot

VI. CONCLUSION

In this work, the problem of key management in mobile ad hoc networks is addressed. A fully self-monitored key management system for mobile ad hoc networks is developed and it is observed that two users in a mobile ad hoc network can perform key authentication based only on their local information, even if security is performed in a self-monitored way, it is shown that with a simple local repository construction algorithm and a small communication overhead, the system achieves high performance on a wide range of certificate graphs; (iv) it is also shown that nodes can have mobility to facilitate authentication and to detect inconsistent and false certificates. An important feature of this scheme is that key authentication is still possible even when the network is partitioned and nodes can communicate with only a subset of other nodes. In this method the involvement of all the nodes are required only when their key pairs are created and for issuing and revoking certificates; all other operations including certificate exchange and construction of certificate repositories are self monitored.

REFERENCES

[1] Andreas Pfitzmann, Birgit Pfitzmann ,Matthias Schunter, Michael Waidner, “Trusting Mobile User Devices and Security Modules”, Information infrastructure for virtual envirnment, IEEE 1997.

[2] Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks”, IEEE network , Nov/Dec –1999.

[3] Panagiotis Papadimitratos and Zygmunt J. Haas, “Secure Routing for Mobile Ad hoc Networks”, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[4] N. Asokan and P. Ginzboorg, Chuk Yang Seng , “Key Agreement in Ad-hoc Networks” presentation.

[5] David B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts”, Computer Science Department Carnegie Mellon University Pittsburgh, IEEE-1995.

[6] Emre Sayın & Albert Levi, “Open Trust Scheme for Ad Hoc Networks”- 2006.

[7] Nancy C. Roberts, Raymond Trevor Bradley, “Research Methodology for New Public Management”, the International Public Management Network workshop in Siena, Italy, July 28-30, 1999.

[8] Seung Yi, Prasad Naldurg, Robin Kravets, “A Security-Aware Routing Protocol for Wireless Ad Hoc Networks”, University of Illinois at Urbana-Champaign Urbana, IL 61801

[9] Anne Vanhala, “Security in Ad-hoc Networks” ,Research seminar on Security in Distributed Systems University of Helsinki

[10] Frank Stajano and Ross Anderson, “The Resurrecting Duckling:Security Issues for Ad-hoc Wireless Networks” ,Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999.

[11] Ljubica BlaZevit, Levente Buttyan, Srdjan tapkun, Silvia Giordano, Jean-Pierre Hubaux, and Jean-Yves Le Boudec, “Self-Organization in Mobile Ad Hoc Networks: The Approach of Terminodes”, IEEE communication Magazine, June 2001

[12] Levente Buttyan and Jean-Pierre Hubaux, “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks”, Laboratory for Computer Communications and Applications Swiss Federal Institute of Technology EPFL-IC-LCA, CH-1015 Lausanne, Switzerland March 19, 2002. ACM/ Kluwer Mobile Networks and Applications (MONET).