Virtual Operator based AAA in Wireless LAN Hot Spots with Ad-hoc Networking Support

ACM MobiHoc 2002

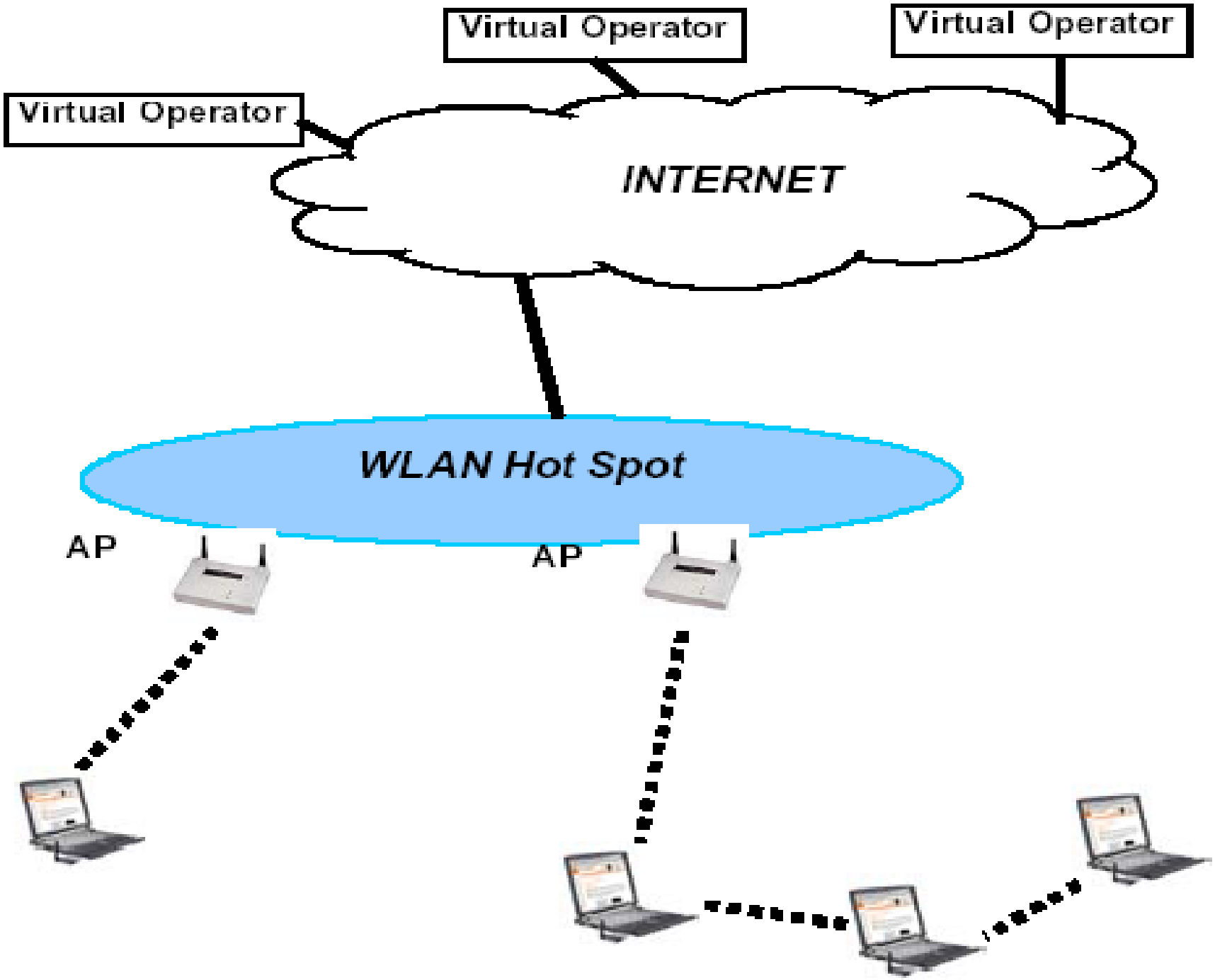
林佑青　2003.5.29

Outline

- Introduction
- Virtual Operator
- Solutions
- Authentication
- Accounting
- Broker model
- Conclusion

Introduction

- Wireless LAN access points (AP) are starting to be deployed in public hot spots for public Internet access.
- To ensure the proper operation under this model, it is critical that Authentication, Authorization and Accounting (AAA) be done.
- It is inconvenient if a mobile user has to maintain an account with each WLAN provider.


Virtual Operator
Virtual Operator
Virtual Operator
INTERNET
WLAN Hot Spot
AP
AP

Virtual Operator

- Uses the mobile users' service providers as the single point of contact for AAA transactions.
- A service provide that has a contractual relationship with the Wireless LAN provider.
- It's possible for a single user to have an account with each WLAN provider.
- The solution is entirely based on IP.
- A packet filtering function employed at an AP, similar to the firewall function.

Types of Virtual Operators

- Internet Service Providers
- Cellular operators
- Pre-paid card provider

Current solutions

Cisco

- Uses IEEE 802.1X and EAP to provide a virtual link between the access point and the mobile terminal.
- The solution is not backward compatible.
- Key exchange problem.

  All session keys between the MTs and the APs are assigned by the authentication server.

Lucent

- Uses the RADIUS protocol.
- Mutual authentication is not considered.
- Diffie-Hellman algorithm is prone to “man in the middle” attack.

Nokia

- Announced their “Operator Wireless LAN” solution.
- Each wireless LAN card has an integrated SIM card reader.
- RADIUS protocol is used between the public access controller and the GSM authentication and billing gateway.
- The solution only targets cellular network based virtual operators.

Web Browser based approach

- The authentication process are carried out in the web browsers on the client machines using the secure HTTPS protocol.
- The access control mechanism is not secure .

  The browser can not perform any key configuration on the client machine after the authentication.

Solution

- The entire AAA process is carried out over the IP layer.
- Based on filtering function.
- AP controls the authentication, which includes the establishment of the authentication channel, the controlling mechanism, and the session key assignment and management mechanisms.
- A gateway between the AP and the network to control the MT access and to relay the AAA messages.

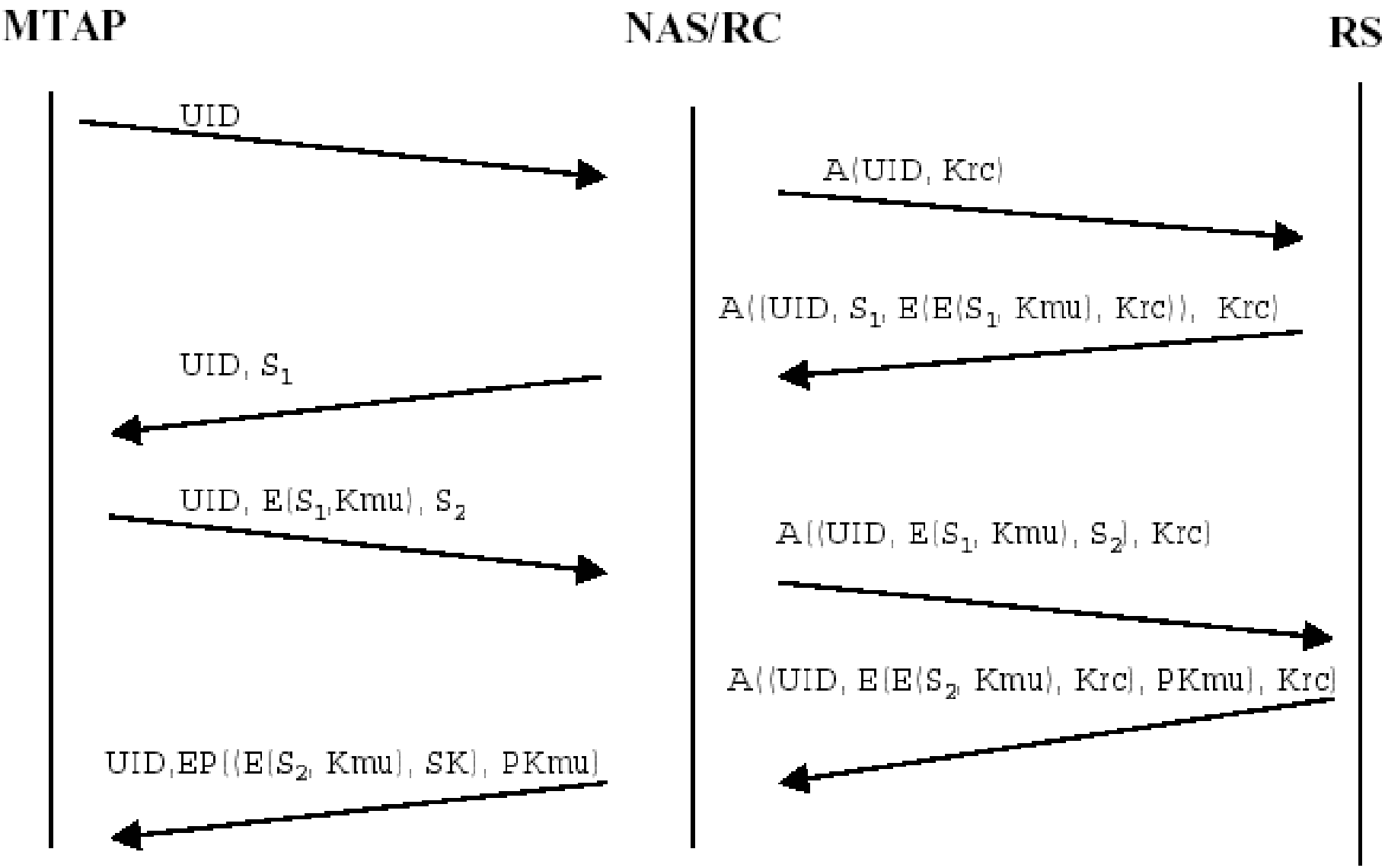
Benefits

- Works over different air interfaces.
- It does not require modification to layer 2 protocols.
- Since encryption can be done at the IP layer using IPSEC, it does not require that the AP support layers session keys.
- It supports ad-hoc networking without any protocol change.

Authentication and Authorization

- Allows APs to determine session keys and communicate them securely to the associated MTs.
- Each authenticated user has a shared session key with the AP.
- AP filters the IP addresses and authenticated user traffic with the session key.

Authentication Procedure



Fast AAA handoff

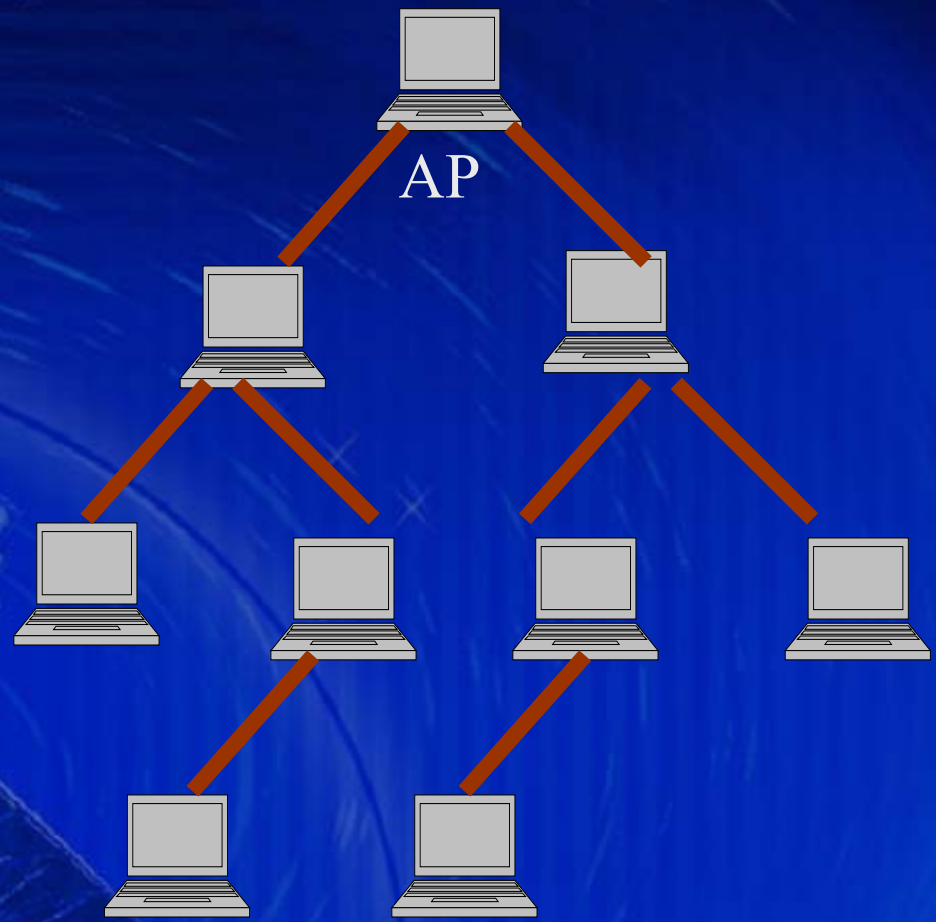
- The user does not have to go through the authentication process all over again.
- New AP contacts the old AP, notifies the old AP and fetches the user profile.
- The new AP then encrypts the new session key it shares with the user together with the old session key using the user's public key.

Accounting

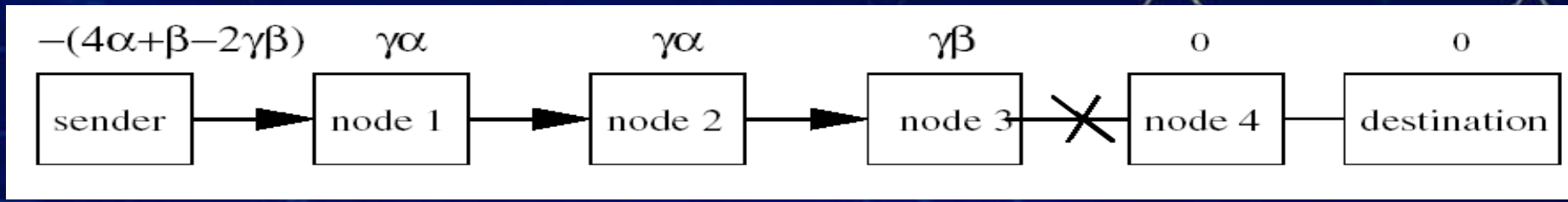
- Using mutual accounting proof from both the mobile users and the wireless LAN operators.
- A traffic monitoring module on the MT monitors wireless LAN traffic, and sending usage profile to the AP.
- AP checks the usage profiles, if match, send profile to Virtual operator.
- Virtual operator has the proof that user and WLAN operators agree on the usage profile.

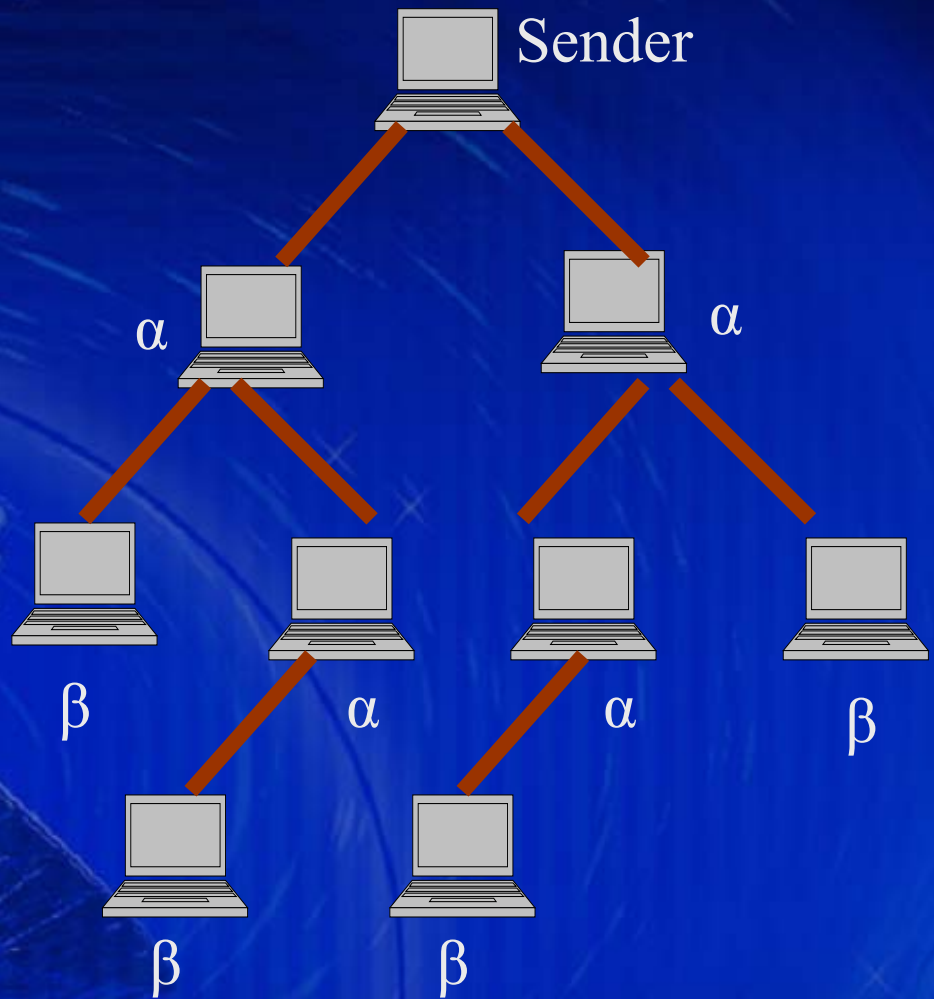
Ad-hoc network accounting

- Minimum spanning tree rooted at the AP.



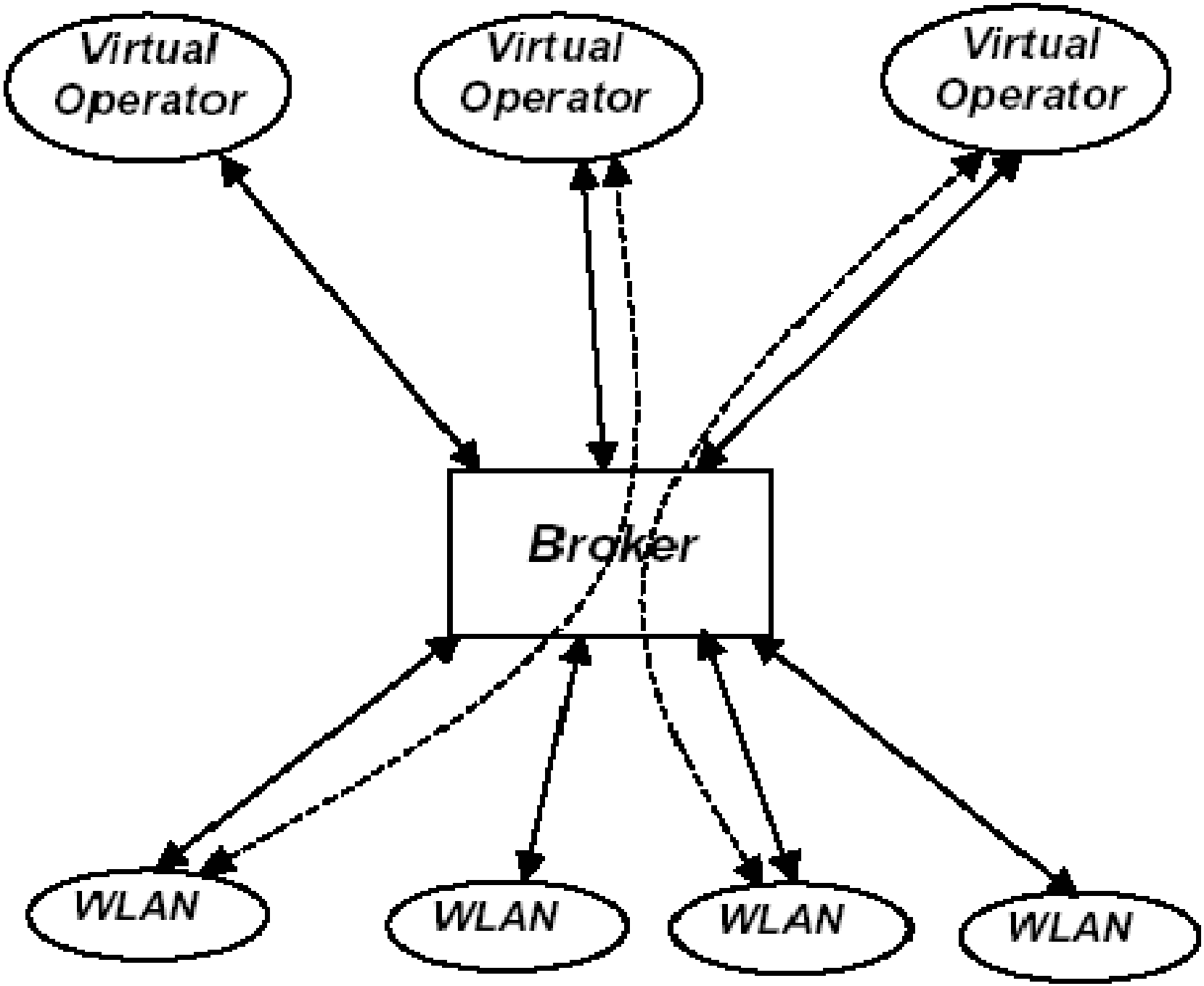
Sprite


−(4α+β−2γβ)
γα
γα
γβ
0
0
sender
node 1
node 2
node 3
node 4
destination


Sender
α
α
β
α
α
β
β
β

Broker

- Each wireless LAN operator and virtual operator pair with a business agreement need to establish a trust relationship.
- AAA proxying and dynamic relationship set-up.
- Once the relationship is established, all the AAA transaction will be carried out through the direct communication channel between the WLAN and the virtual operator.


Virtual Operator
Virtual Operator
Virtual Operator
Broker
WLAN
WLAN
WLAN
WLAN

Conclusion

- Virtual Operator is a very useful concept in providing public Internet access with wireless LAN technologies.
- In a public access LAN environment, a diverse set of wireless products and different types of wireless operators may coexist to provide mobile users with convenient and comprehensive wireless access solutions.