

# Security issues in Wireless Distance-Vector Routing Protocols

sef. lucr. dr. ing. Haller Piroska  
ing. Genge Bela

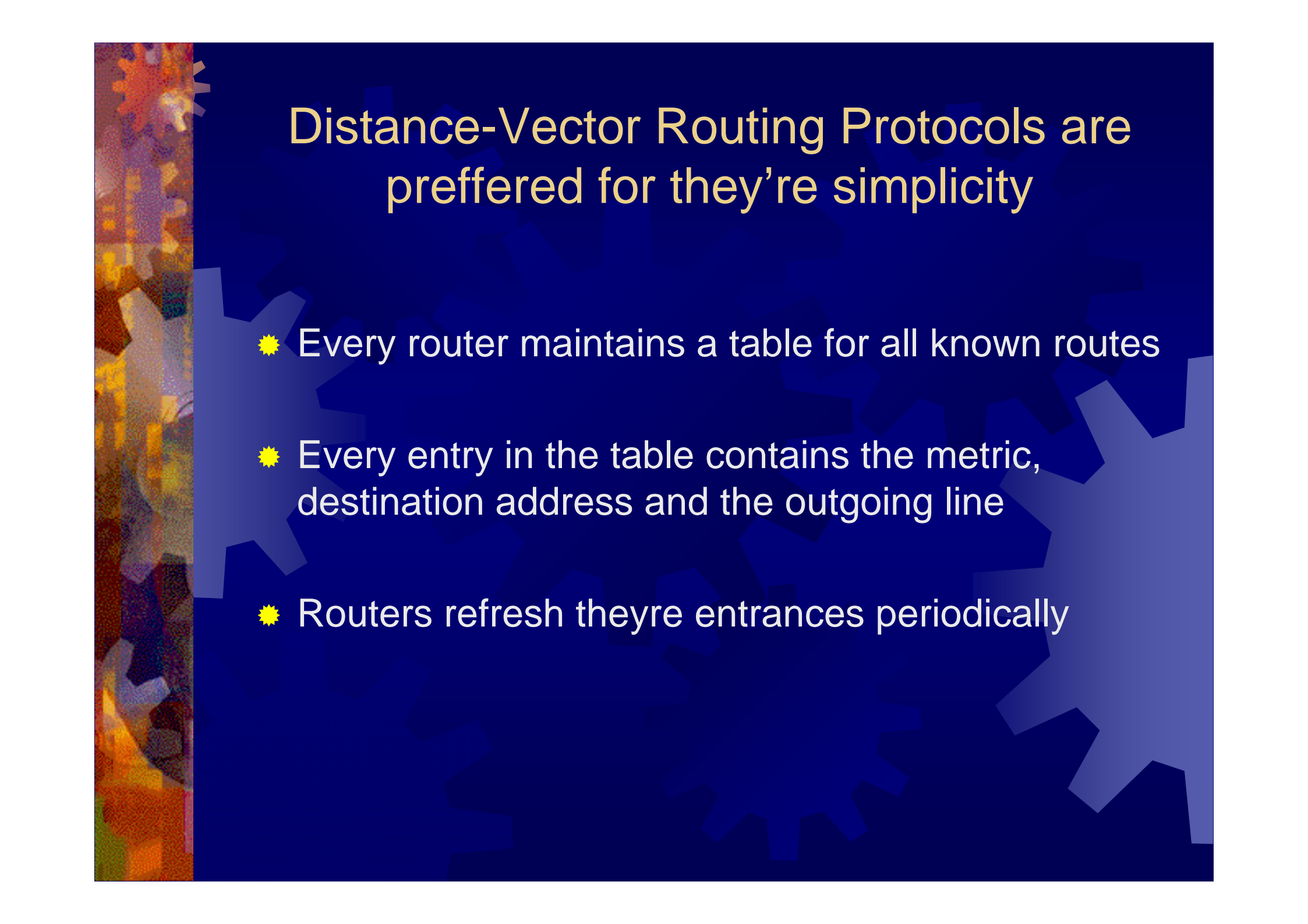
# What is a Wireless Ad Hoc Network?

## ★ A Wireless network where:

- The network does not have a fixed infrastructure
- The nodes can move around freely
- Nodes can appear and disappear in matter of seconds

## ★ Appliabilities:

- Emergency situations
- Military
- Where there is no possibility for creating a network fixed infrastructure



## Distance-Vector Routing Protocols are preferred for their simplicity

- ✦ Every router maintains a table for all known routes
- ✦ Every entry in the table contains the metric, destination address and the outgoing line
- ✦ Routers refresh their entries periodically



# “Denial of Service (DoS)” Attack

**Attack purpose:** occupy physical resources of router

**Achieving this attack:**

- ✦ Sending random packages
- ✦ Sending packages according to the communication protocol

**Defending against this attack:**

- ✦ Implementing multiple levels of authentication
- ✦ Implementing the “leaky bucket algorithm”
- ✦ Denial of packages from one specific interface – where the attack has been detected – announcing the admin



# Router Impersonation

**Attack purpose:** routing table modification

## **Achieving this attack:**

- ✦ Conversation listening – package spoofing
- ✦ Modifying the spoofed packages and injecting invalid routes

## **Defending against this attack:**

- ✦ Implementing an introduction protocol for newly started routers – like the “resurrecting duckling” principle
- ✦ Using session passwords between two routers – for Wireless environments the HMAC is more preferred as a MAC for packages

# Atacul tip Ignoranță

**Attack purpose:** ignore all received packages

**Achieving this attack:**

- ✦ Total compromise of a router
- ✦ Autointroduction of the attacking router as a valid router

**Defending against this attack:**

- ✦ If the attacking router succeeds in finding out all the passwords and introduce himself as a valid router, there is no defence possibility – this kind of attack is a rather inoffensive

# “Wormhole” Attack

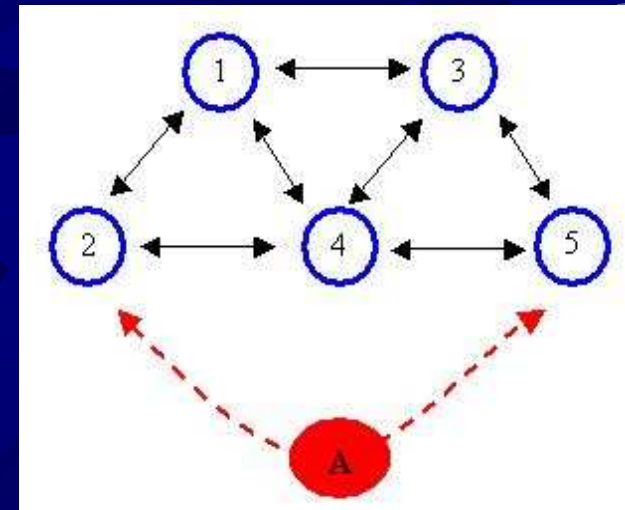
**Attack purpose:** package captureing

**Achieving this attack:**

- ✦ The attacker places himself between two routers
- ✦ Transmitting of packagers from one router to another, making the impression that the 2 routers are adjacent

**Defending against this attack:**

- ✦ Implementing packet leases:
  - ✦ Timestamp
  - ✦ Geographic stamp



# Injection of shorter routes

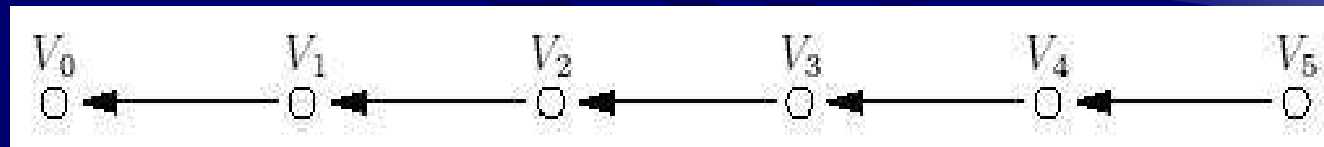
**Attack purpose:** traffic deviation, package capturing

**Achieving this attack:**

- ★ Total compromise of a specific router – determining all the passwords and security protocols

**Defending against this attack:**

- ★ Implementing One-Way HASH chains



Where:  $V_5 = \text{RAND}$ ,  $V_4 = H(V_5)$ ,  $V_3 = H(V_4)$ ,  $V_2 = H(V_3)$ ,  $V_1 = H(V_2)$ ,  $V_0 = H(V_1)$   
H may be SHA1 or MD5

# Injection of same-distance routes

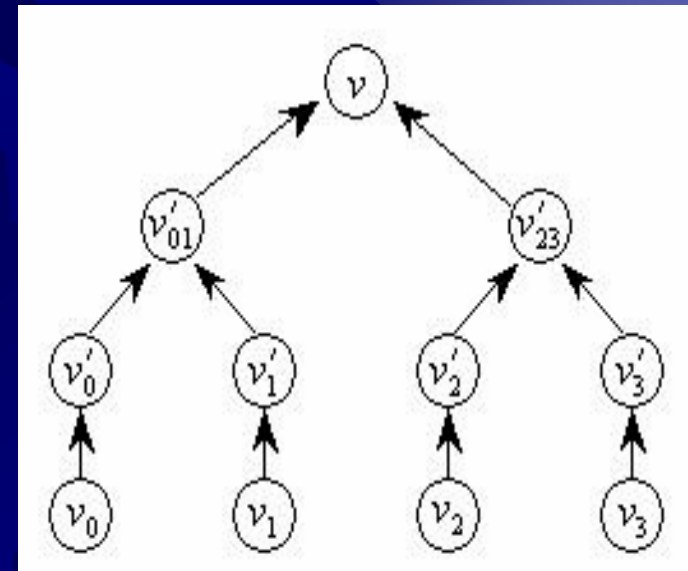
**Attack purpose:** traffic deviation, package capturing

**Achieving this attack:**

- ☀ Completely compromise a router
- ☀ Repeat same package

**Defending against this attack:**

- ☀ Construct HASH trees where each node is an element of the tree, having a specific ID





Thanks for you're attention!