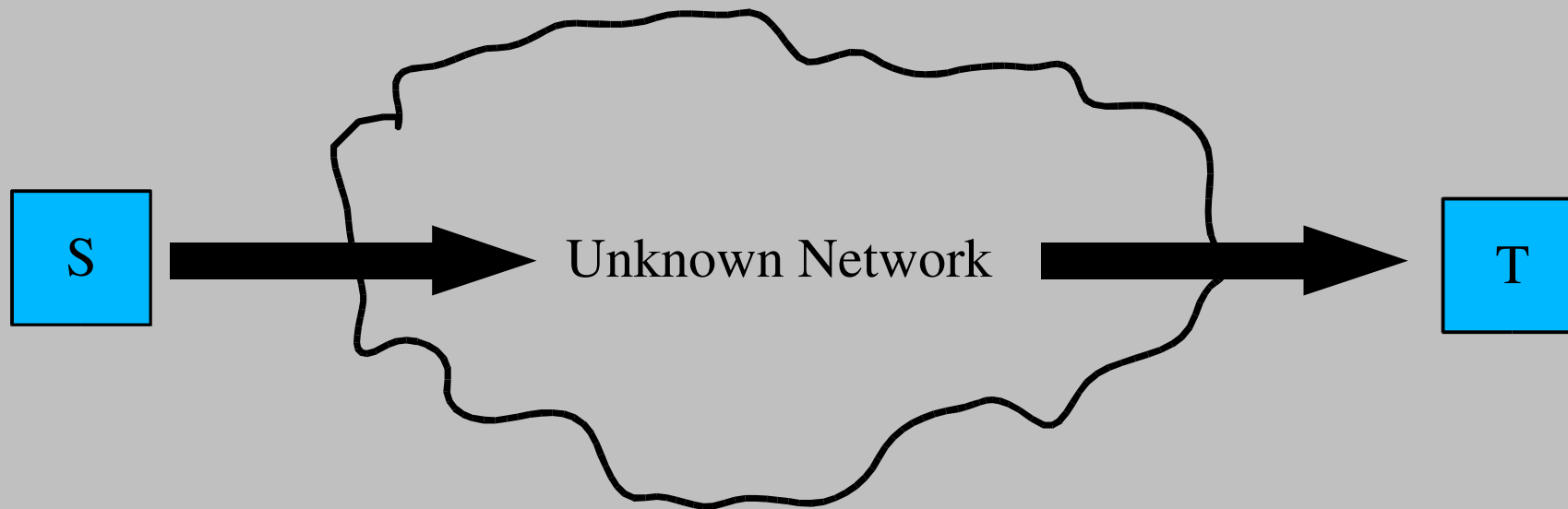


Secure Message Transmission in Mobile ad hoc Networks

(SMT in MANET)

Based on a paper by: Panagiotis Papadimitratos and Zygmont J. Haas
Presentation by: Christoph Probst
Date: 27/05/2004

1. Introduction to wireless communication
2. Possible attacks to wireless communication
3. The SMT protocol
4. Requirements, Redundancy, Adaption, ...
5. Performance
6. Related Work
7. Conclusion

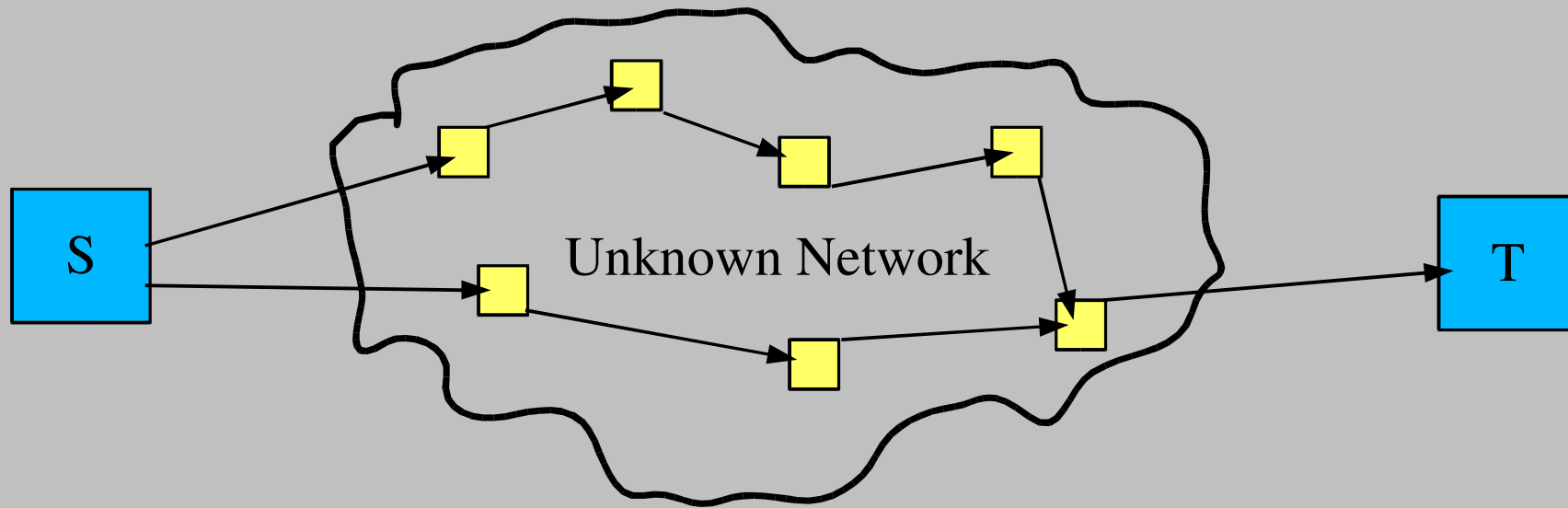


Unknown Networks are insecure by definition.

How can we set up a reliable connection between Source and Target?

Communication Process has Two Phases (1)

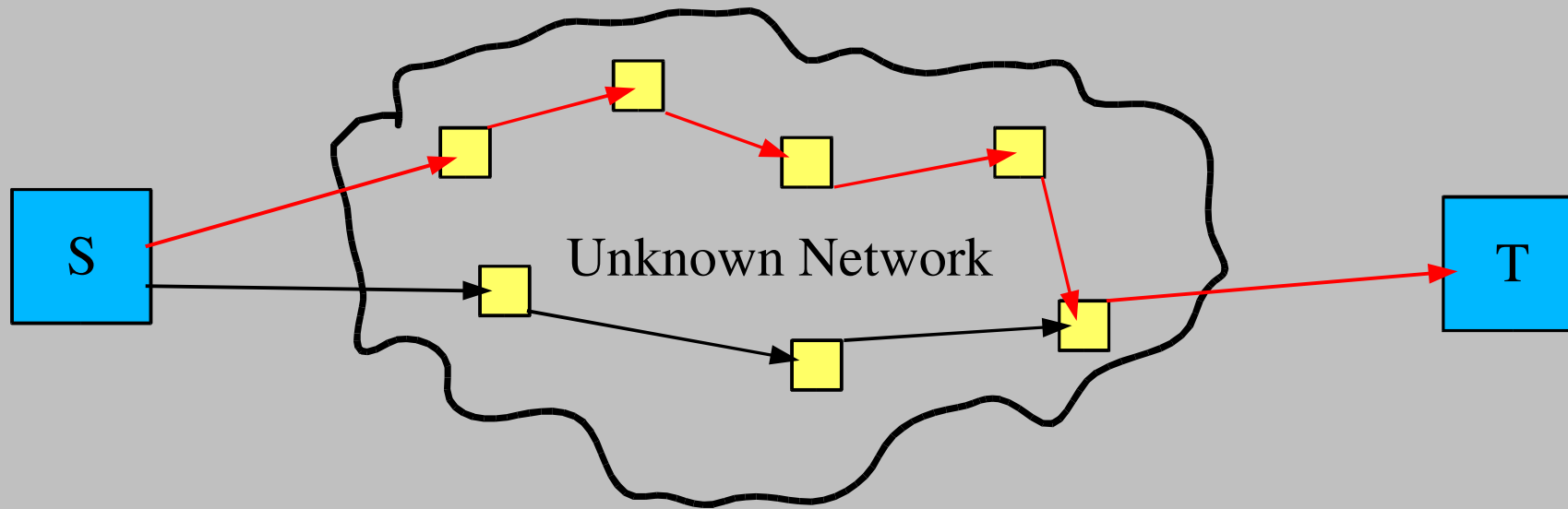
Phase 1: Find at least one path through the network from S to T.



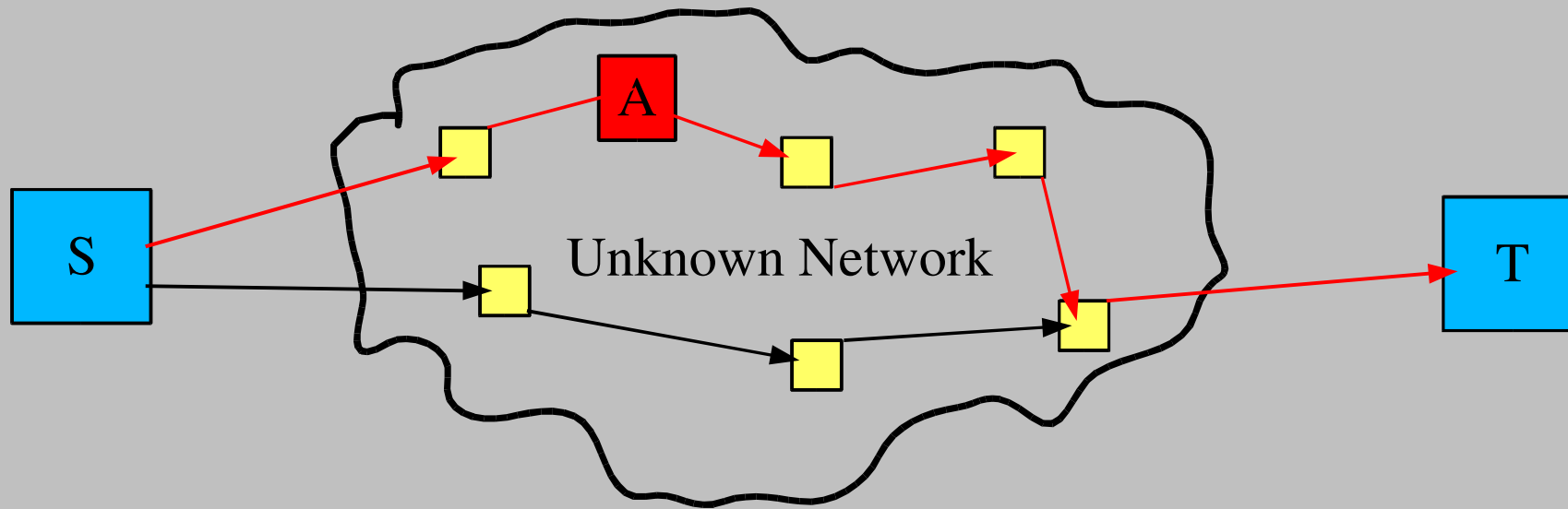
- Not in the responsibility of the SMT protocol
- Done by protocols like Secure Routing Protocol (SRP)
- Better more than a single path: We want an “Active Path Set” (APS)

Communication Process has Two Phases (2)

Phase 2: Transmit a message from S to T



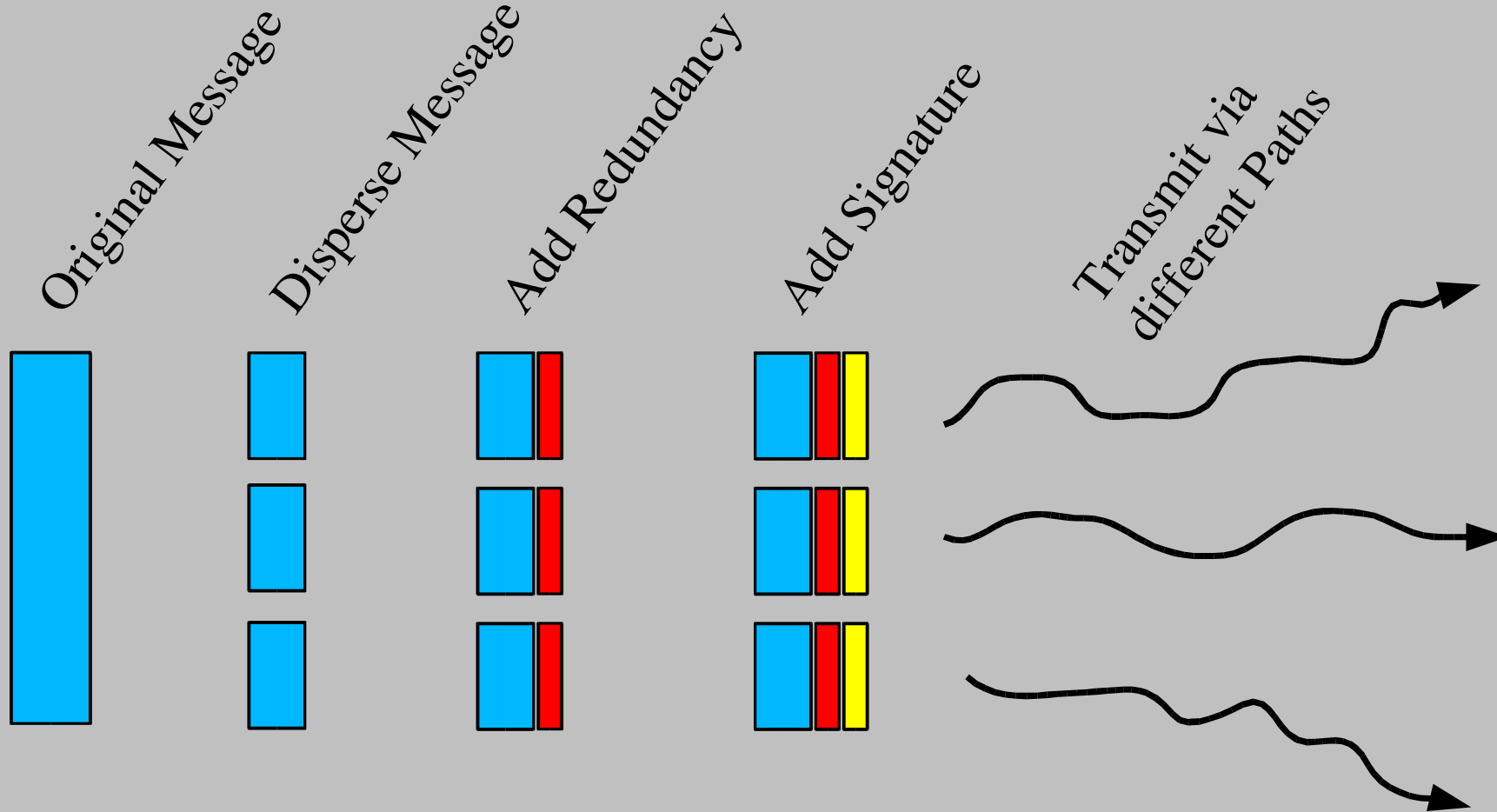
- Normally using a single path
- Only this phase is improved by SMT protocol



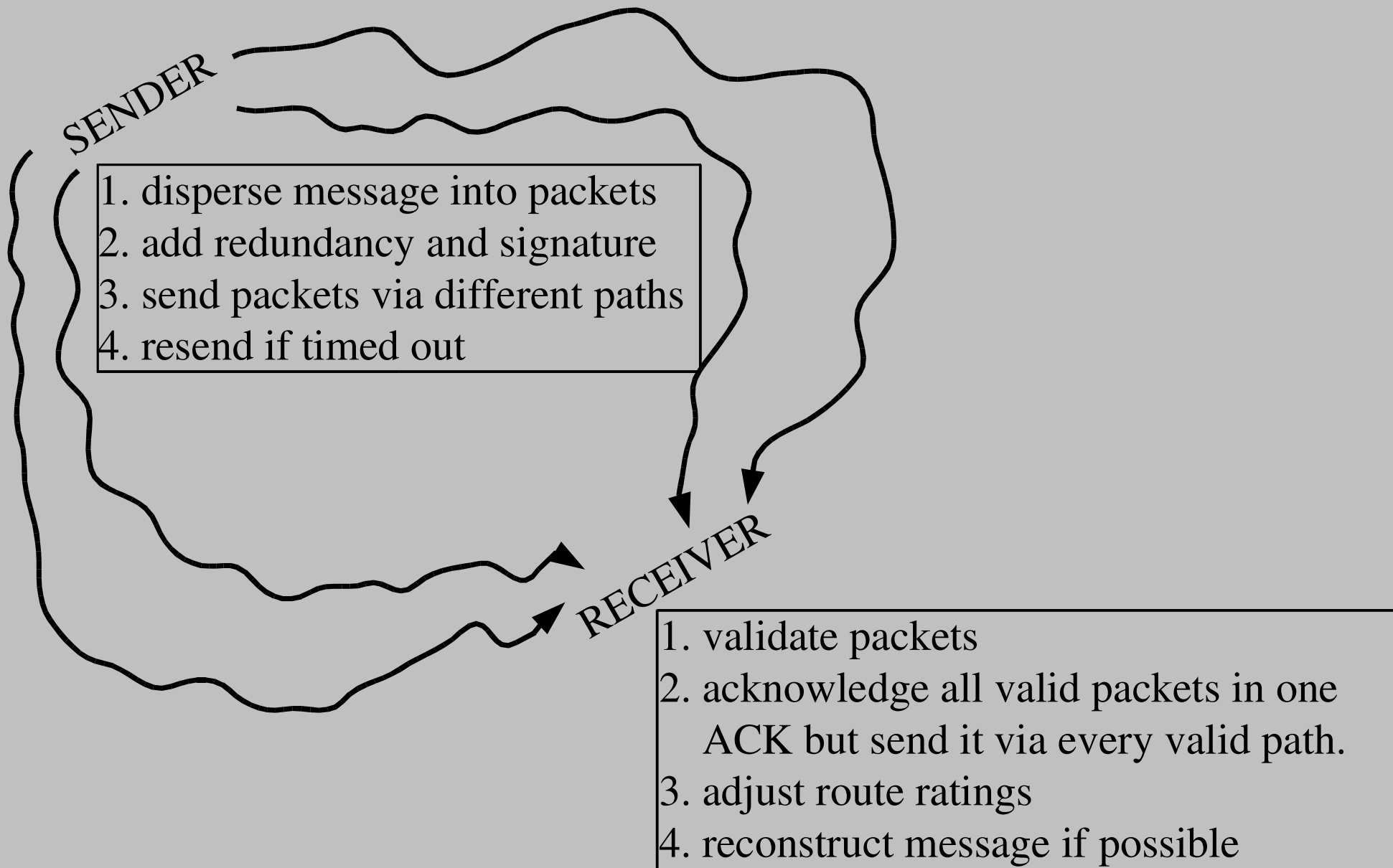
Attacker (A) can

- manipulate, fake or drop messages
- manipulate or block route
- wait for the best opportunity or do nothing

Neither S nor T can rely on the network!



How is a Message send?



Communicating Hosts share a secret for redundancy.

Communicating Hosts share a secret for signature verification

At least one route is NOT compromised.

Routing Protocol provides more than one route (APS)

1. Source and Target share a secret A
2. Source multiplies the A matrix by the message matrix (**Matrix Multiplication**)
3. The result matrix has N lines and is transmitted to Target.

$$\begin{matrix} A \\ (N \times M) \end{matrix} * \text{Message } (M \times L) = \text{Result } (N \times L)$$

4. Target multiplies **Inverse** of A by the transmitted matrix. Even if a single line is missing the Message will still be recovered!

$$\begin{matrix} A^{-1} \\ (N \times M) \end{matrix} * \text{Transmitted } (? \times L) = \text{Message } (M \times L)$$

The choice of the current Active Path Set is made out of the number of hops within a route. And change

Failed Transmission

Short Term Rating



Successful Reception

Short Term Rating



Successful Reception

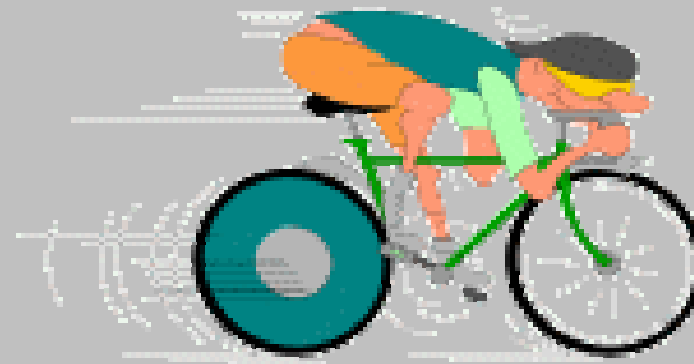
Log Term Rating



- * non-operational routes are promptly discarded (if rate drops below a certain value.
- * there is a maximum Rating but no bonus for routes, even if they were operational for a long time.

Compared to other protocols like **Secure Single Path (SSP)** and **Non-secure Single Path (NSP)** **Secure message transmission (SMT)** usually performs better:

- Higher number of successful transmissions within high numbers of adversaries.
- Lower end to end delays (as using multiple routes)
- Overhead generally only marginal higher than in SSP



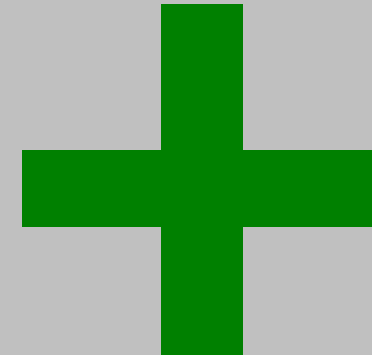
SSP (Secure Single Path): Like SMT but only using a single path and no dispersion.

IPSec (IP Secure): Assumes fixed routing and security infrastructure --> not applicable to MANET

SCTP (Stream Control Transport Protocol): Is vulnerable to intermittent attacks. --> not applicable to MANET

SMT ...

- ... can deal with a high number of adversaries
- ... handle most common attacks
- ... performs quite good even under high load
- ... works even with just a single path



- ... has a routing overhead (to discover the ASP)
- ... falls back to SSP when only a single path is left

