



# Mobile Ad Hoc Networks and Secure Routing

John Marshall  
marshall@cs.fsu.edu

13 February 2003

1



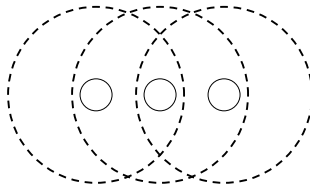
## Introduction

- ◆ Ad hoc networks
- ◆ Routing
- ◆ Secure Routing Protocol (SRP)
- ◆ Attack on SRP
- ◆ Solution
- ◆ Theoretical basis for attacks

2

## Mobile Ad Hoc NETWORKS

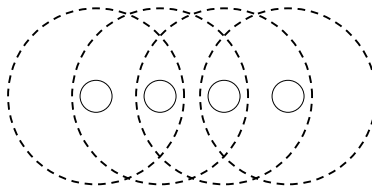
- ◆ MANET – “infrastructure-less”
- ◆ Transmission range
- ◆ Group coordination – routing



3

## Ad Hoc Routing Protocol

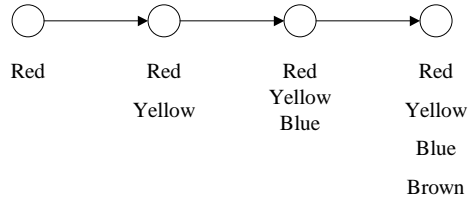
- ◆ Route discovery
- ◆ Source-driven
- ◆ Intermediate nodes forward & accumulate path



4

# Routing Example

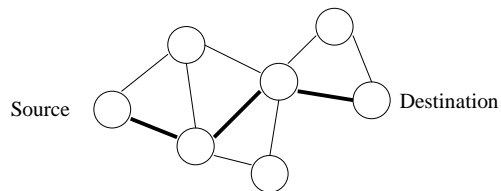
Route request  
issued by Red  
to Brown



5

# Security for MANETs

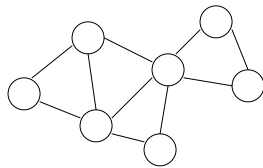
- ◆ Secure Routing Protocol (SRP)
- ◆ Goal – **guarantee** route to destination non-corrupted



6

## SRP Assumptions

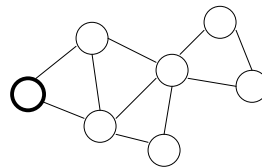
- ◆ Bi-directional communication
- ◆ Security Association (SA) between **source** and **target**, includes  $K_{S,T}$
- ◆ Non-colluding nodes



7

## SRP – Route request

- ◆ Issued by **source**
- ◆ Includes
  - Sequence number ( $Q_{seq}$ )
  - Unique identifier ( $Q_{ID}$ )
  - Message Authentication Code (MAC) using  $K_{S,T}$
  - Route field



8

# An Example of SRP

## 1. Route request



route

Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
R

- compute MAC from Source, Target,  $Q_{seq}$  and  $Q_{ID}$

9

# An Example of SRP

## 2. Query propagation



Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
R,Y

- check  $Q_{ID}$
- append IP-address

10

# An Example of SRP

## 2. Query propagation



<b>Source: R</b>
<b>Target: Br</b>
$Q_{seq}$
$Q_{ID}$
$MAC$
$R, Y, Bl$

11

# An Example of SRP

## Route request receipt



- validate  $Q_{seq}$  and  $MAC$

<b>Source: R</b>
<b>Target: Br</b>
$Q_{seq}$
$Q_{ID}$
$MAC$
$R, Y, Bl, Br$

12

# An Example of SRP

## 3. Route reply



- compute new *MAC* with *route*
- send response packet

route

Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
Br

13

# An Example of SRP



Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
Br,Bl

14

# An Example of SRP



<b>Source: R</b>
<b>Target: Br</b>
$Q_{seq}$
$Q_{ID}$
$MAC$
$Br, Bl, Y$

15

# An Example of SRP

## 4. Reply validation



<b>Source: R</b>
<b>Target: Br</b>
$Q_{seq}$
$Q_{ID}$
$MAC$
$Br, Bl, Y, R$

- check  $Q_{seq}$  and  $Q_{ID}$  for legitimacy
- compute and compare  $MAC$  using reverse of accumulated *route*

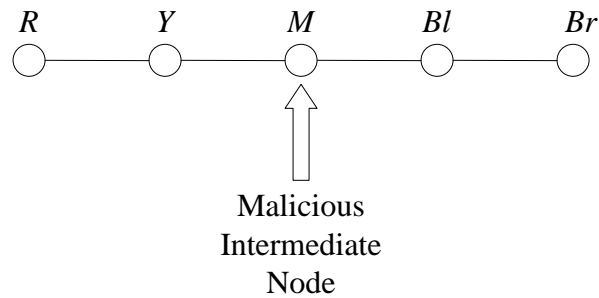
16

## Result of SRP

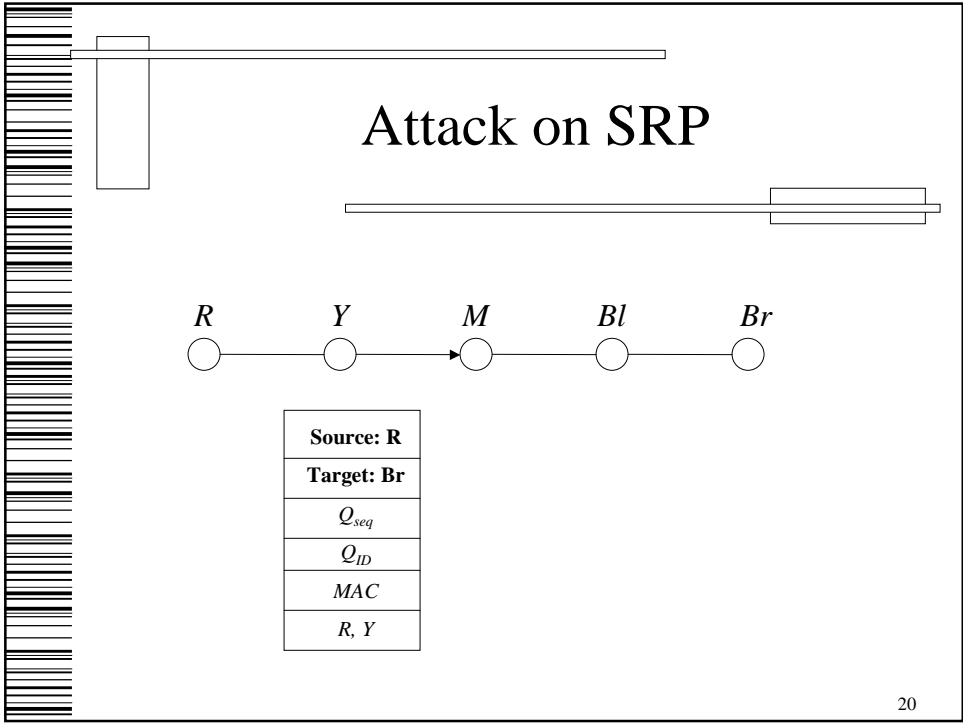
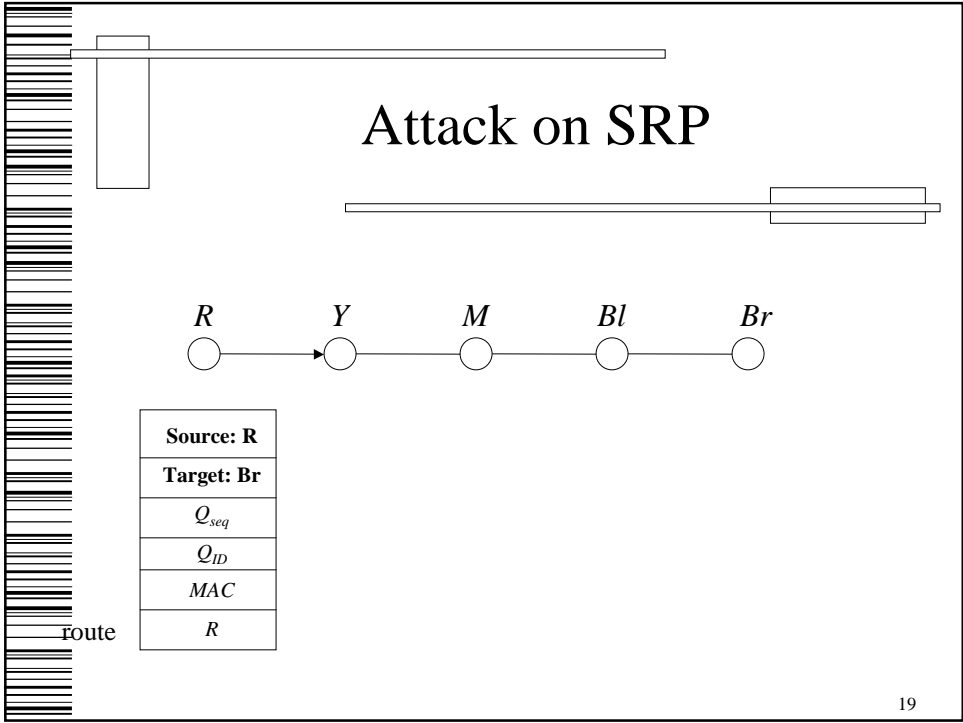
- ◆ Authors claim the route is **guaranteed** to be successfully established and legitimate
- ◆ Weaknesses
  1. Intermediate nodes not forced to append address
  2. Destination cannot authenticate *route*

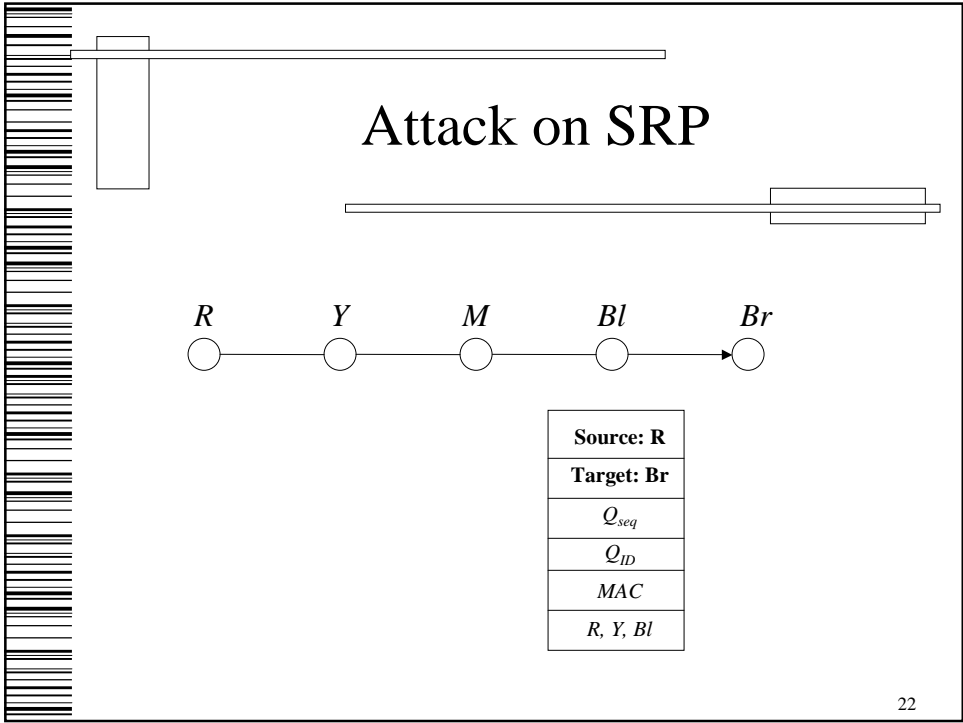
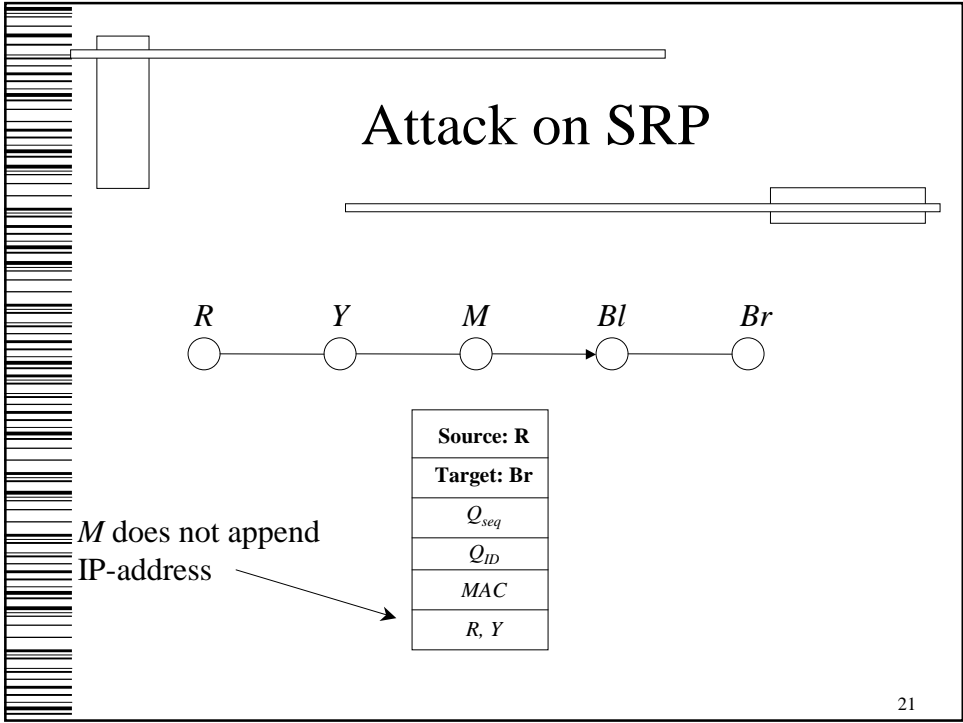
17

## Attack on SRP



18





# Attack on SRP

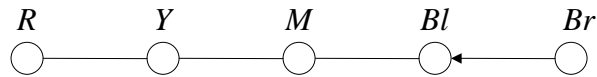


- **target** validates  $Q_{seq}$  and  $MAC$
- accepts route request packet
- issues route reply packet

Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
R, Y, Bl, Br

23

# Attack on SRP

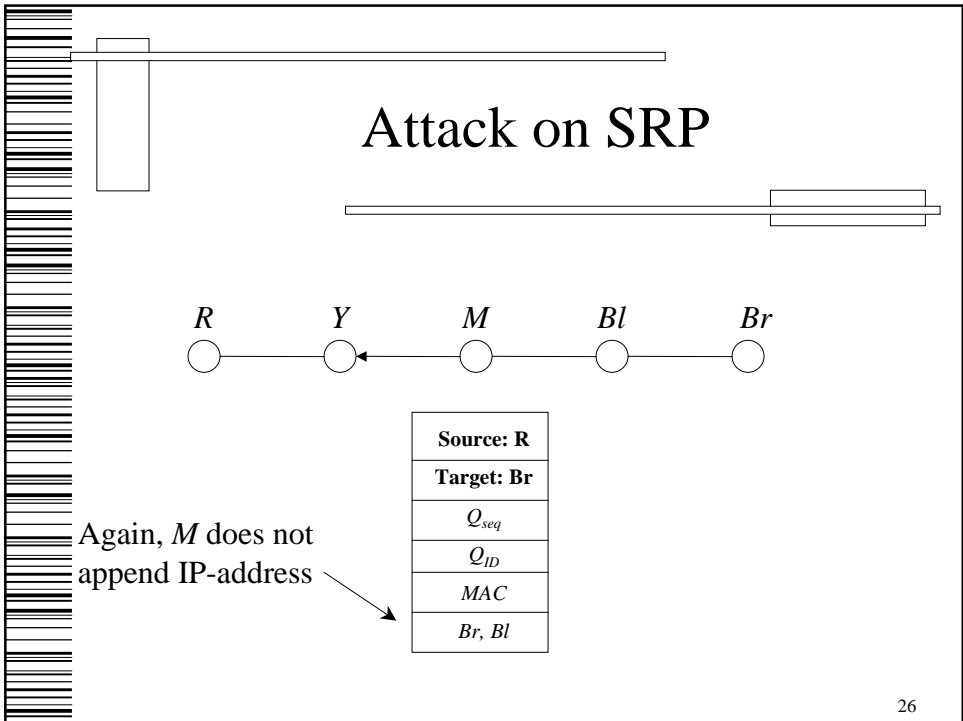
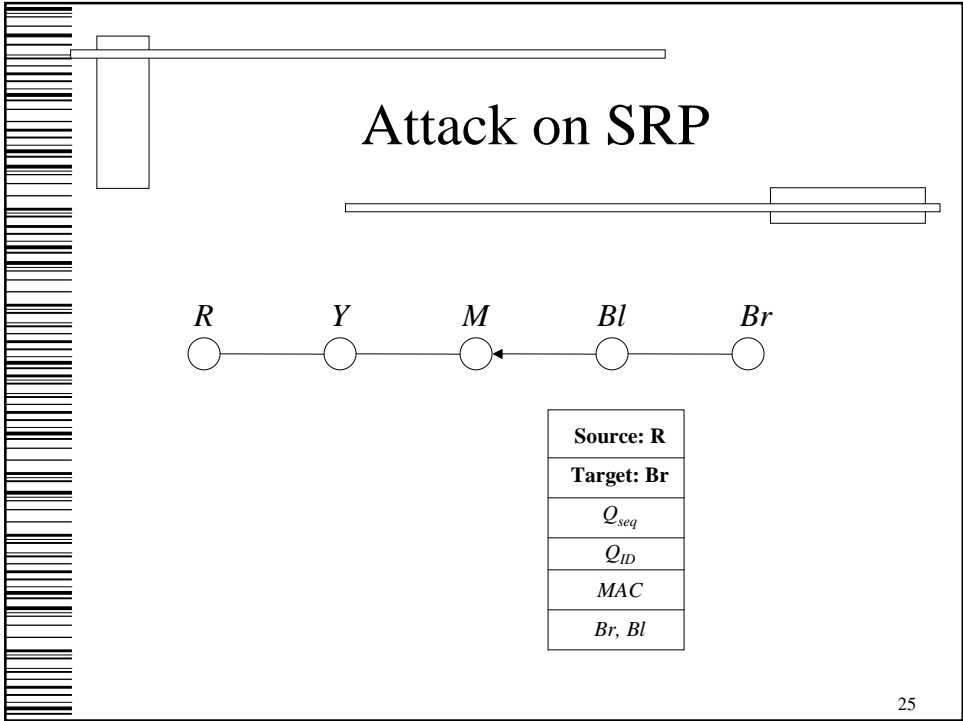


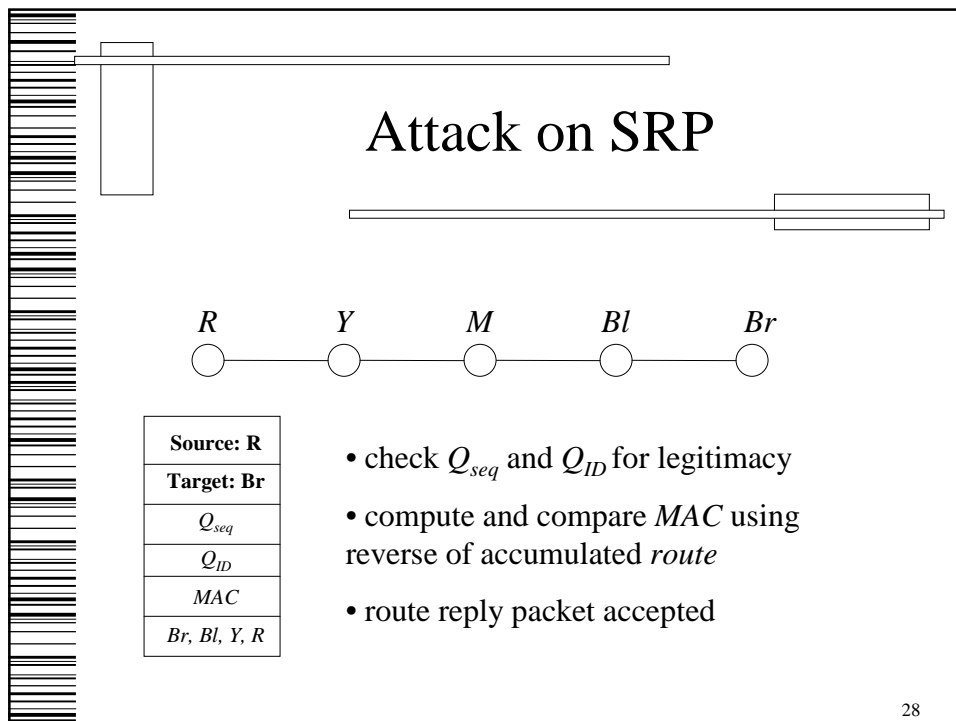
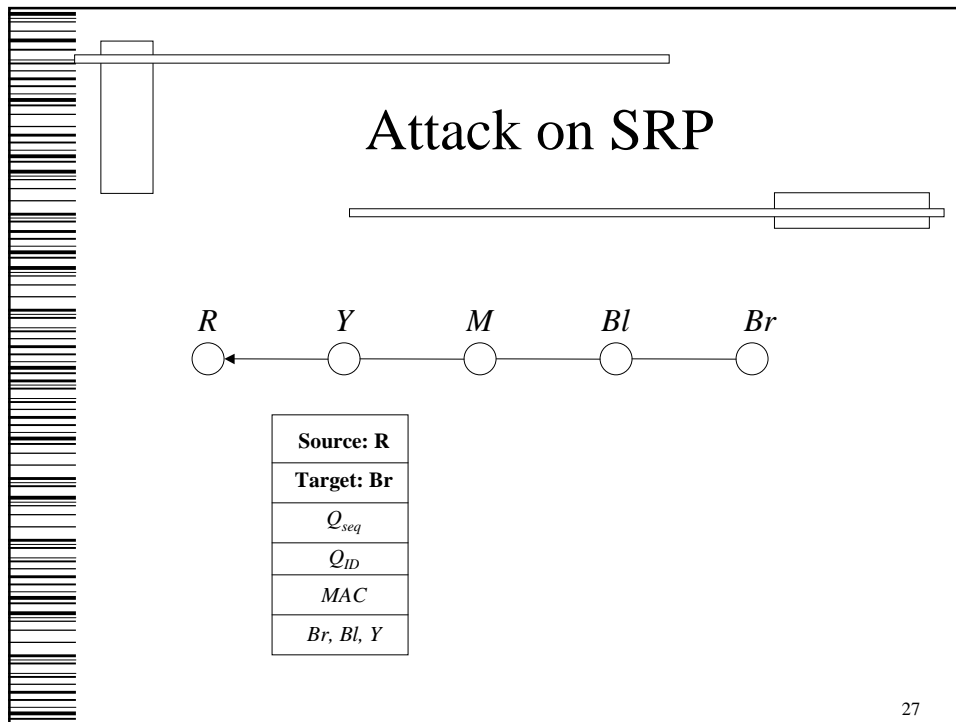
- route {R, Y, Bl, Br} part of  $MAC$

route

Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
Br

24





## Implications of Attack

- ◆ Source has erroneous *route*
- ◆ *route* depends on malicious node  $M$
- ◆  $M$  bears some level of control over *route*

29

## Solution Detecting the Attack

- ◆ Detects and mitigates node misbehavior
- ◆ *bloodhound*

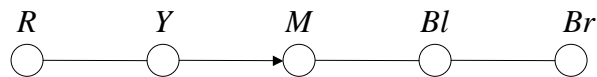
30

## *bloodhound*

- ◆ Node should never receive packet identical to one it sent
- ◆ *bloodhound* listens in to overhear identical packets

31

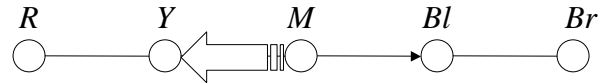
## Illustration of *bloodhound*



Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
R, Y

32

## Illustration of *bloodhound*



*M* does not append IP-address, so *M* broadcasts **identical** packet

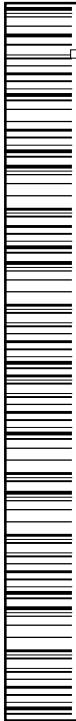
Source: R
Target: Br
$Q_{seq}$
$Q_{ID}$
MAC
R, Y

33

## Finding Attacks

- ◆ Intuitive attacks
- ◆ BAN logic analysis
- ◆ Formal methods (CPAL-ES)

34



Question, Comments,  
Answers...

35

The image shows a slide with a barcode on the left side. The text "Question, Comments, Answers..." is centered on the slide. There are several horizontal lines and rectangular boxes around the text, possibly indicating a design or editing process. The number "35" is located in the bottom right corner of the slide.