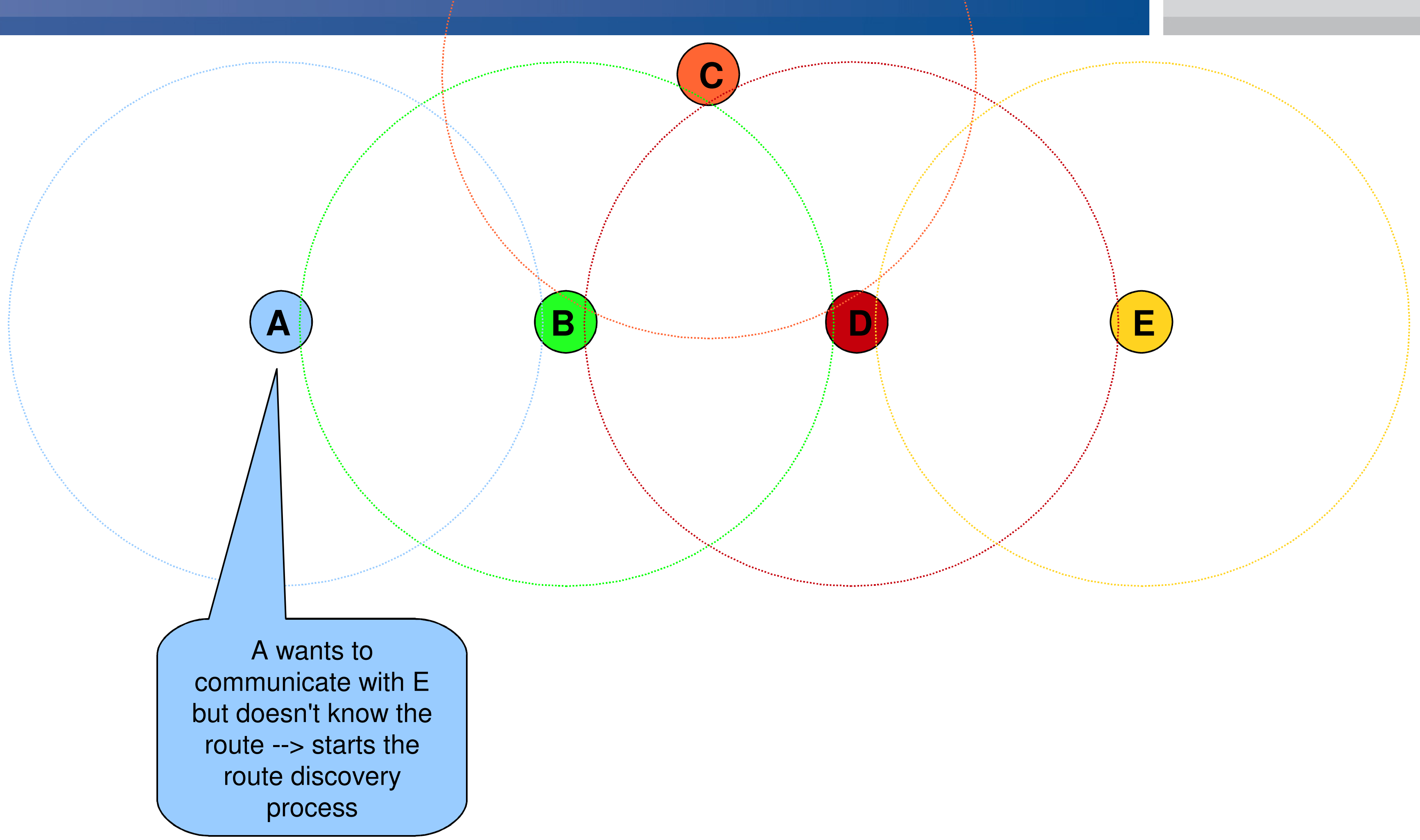
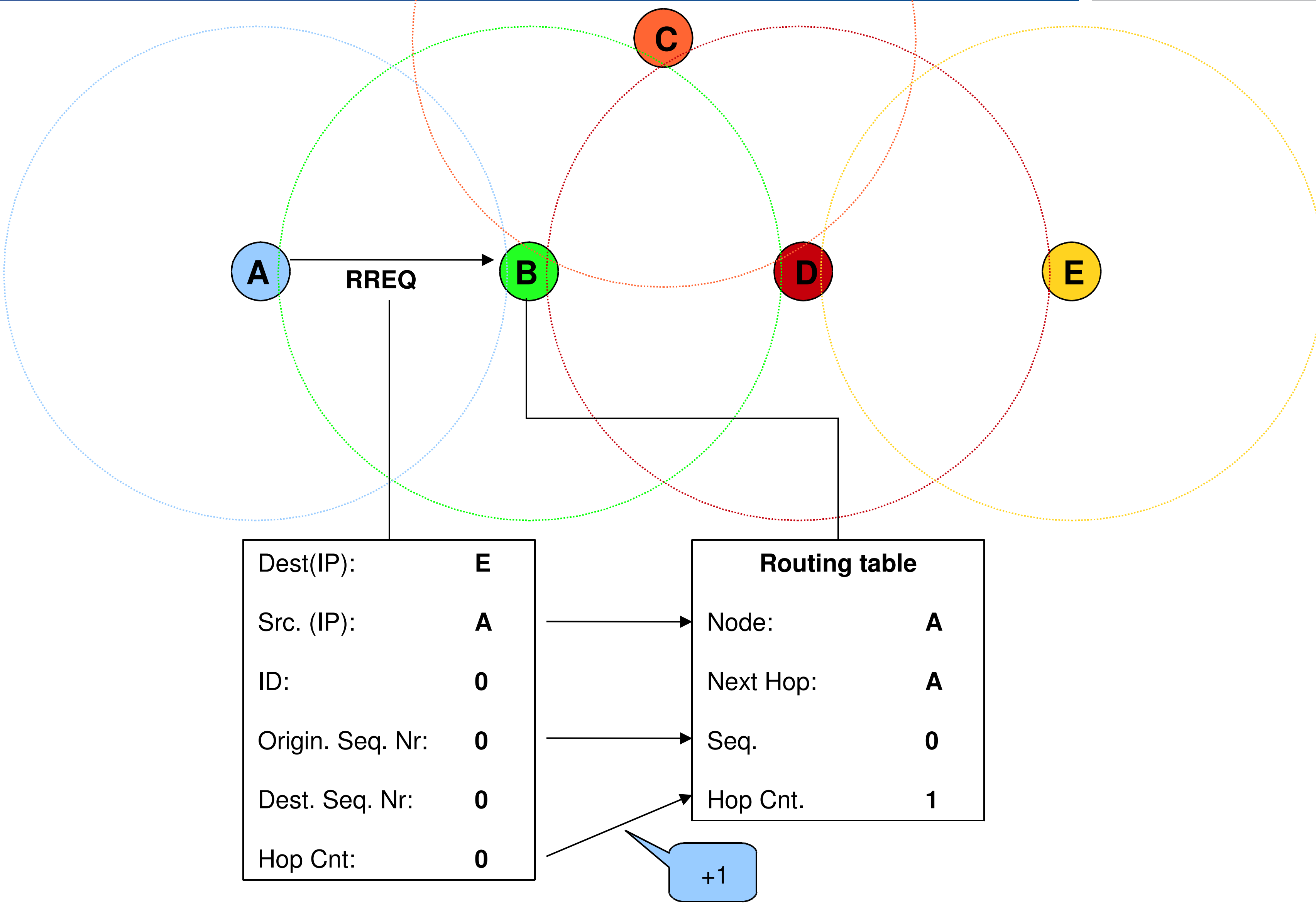
CASE STUDY:
Formation and Prevention of Hidden-mode Wormholes in the AODV (Ad hoc On Deman Distance Vector) protocol

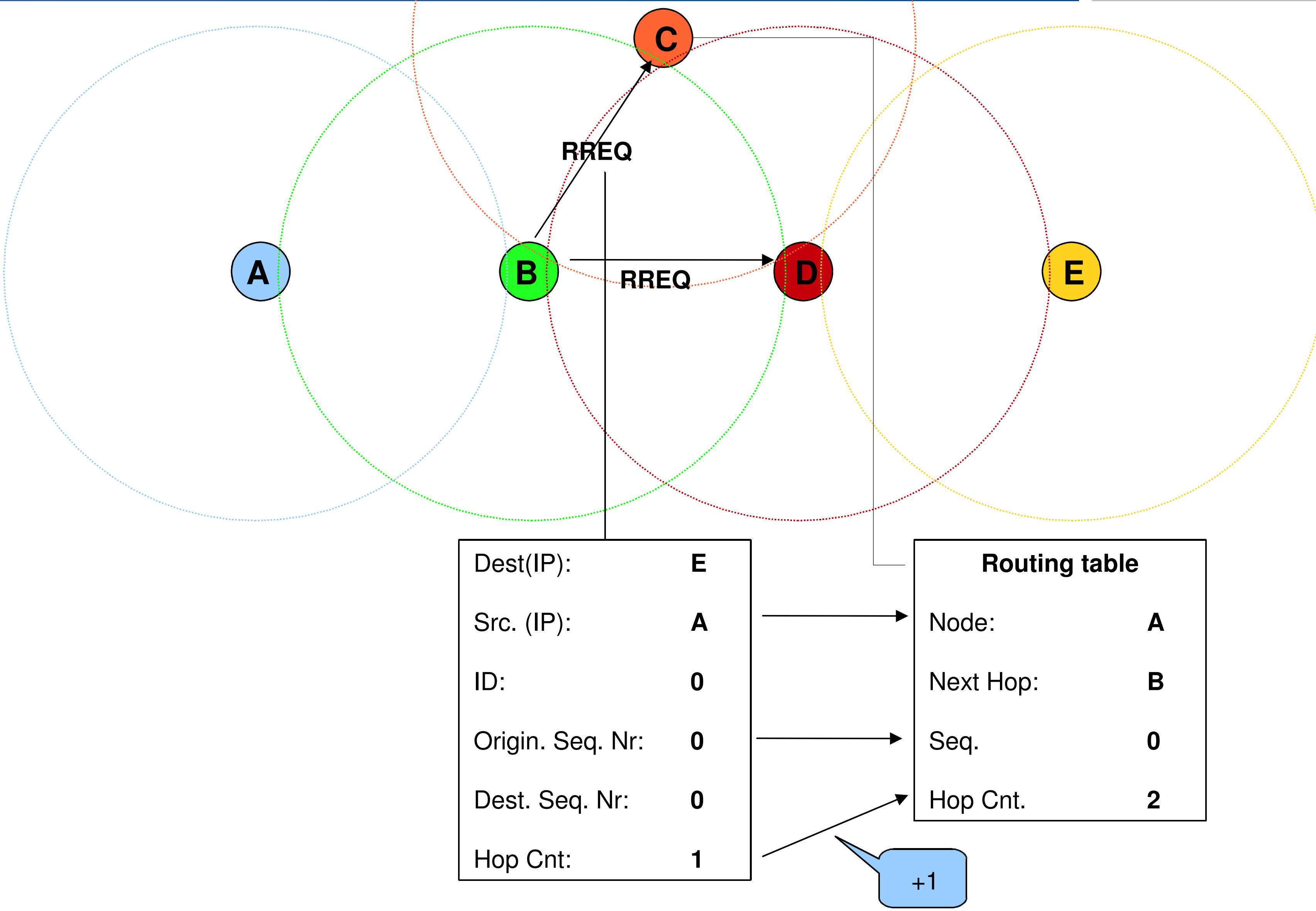
Research meeting 10.6.2009 – Jonny Karlsson



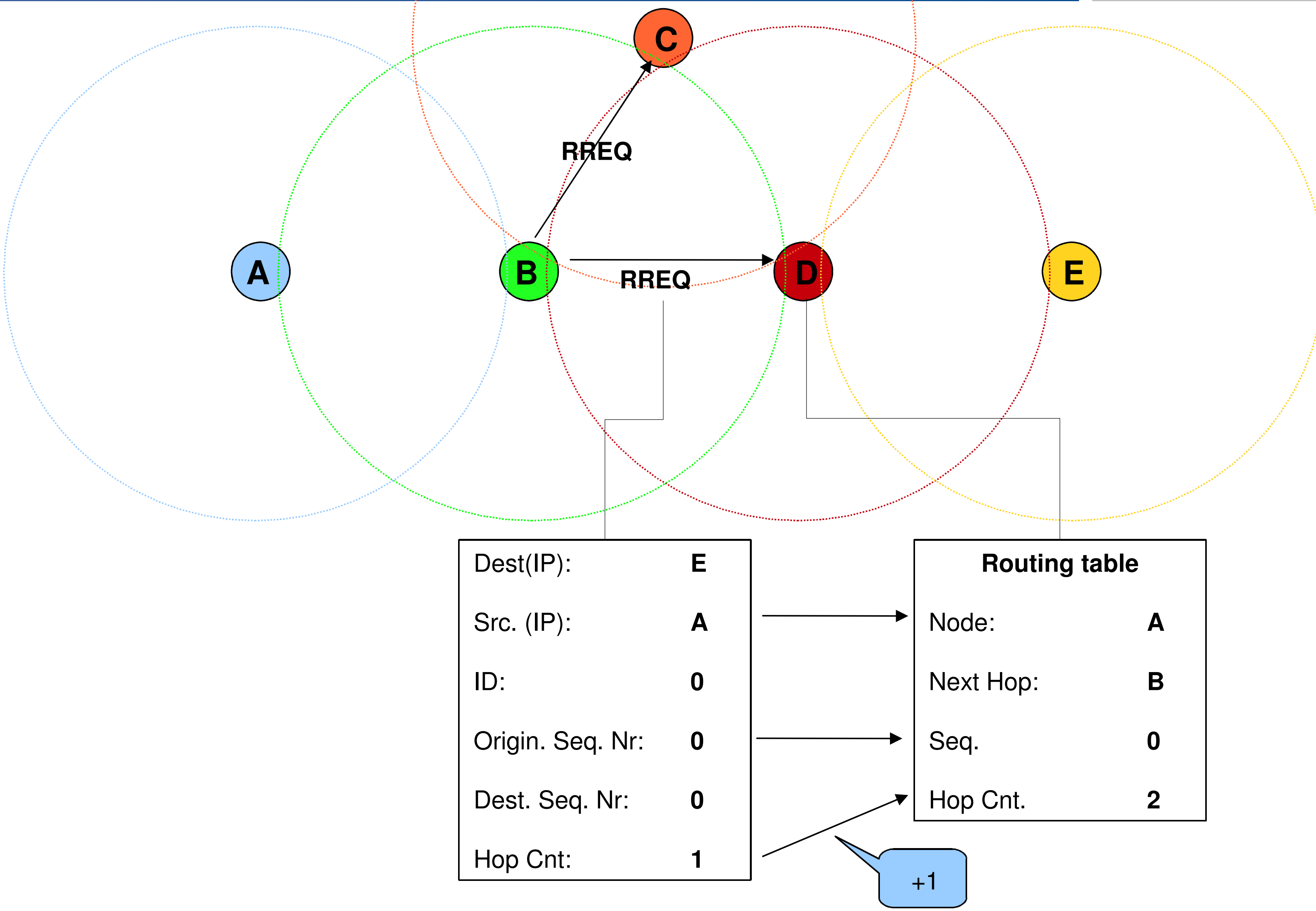
The AODV Route Discovery Process



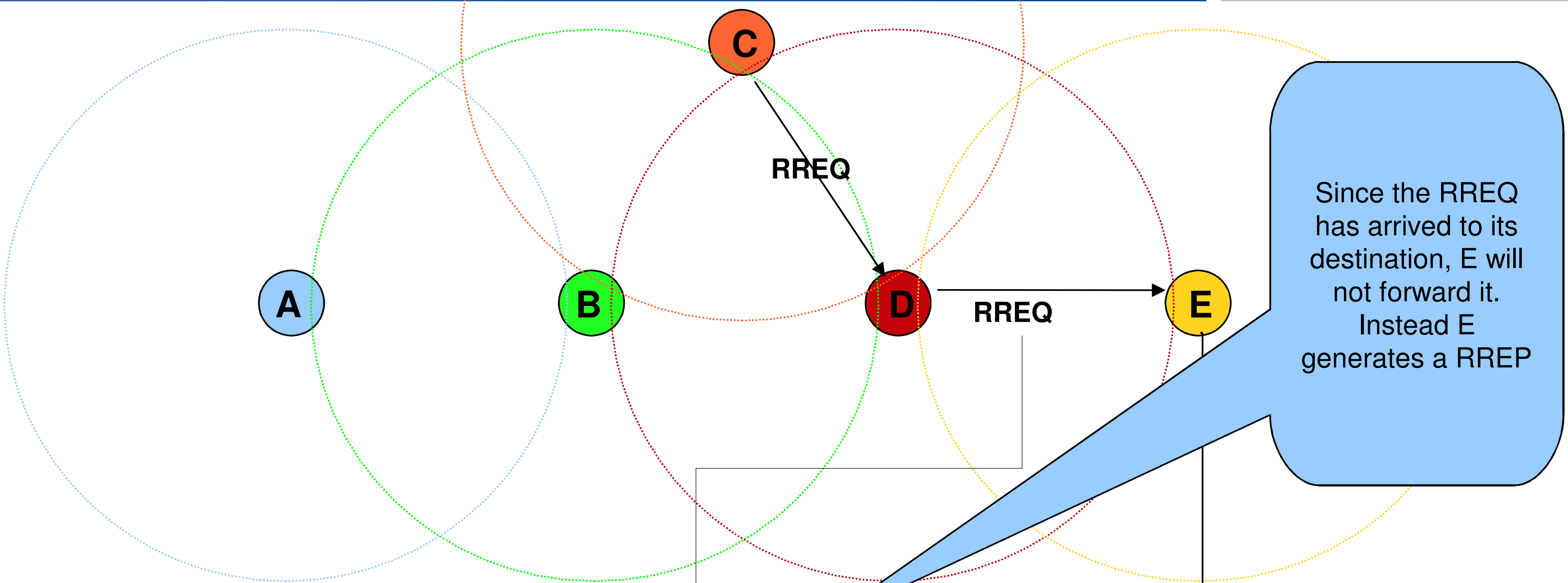
The AODV Route Discovery Process



The AODV Route Discovery Process



The AODV Route Discovery Process

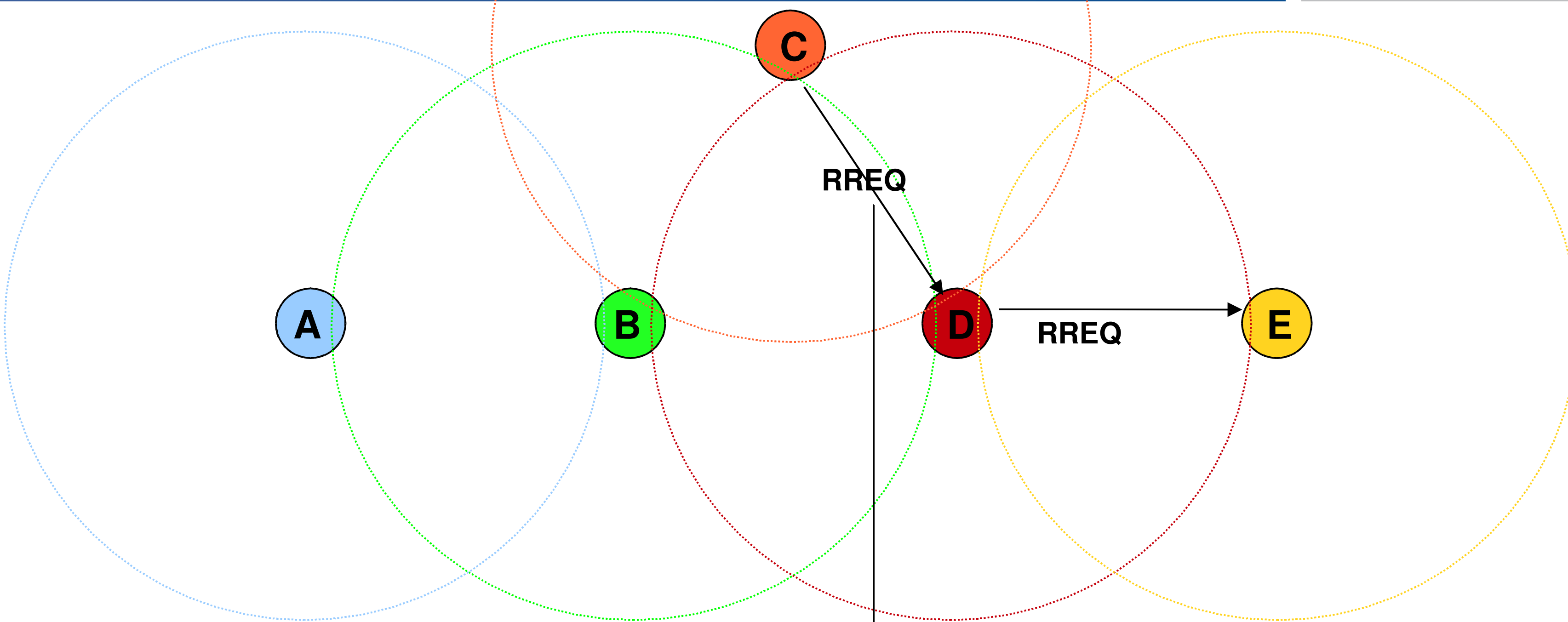


Dest(IP):	E
Src. (IP):	A
ID:	0
Origin. Seq. Nr:	0
Dest. Seq. Nr:	0
Hop Cnt:	2

Routing table	
Node:	A
Next Hop:	D
Seq.	0
Hop Cnt.	3

+1

The AODV Route Discovery Process

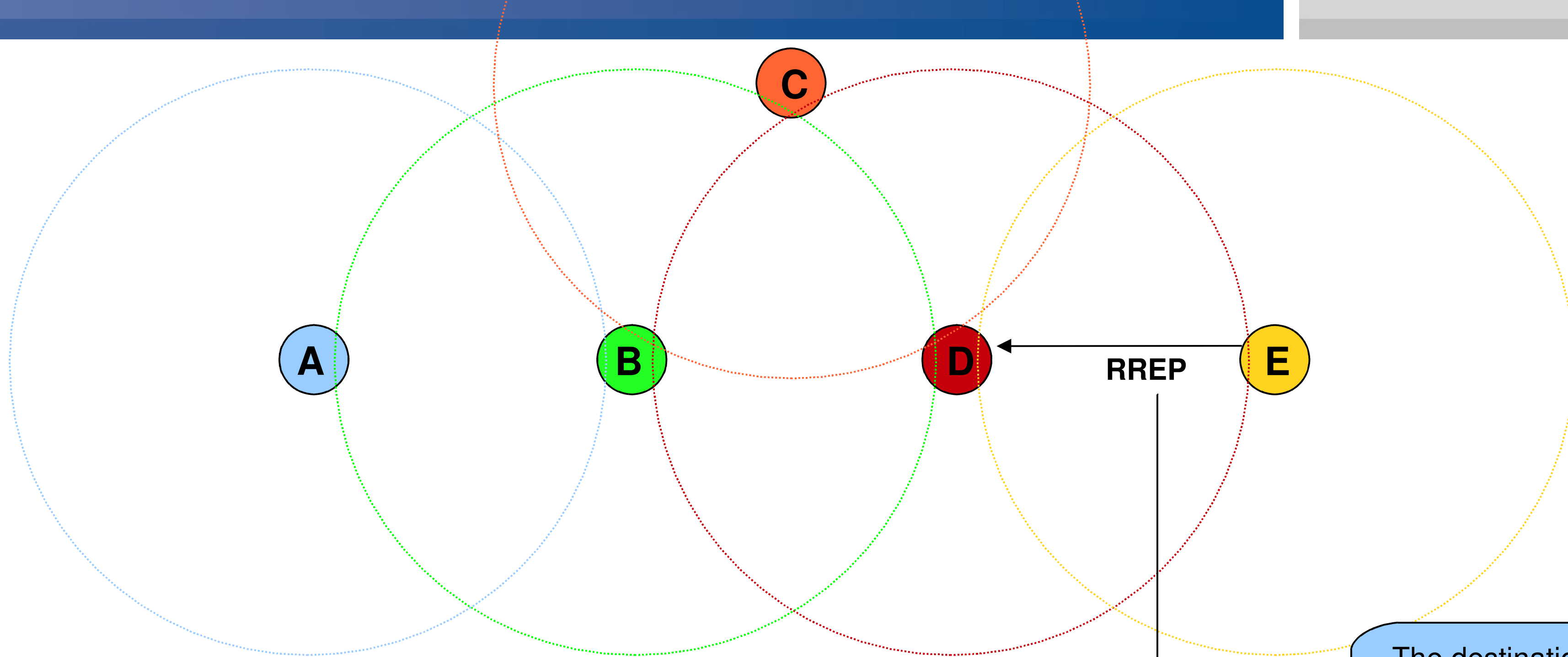


Dest(IP):	E
Src. (IP):	A
ID:	0
Origin. Seq. Nr:	0
Dest. Seq. Nr:	0
Hop Cnt:	2

A RREQ with this combination has been received earlier.
-> D will not forward the RREQ

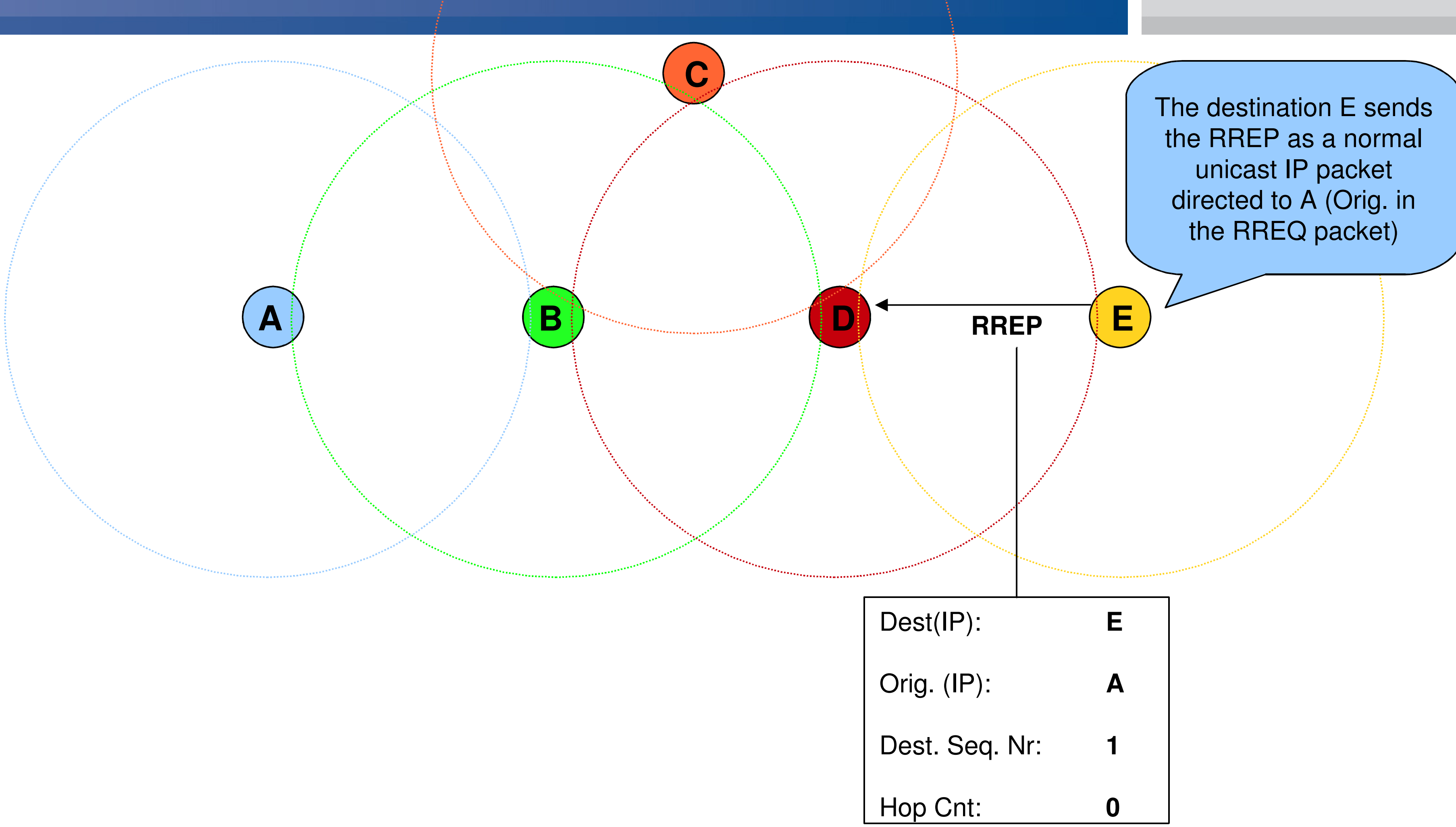
The AODV Route Discovery Process

The AODV Route Discovery Process

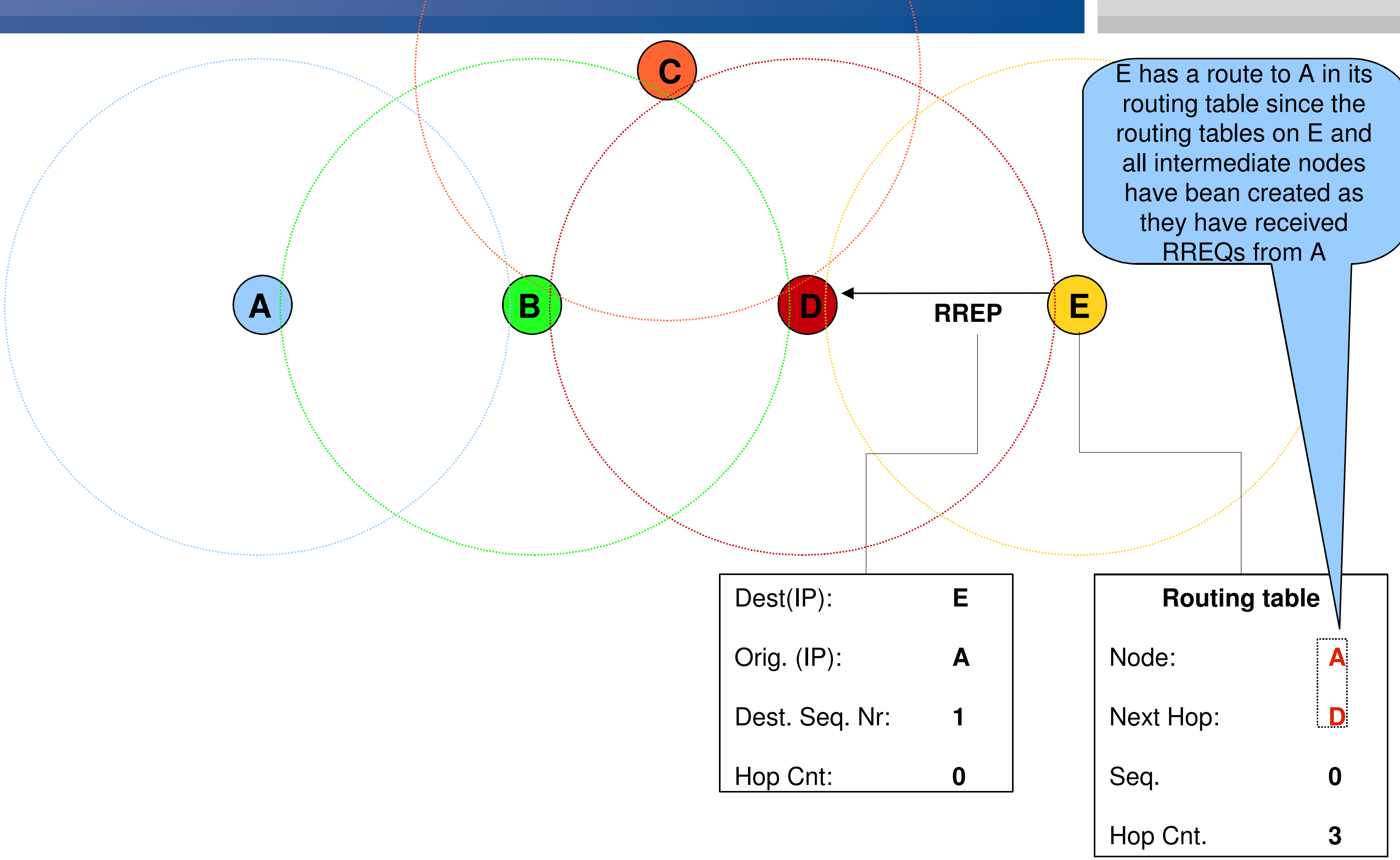


Dest(IP):	**E**
Orig. (IP):	**A**
Dest. Seq. Nr:	**1**
Hop Cnt:	**0**

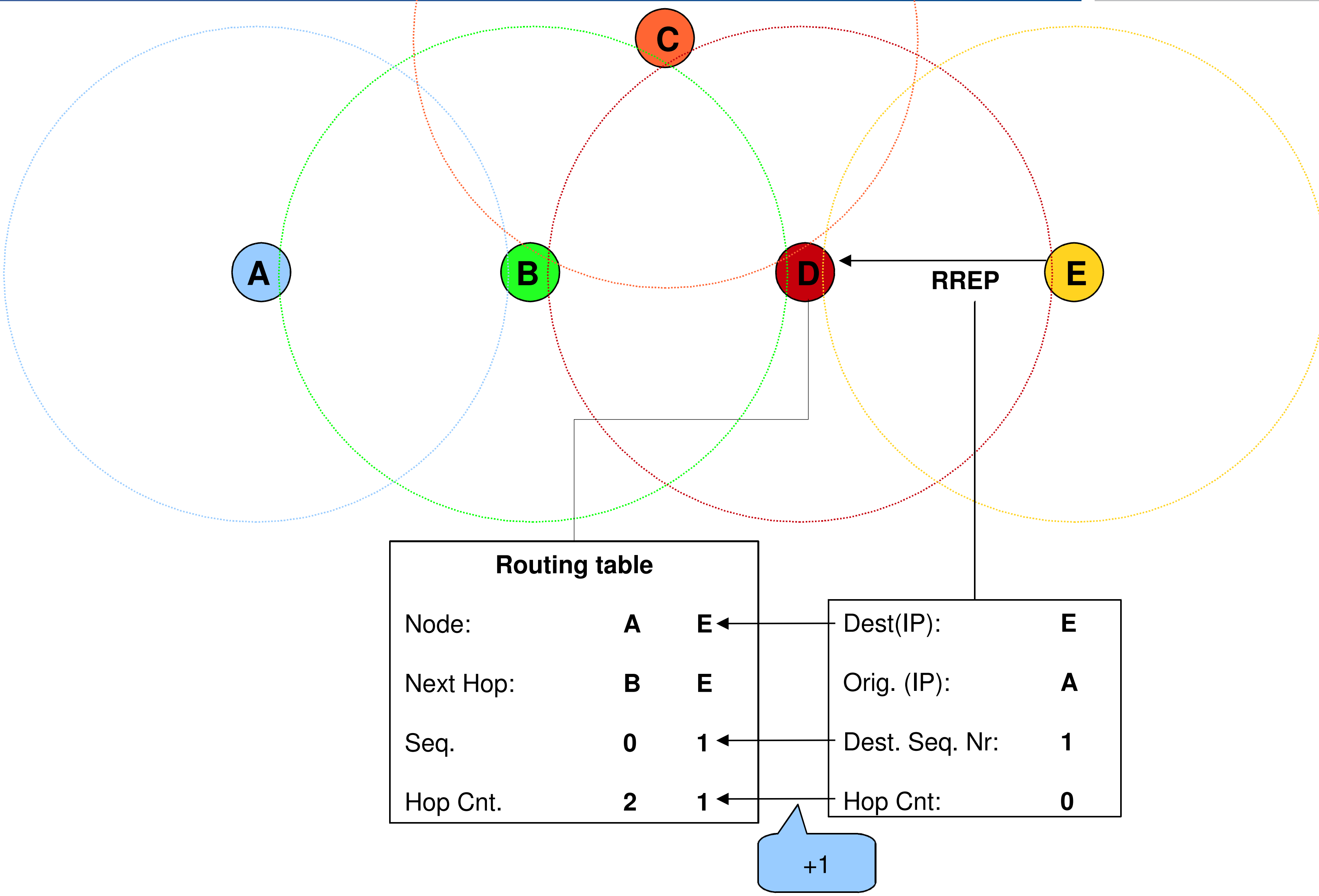
The destination E has incremented its sequeuence number by 1



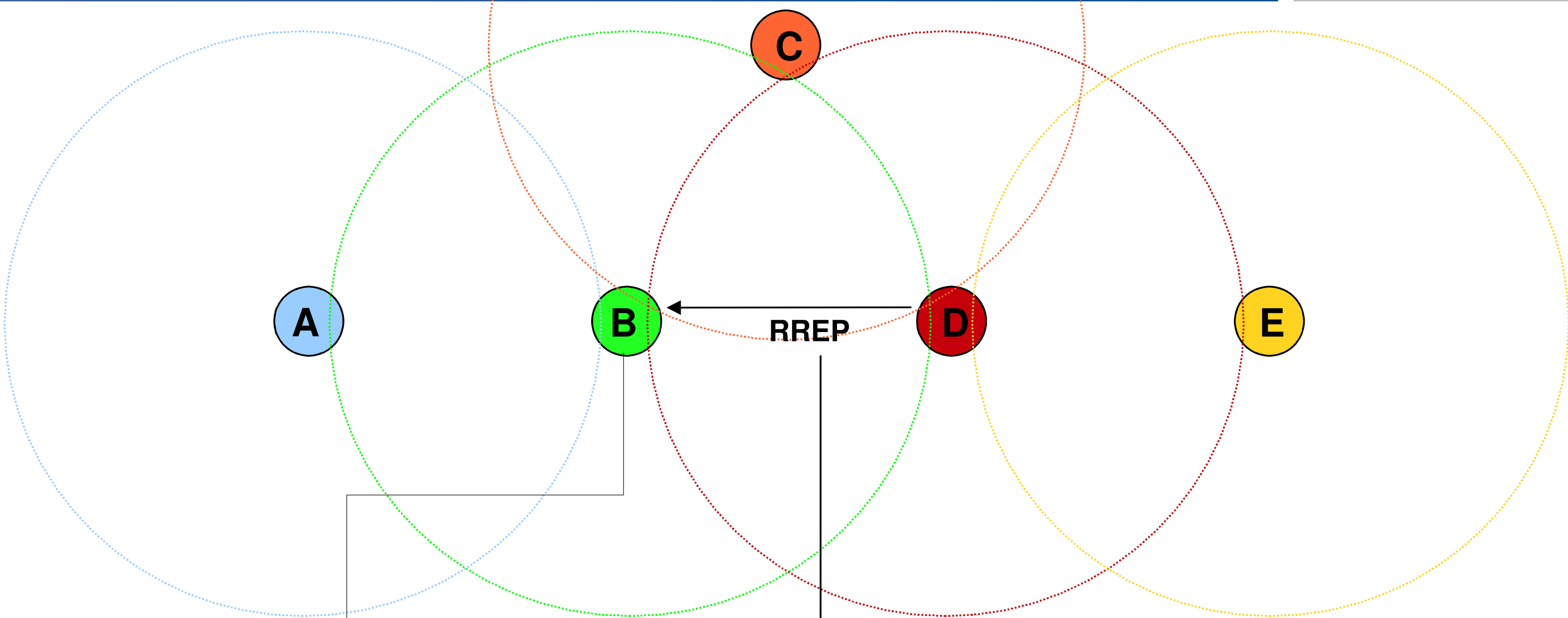
The AODV Route Discovery Process



The AODV Route Discovery Process



The AODV Route Discovery Process



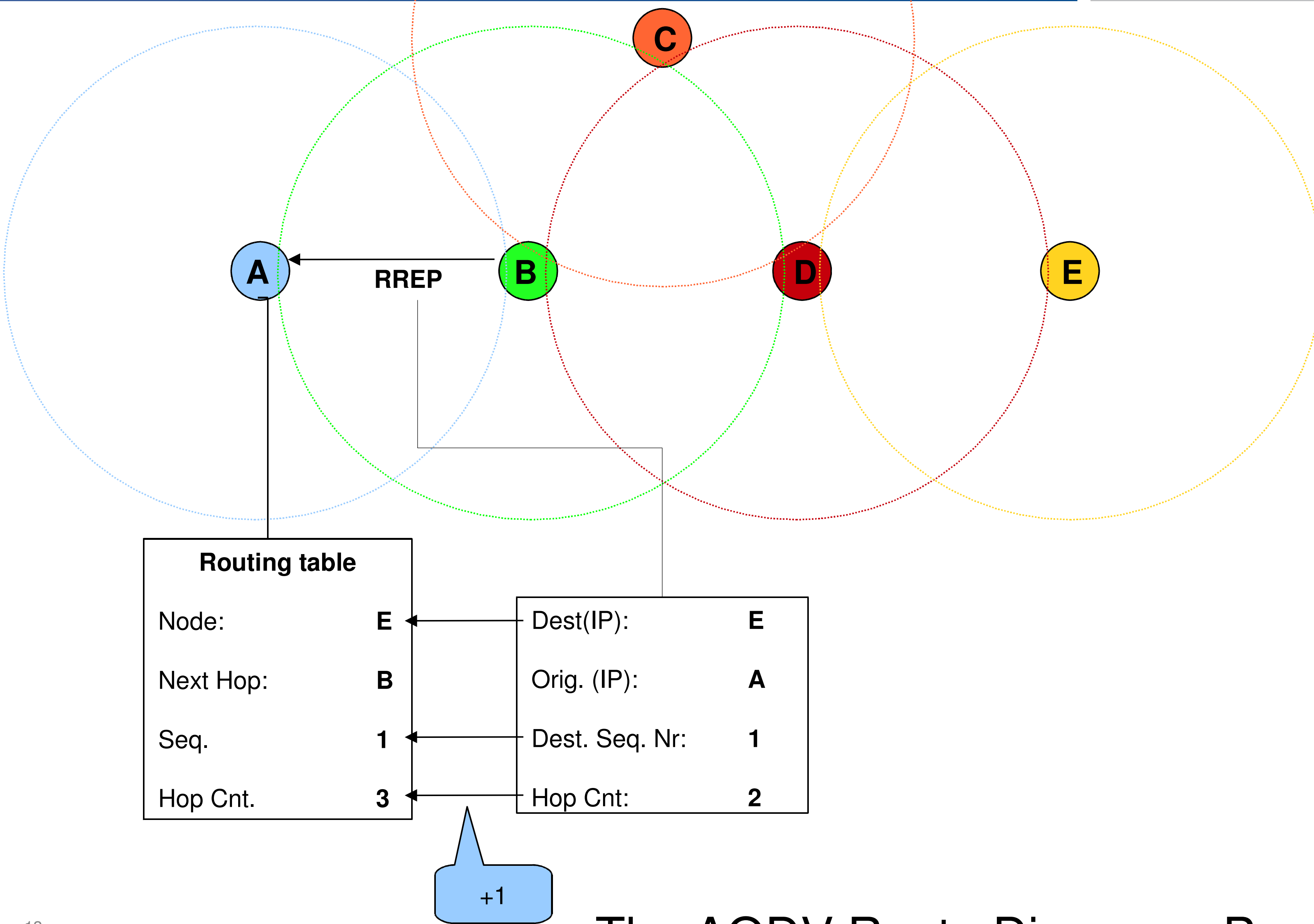
Routing table

Node:	A	E
Next Hop:	A	D
Seq.	0	1
Hop Cnt.	1	2

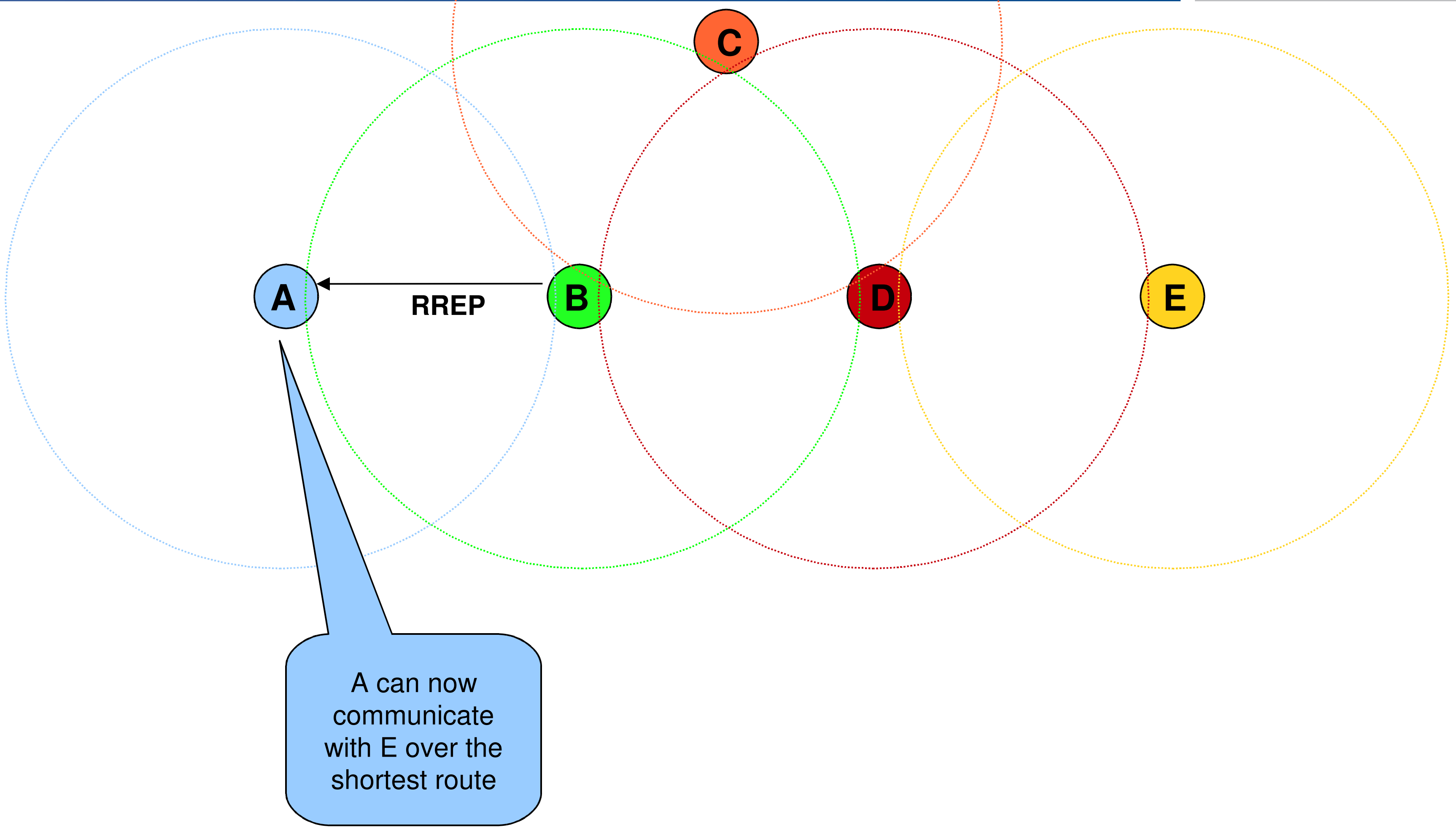
Dest(IP):	E
Orig. (IP):	A
Dest. Seq. Nr:	1
Hop Cnt:	1

+1

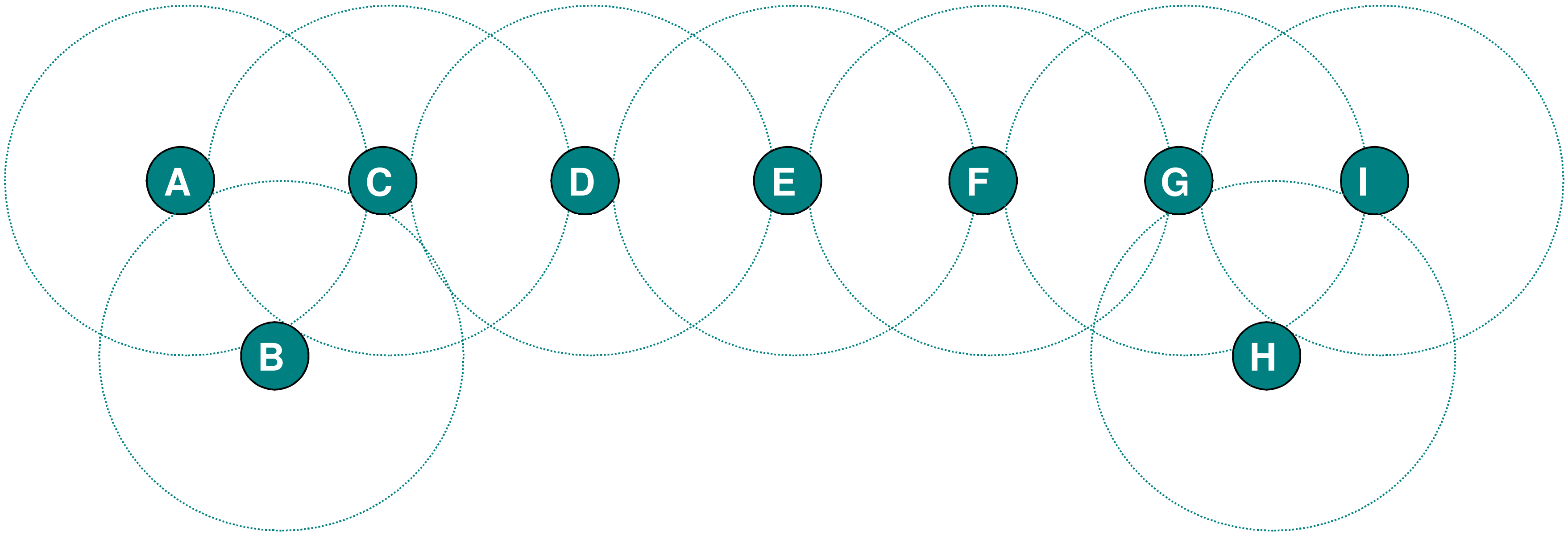
The AODV Route Discovery Process



The AODV Route Discovery Process

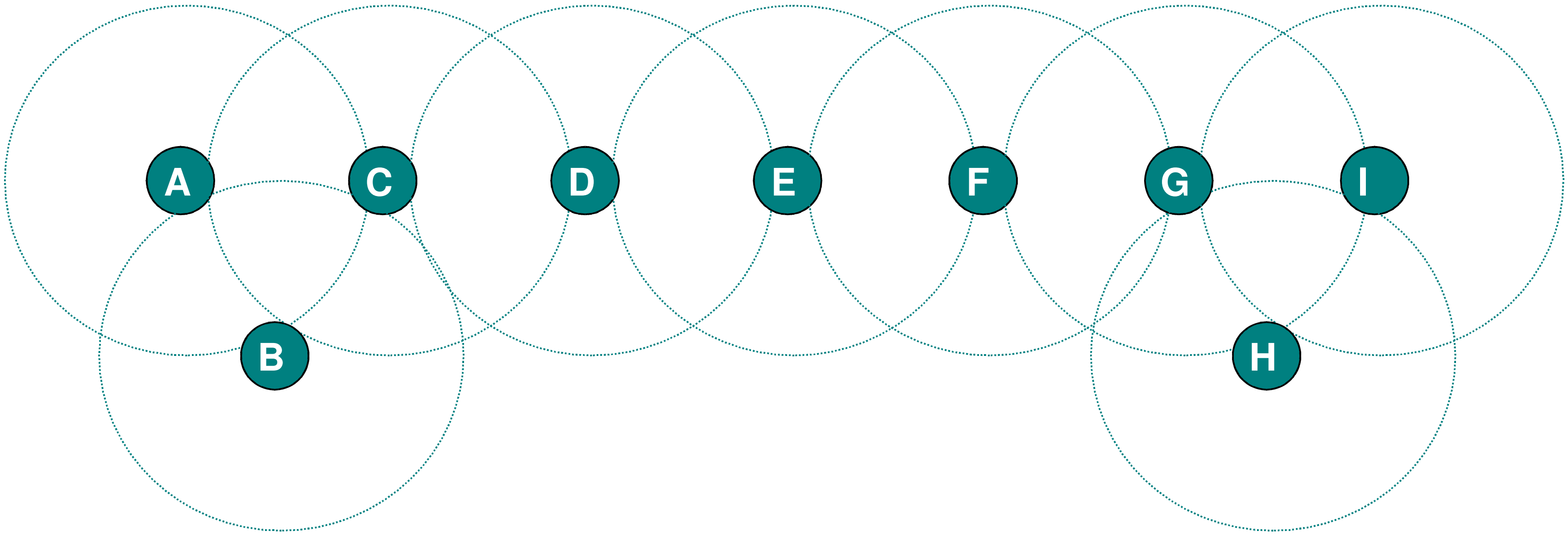


The AODV Route Discovery Process



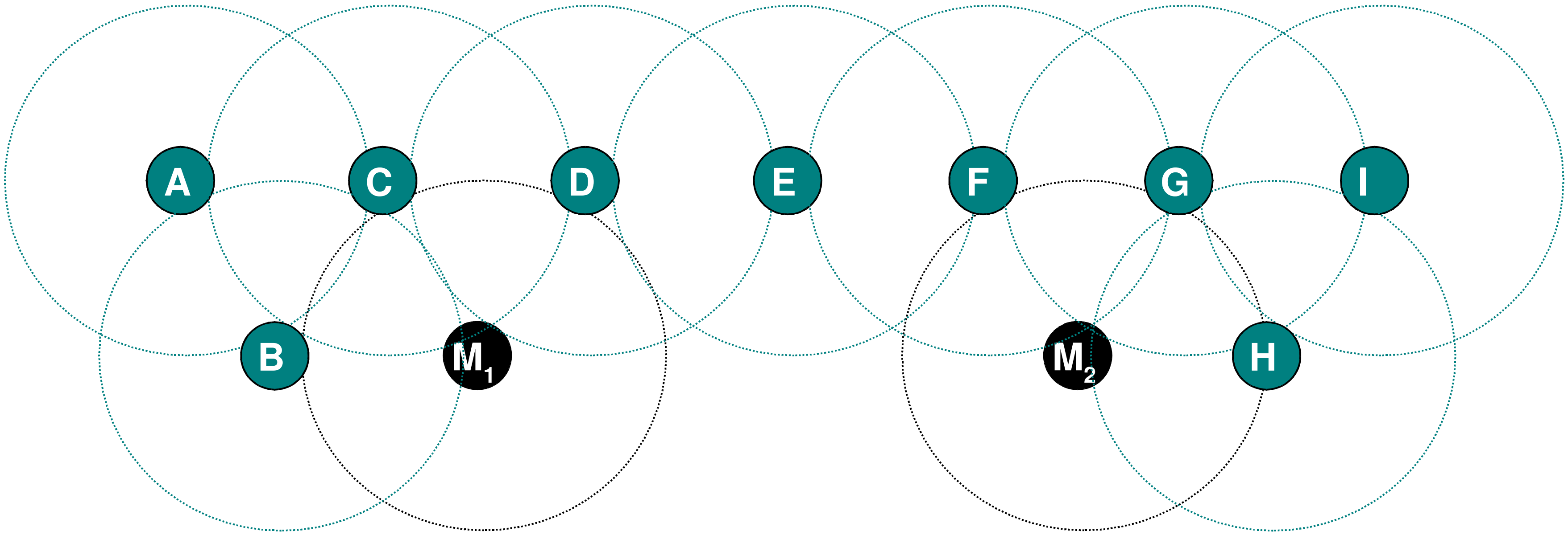
A wants to communicate with I but doesn't know the route:
-> Starts the AODV route discovery

In-band hidden-mode wormhole



After the AODV route discovery process, the shortest route would be:
A - C - D - E - F - G - I

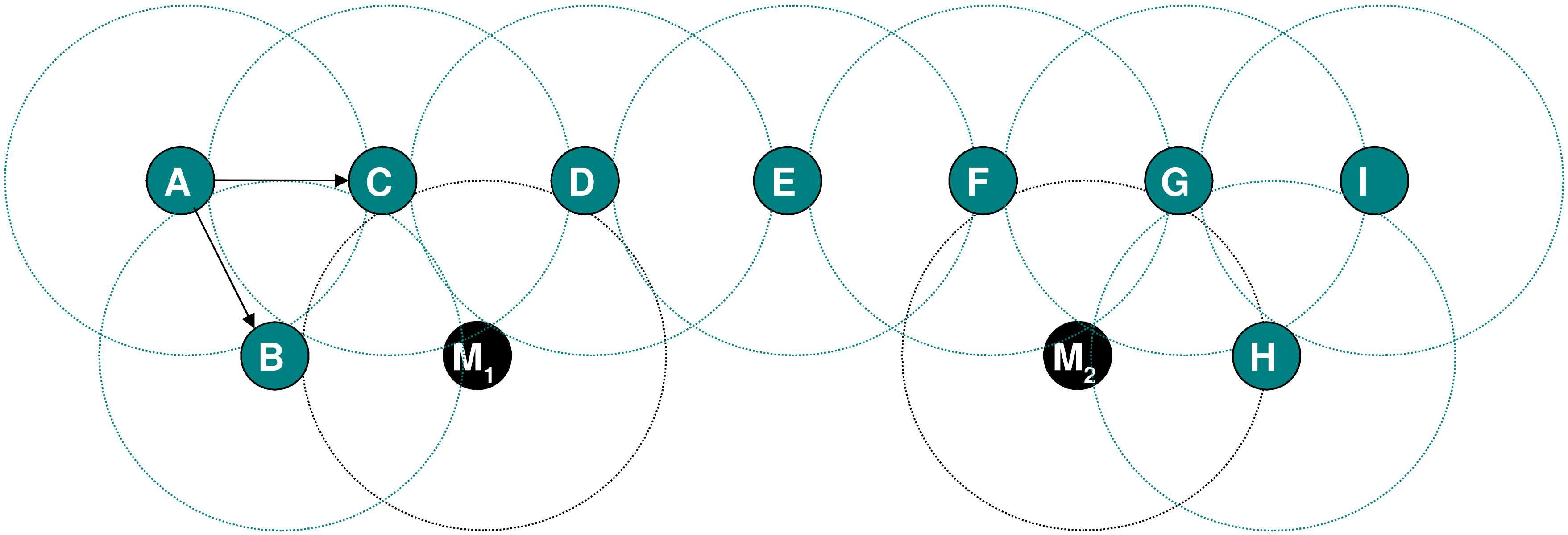
In-band hidden-mode wormhole



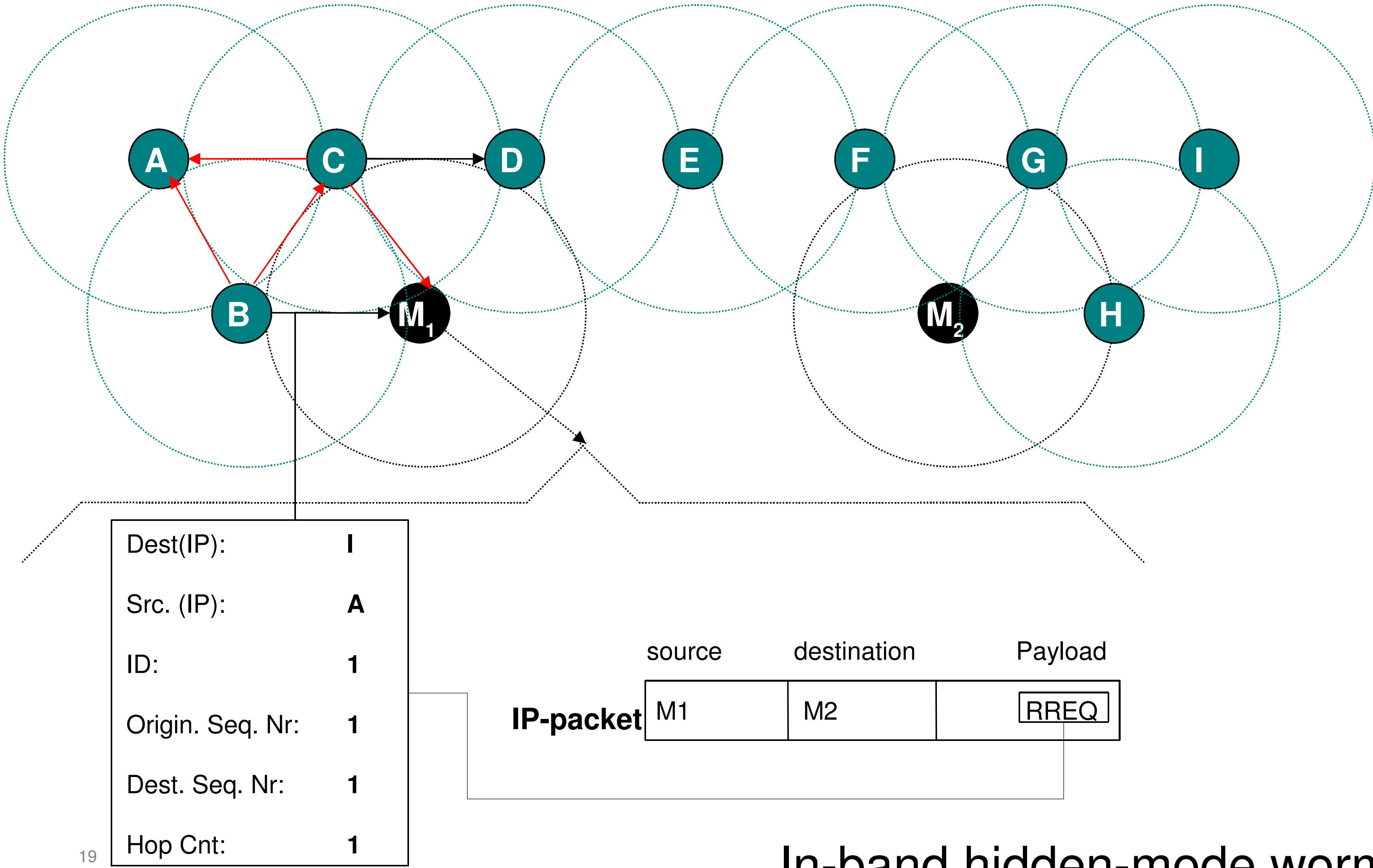
Two malicious nodes M1 and M2 joins the network with the intention to form an in-band hidden-mode wormhole between B and H

Let's see what happens when A want to find the shortest route to I again.

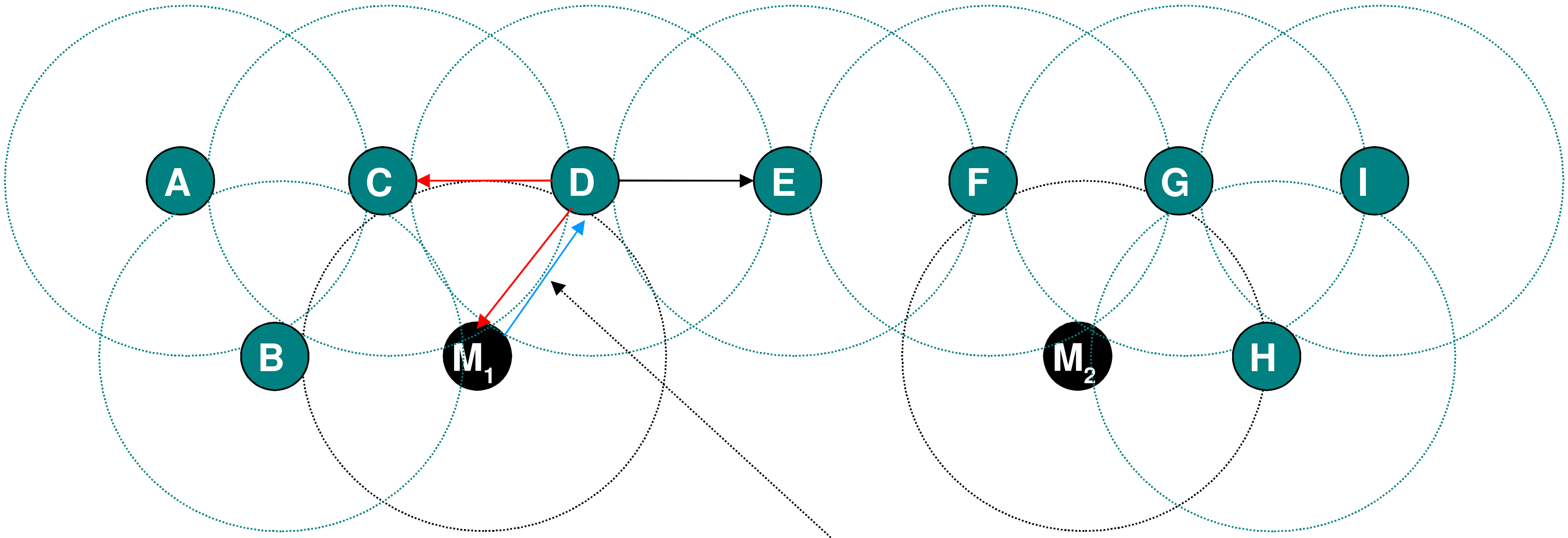
In-band hidden-mode wormhole



In-band hidden-mode wormhole

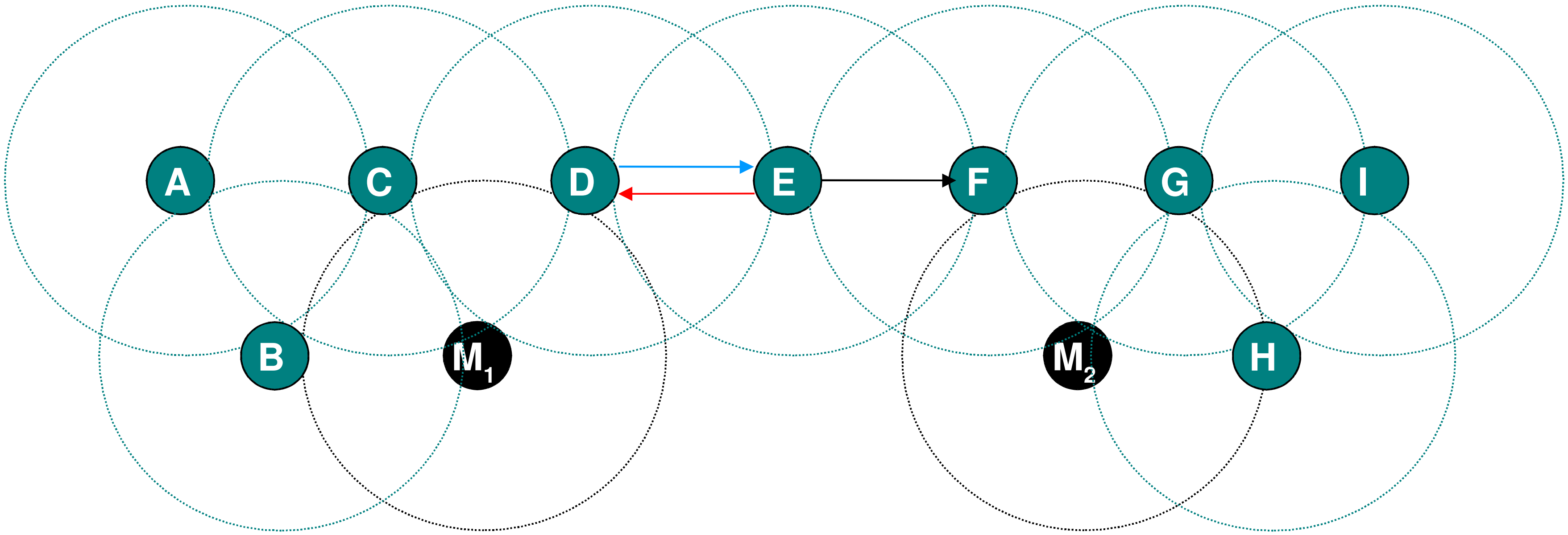


In-band hidden-mode wormhole

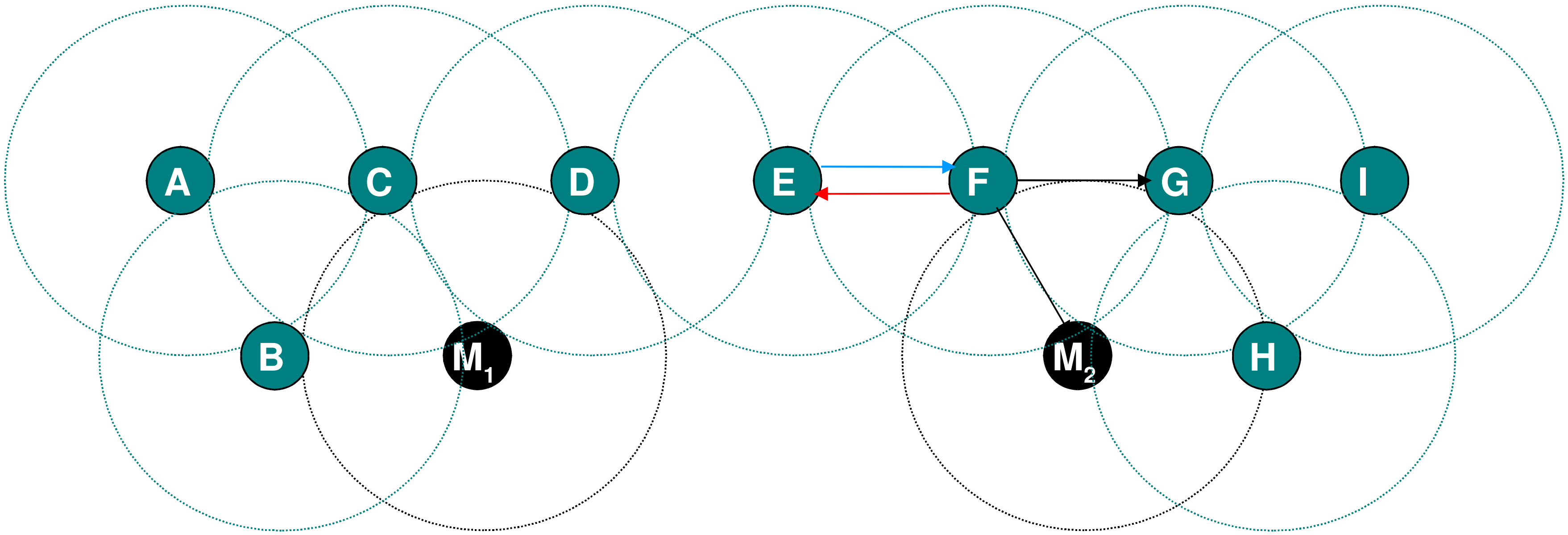


	source	destination	Payload
IP-packet	M1	M2	RREQ

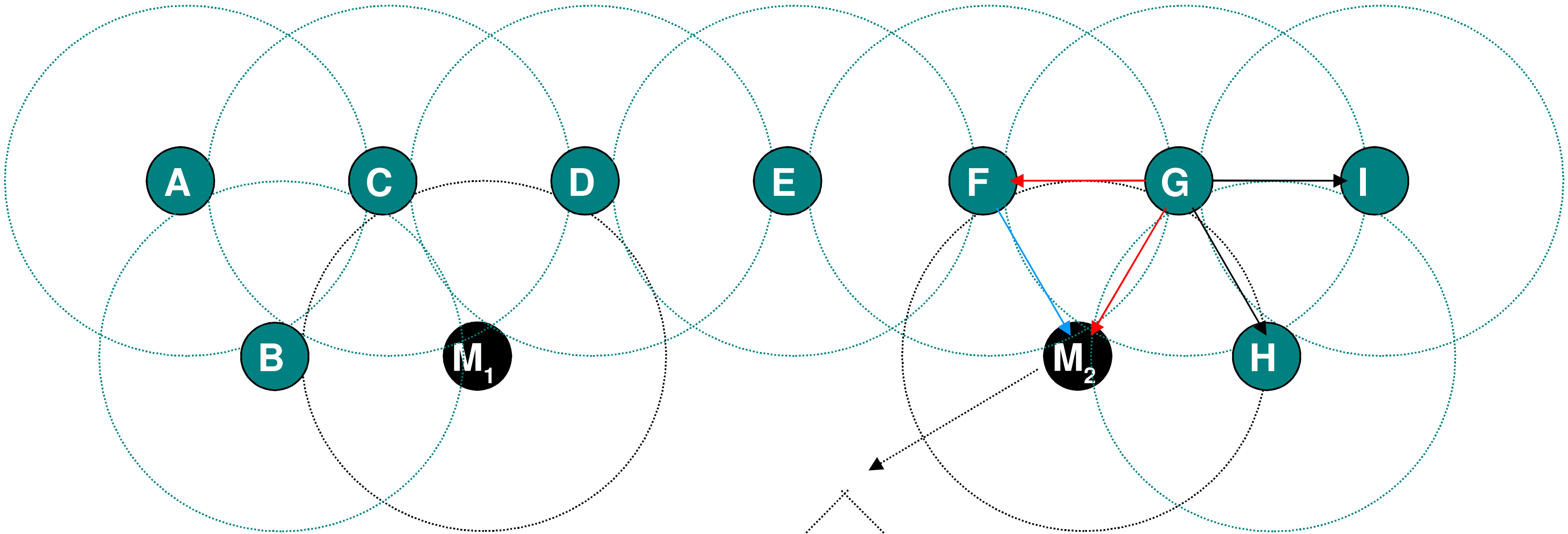
In-band hidden-mode wormhole



In-band hidden-mode wormhole

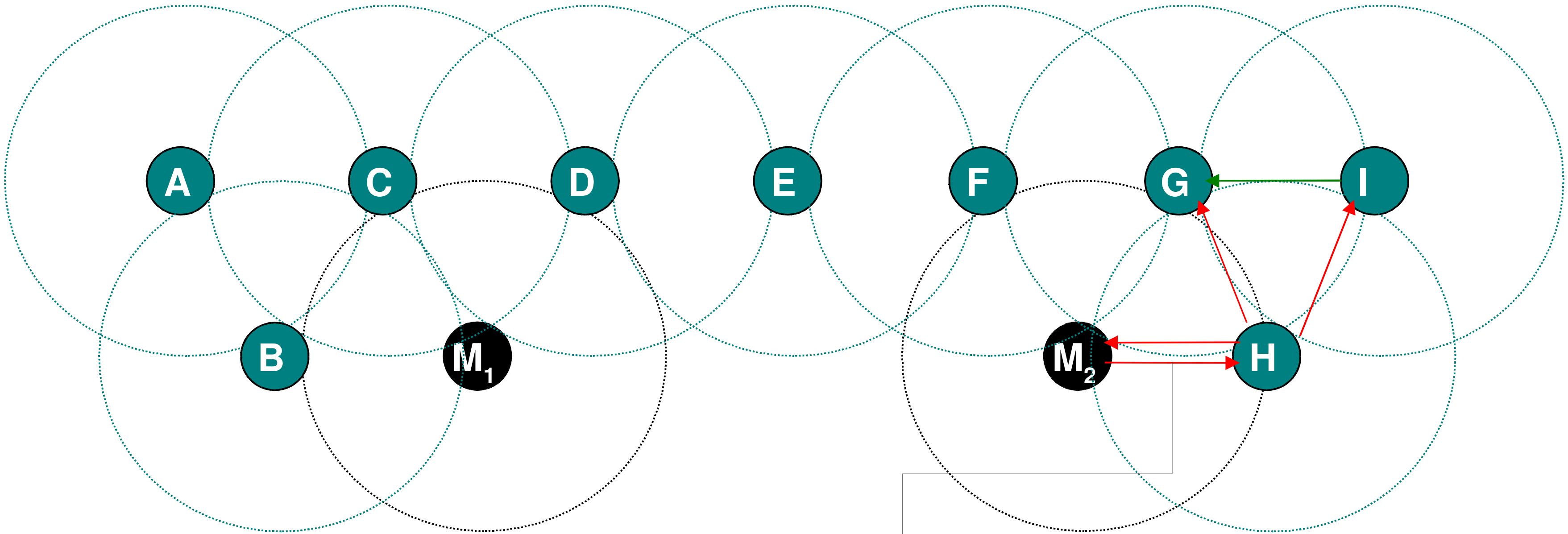


In-band hidden-mode wormhole



	source	destination	Payload
IP-packet	M1	M2	RREQ

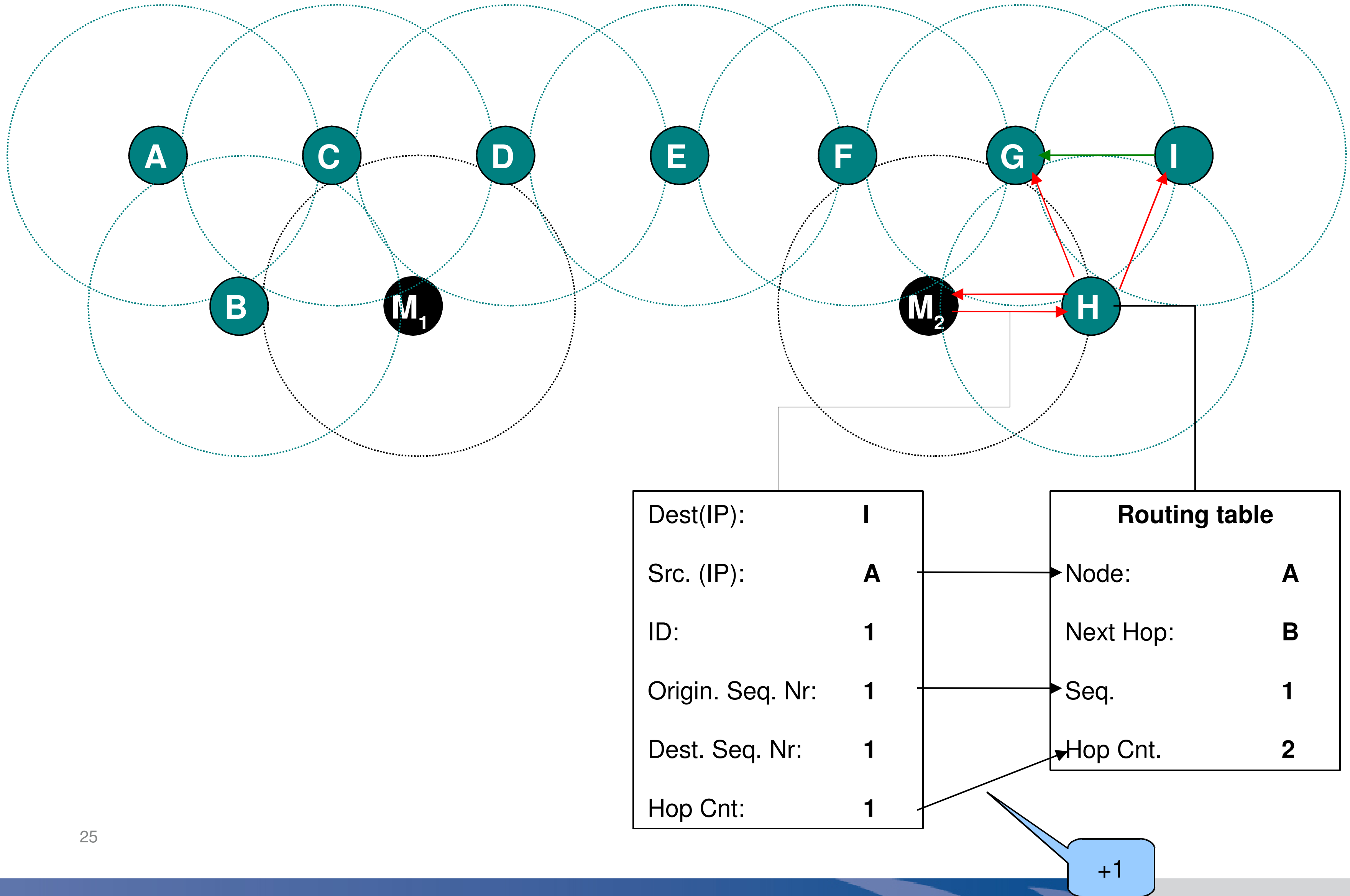
Dest(IP):	**I**
Src. (IP):	**A**
ID:	**1**
Origin. Seq. Nr:	**1**
Dest. Seq. Nr:	**1**
Hop Cnt:	**1**

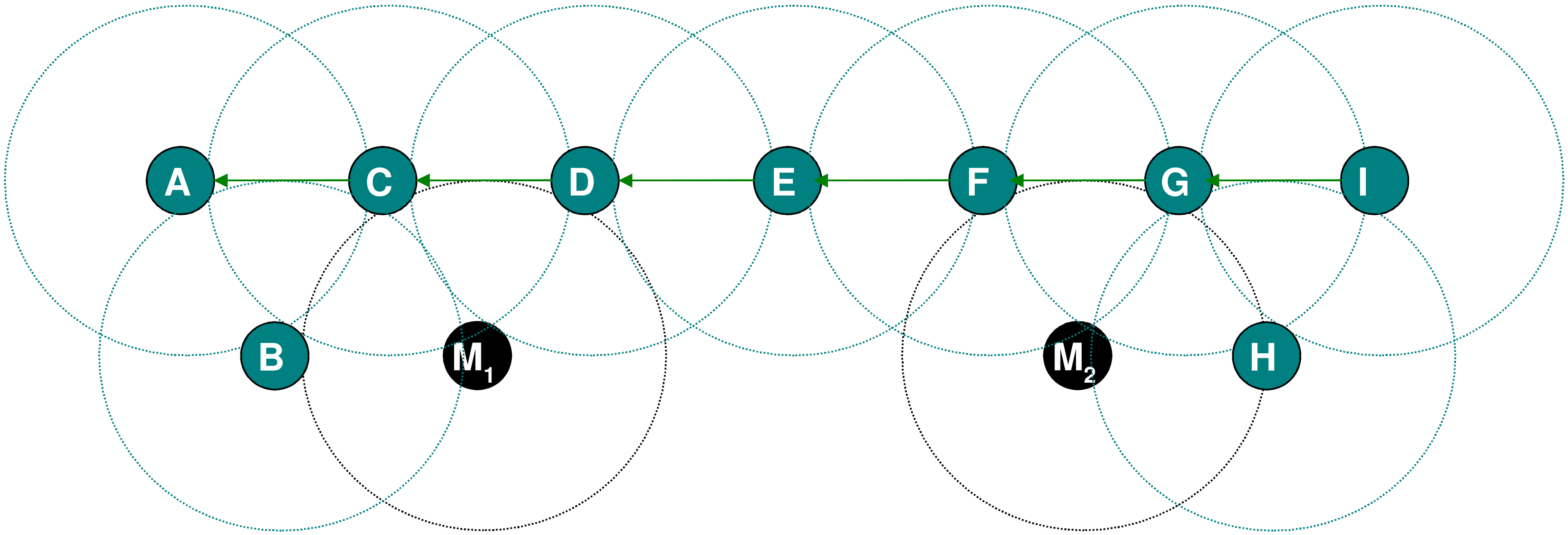


Dest(IP):	**I**
Src. (IP):	**A**
ID:	**1**
Origin. Seq. Nr:	**1**
Dest. Seq. Nr:	**1**
Hop Cnt:	**1**

H will not forward this RREQ since it has already processed a RREQ with ID=1 and Src=A

According to the AODV standard specification it would update its routing table since this “fake” route has smaller amount of hops to A than the previous route


A
B
C
D
E
F
G
H
I
M1
M2
Dest(IP): I
Src. (IP): A
ID: 1
Origin. Seq. Nr: 1
Dest. Seq. Nr: 1
Hop Cnt: 1
Routing table
Node: A
Next Hop: B
Seq. 1
Hop Cnt. 2
+1

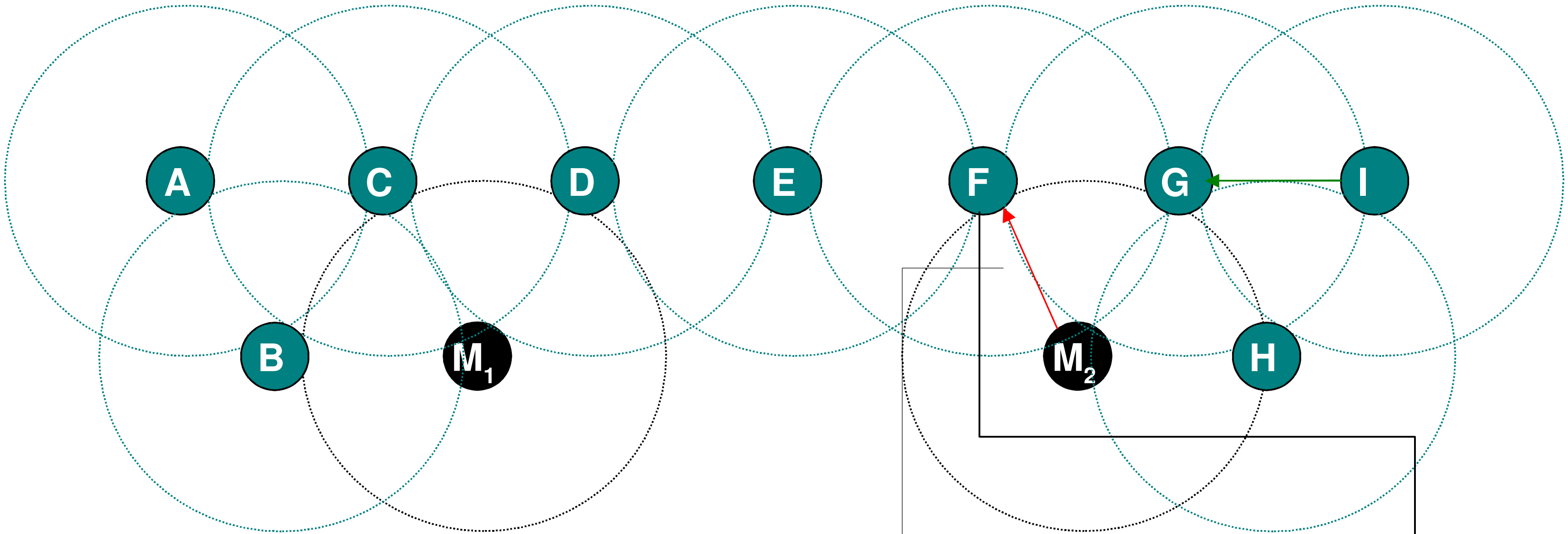


- The launch of an in-band hidden-mode wormhole wouldn't succeed in this case???

- It would at least not affect the route between A and I

- The end of the wormhole cannot be too close to the destination node (I)

In-band hidden-mode wormhole



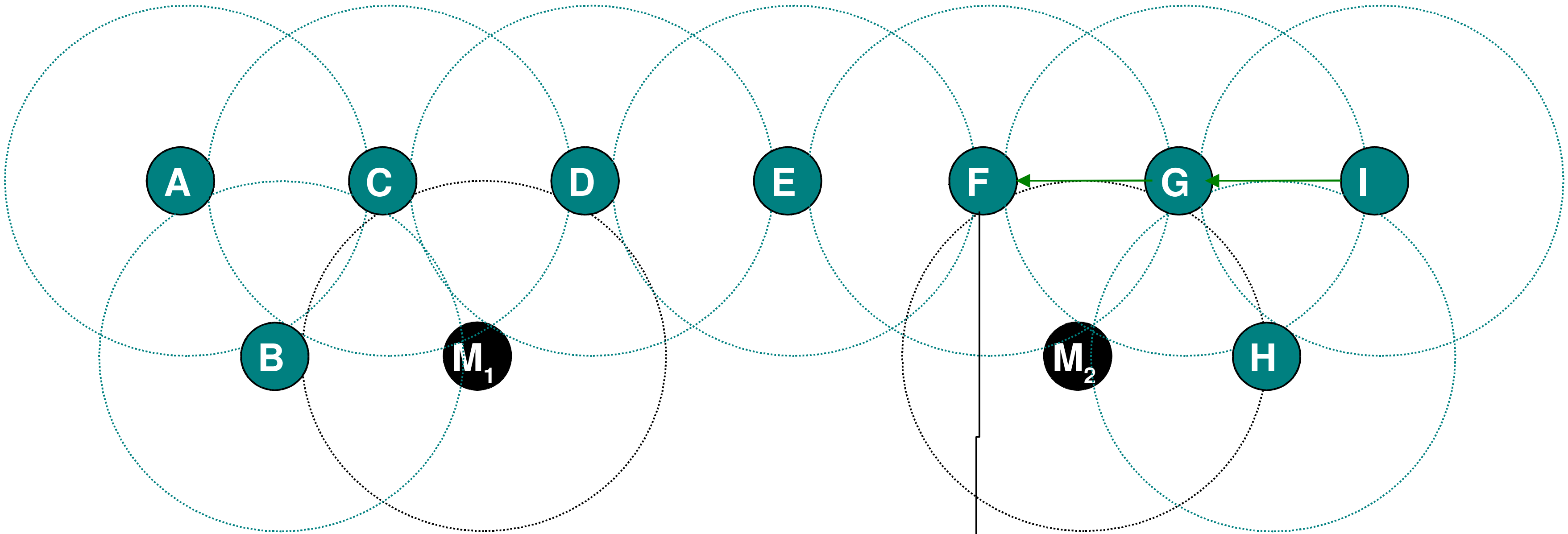
What if M2 redirects the tunneled RREQ to F?

- The Hop Cnt in the tunneled RREQ is smaller than the one associated with the previous route, so the routing table on F will be updated so that a route to A goes through the wormhole!

Dest(IP):	**I**
Src. (IP):	**A**
ID:	**1**
Origin. Seq. Nr:	**1**
Dest. Seq. Nr:	**1**
Hop Cnt:	**1**

+1

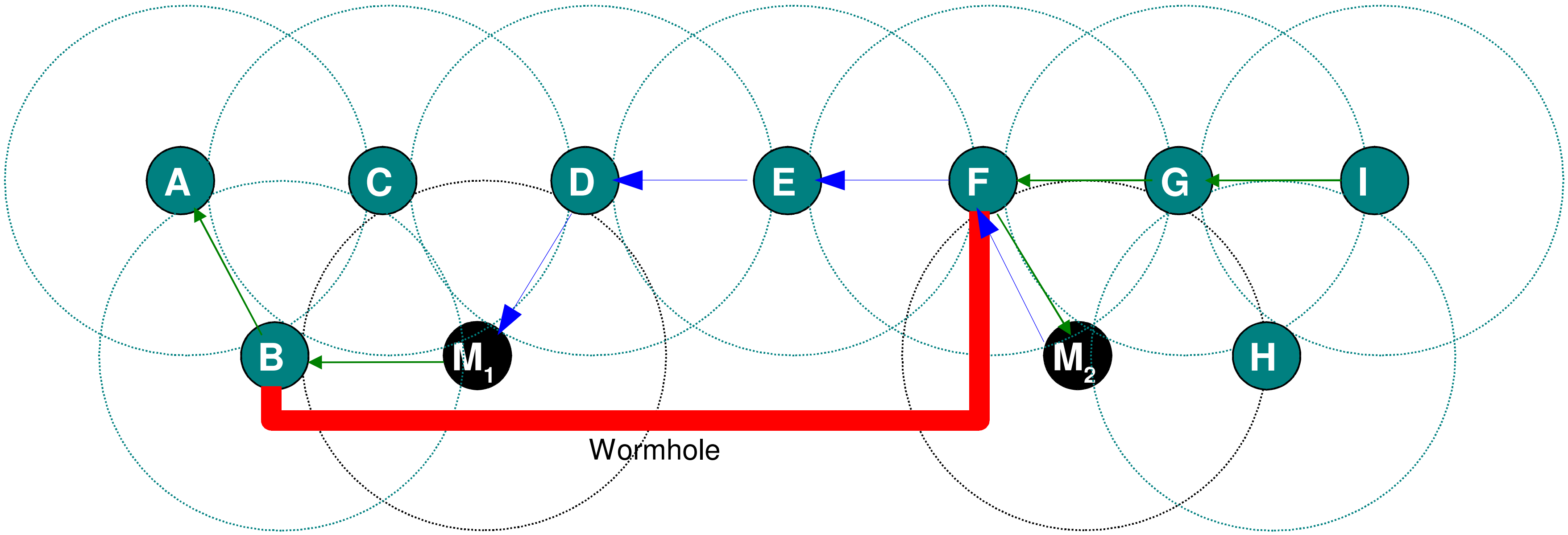
Routing table	
Node:	**A**
Next Hop:	**~~E~~ B**
Seq.	**1**
Hop Cnt.	**4 2**



The update is performed before the RREP arrives to F ---> The RREP will go through the wormhole

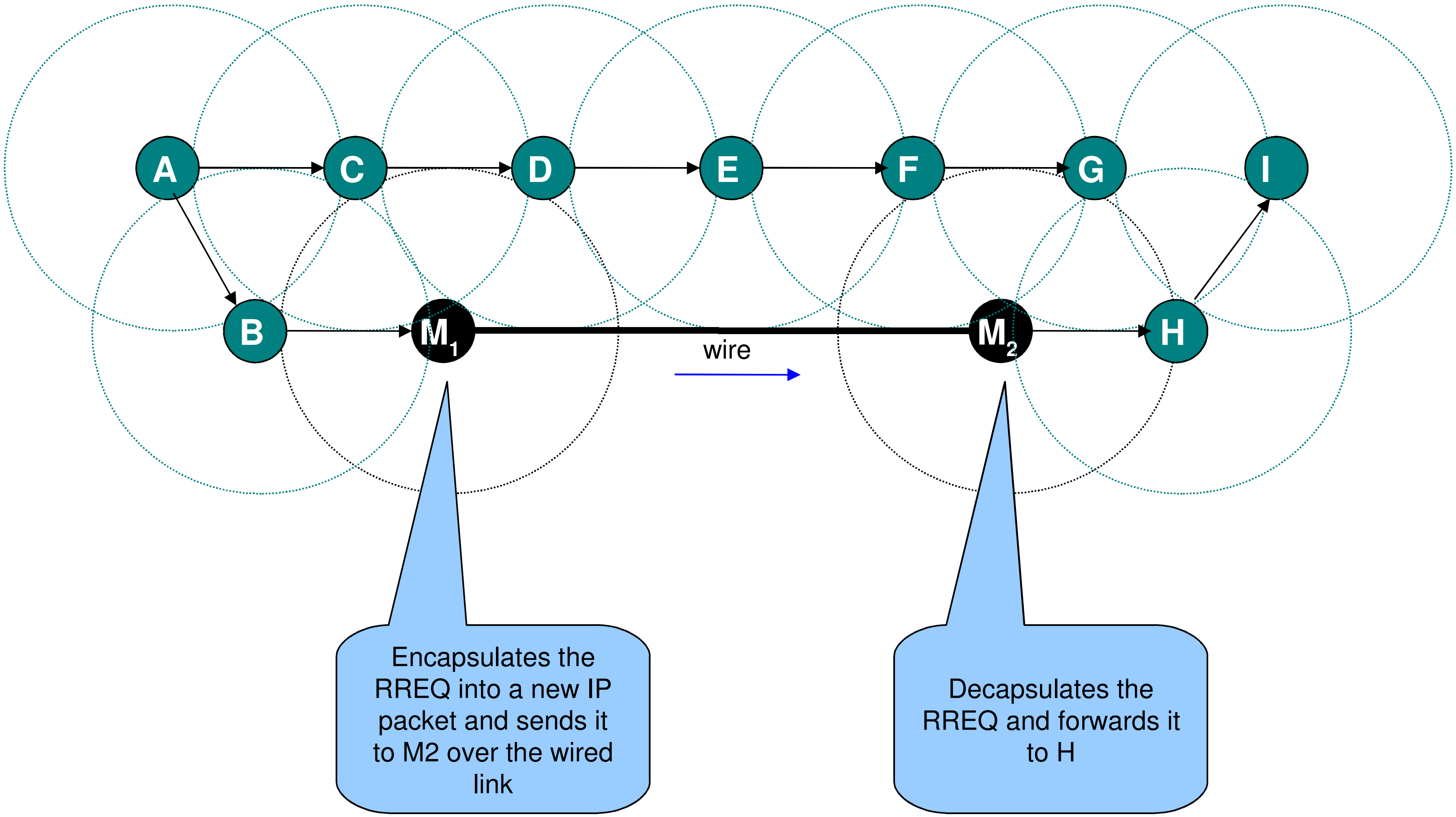
Routing table

Node:	**A**
Next Hop:	**B**
Seq.	**1**
Hop Cnt.	**2**

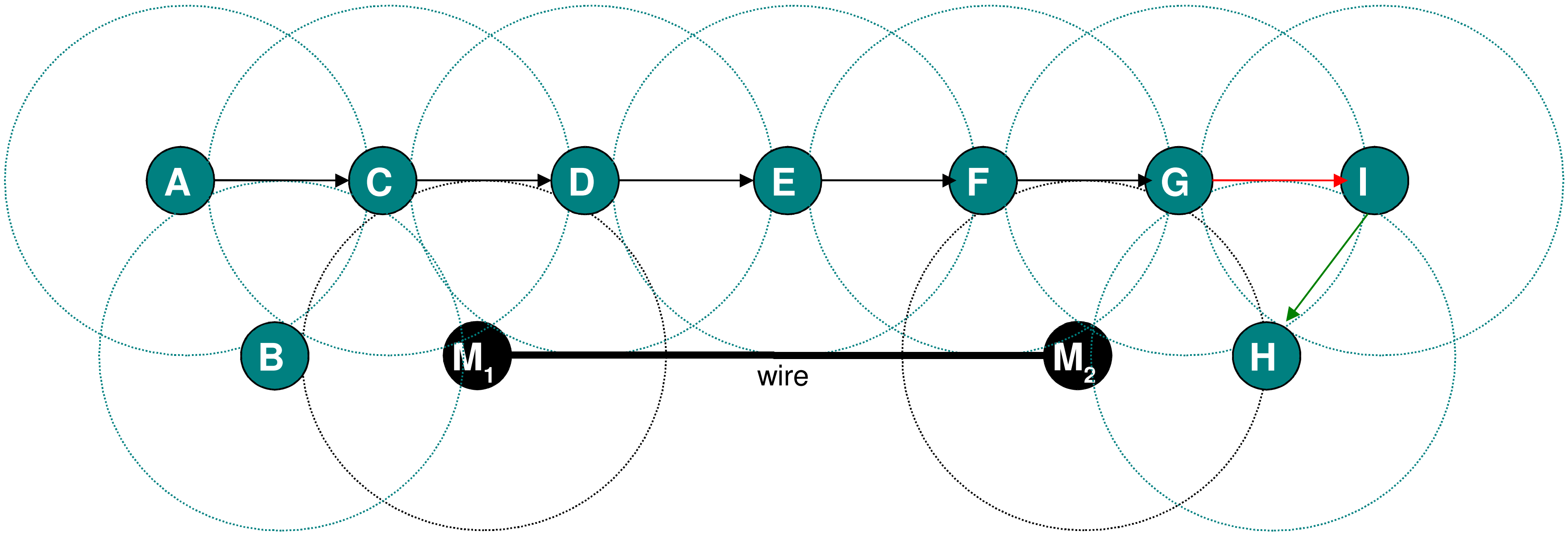


This wormhole formation would must probably succeed and the shortest route from A to I would be:

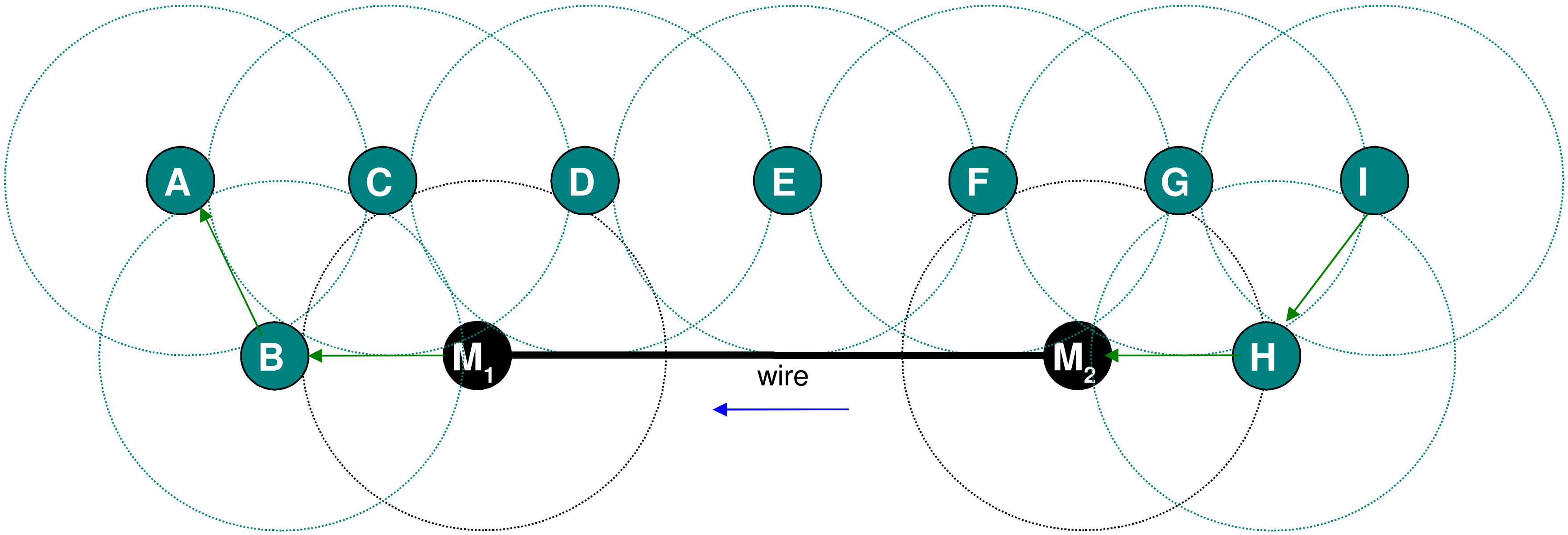
A - B - F - G - I



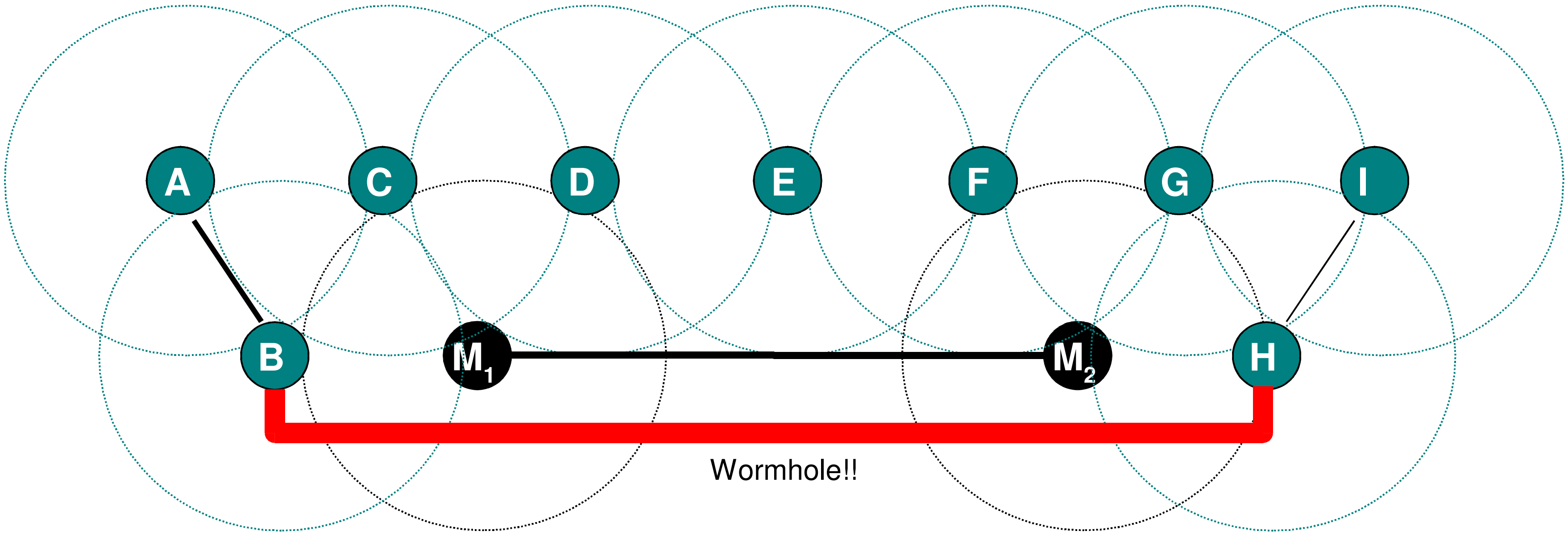
Out-of-band hidden-mode wormhole



Out-of-band hidden-mode wormhole



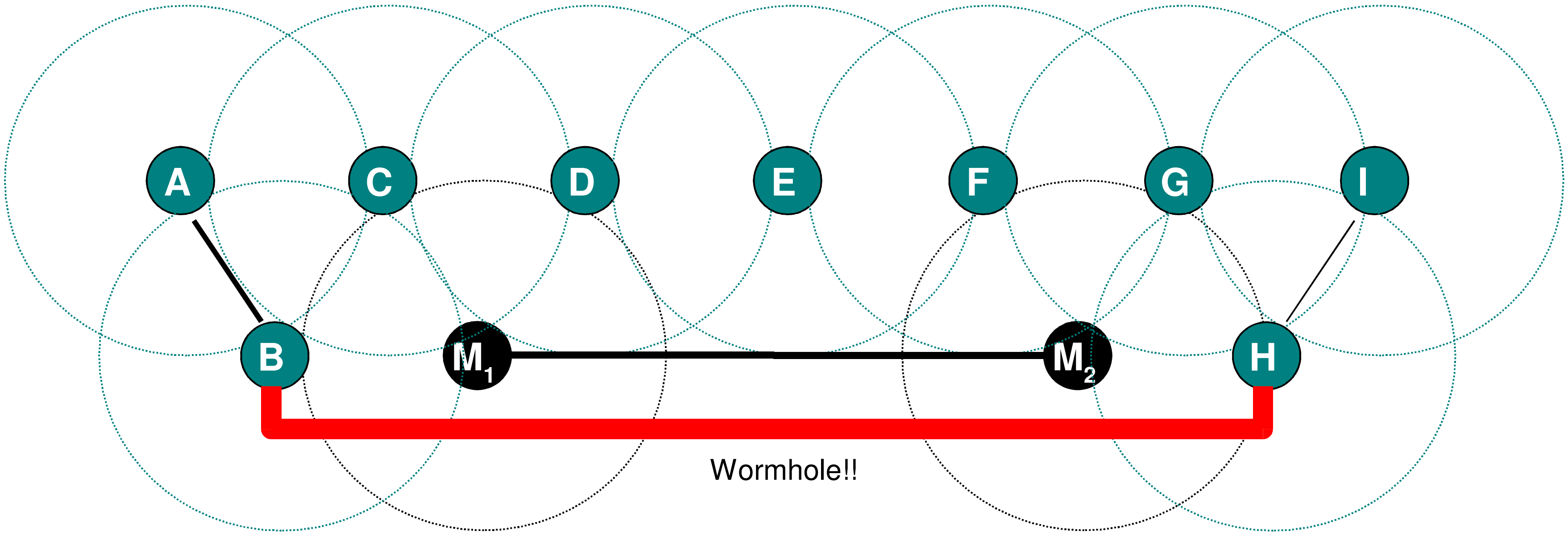
Out-of-band hidden-mode wormhole



The wormhole creation attempt between B and H would in this case most probably succeed

The shortest route is now: A - B - H - I

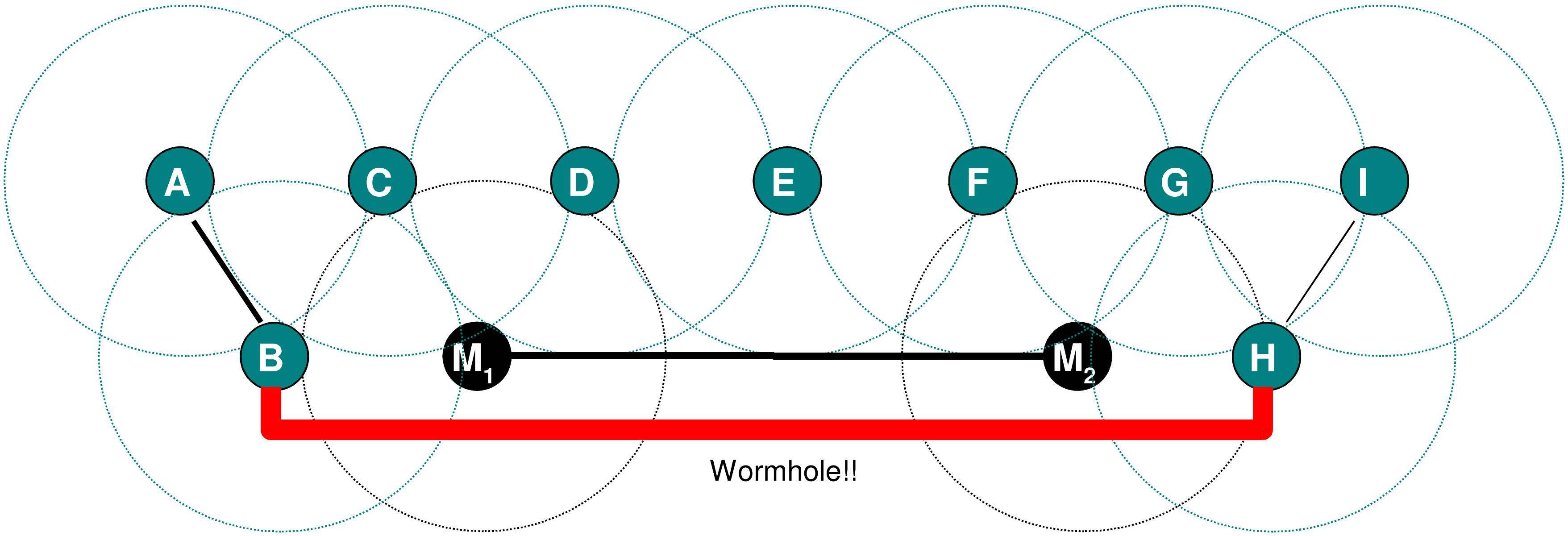
Out-of-band hidden-mode wormhole



How could this wormhole be prevented using the wormhole countermeasure proposed in the “IEEE paper”?

“IEEE paper “ = *Khabbazian, M., Mercier, H., and Bhargava, V. K. (2009). Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. In IEEE Transactions on Wireless Communications. Vol 8, No. 2. February 2009*

Wormhole countermeasure proposal: “IEEE paper”



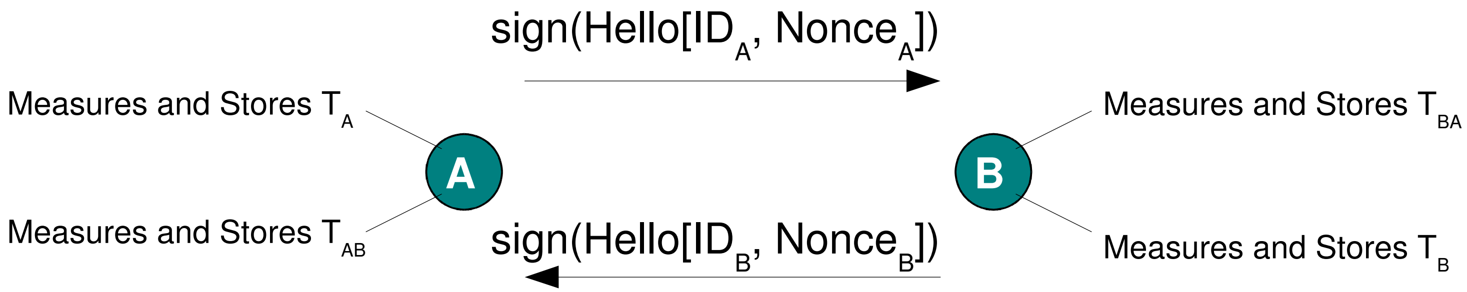
The idea of the proposal is that every node in the network keep track of their closest neighbors and their 2-hop neighbors

This is done by every node by an exchange of only two messages

The solution is time-based but no time synchronization or special hardware is needed

Let's have a closer look at the proposal!

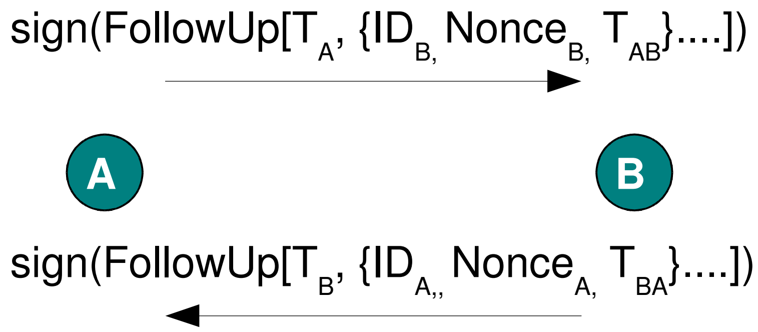
Wormhole countermeasure proposal: “IEEE paper”



Node A can verify if B is its neighbor by sending a Hello message (broadcasted to all neighbors) to which B will respond by an own Hello message

T_A	=	The time when A's hello message was sent, measured by A
T_B	=	The time when B's hello message was sent, measured by B
T_{BA}	=	The time when A's hello was received by B, measured by B
T_{AB}	=	The time when B's hello was received by A, measured by A

Wormhole countermeasure proposal: “IEEE paper”



Both nodes send a Follow-Up message after receiving a Hello message

T_A	=	The time when A's hello message was sent, measured by A
T_B	=	The time when B's hello message was sent, measured by B
T_{BA}	=	The time when A's hello was received by B, measured by B
T_{AB}	=	The time when B's hello was received by A, measured by A

Wormhole countermeasure proposal: “IEEE paper”

sign(FollowUp[T_A, {$ID_{B,}$ $Nonce_{B,}$ T_{AB}}....])

A B

sign(FollowUp[T_B, {$ID_{A,,}$ $Nonce_{A,}$ T_{BA}}....])

If for example A receives B's Hello message after sending its own it can verify that B really is its neighbor if:

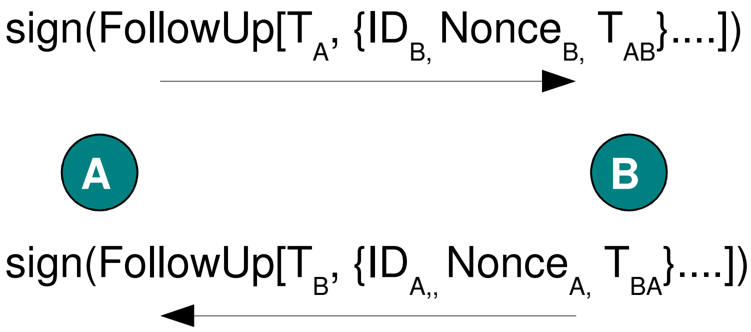
1. It can verify B's signature and ithe received $Nonce_A$ is the same as the one sent in the Hello

AND

2.
$$\frac{(T_{AB} - T_A) - (T_B - T_{BA})}{2} \times C <= T_{max}$$

C	=	The speed of light
T_{max}	=	The maximum transmission range
T_A	=	The time when A's hello message was sent, measured by A
T_B	=	The time when B's hello message was sent, measured by B
T_{BA}	=	The time when A's hello was received by B, measured by B
T_{AB}	=	The time when B's hello was received by A, measured by A

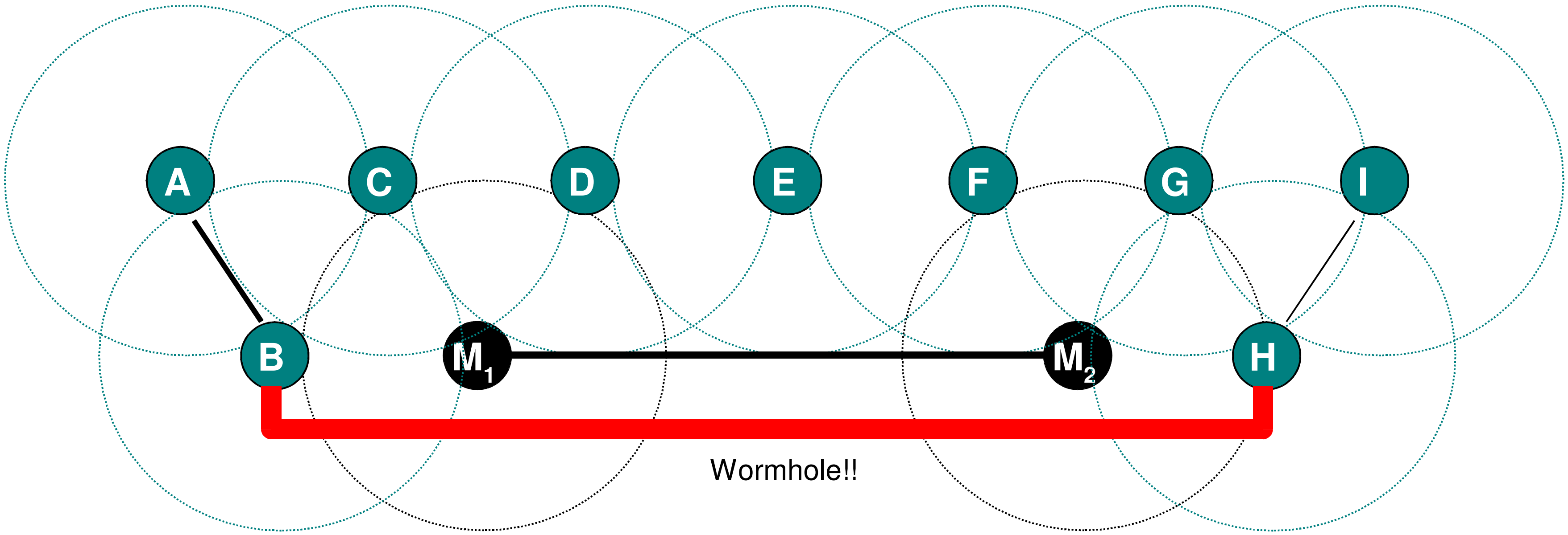
Wormhole countermeasure proposal: “IEEE paper”



B can also verify that A is its real neighbor, even if A initiated the exchange

Note that every node includes a list of all IDs (with their corresponding nonces and receival times) of all nodes it has received a hello message from in the follow-up message. Thus a node can also verify all its 2-hop neighbors

Wormhole countermeasure proposal: “IEEE paper”

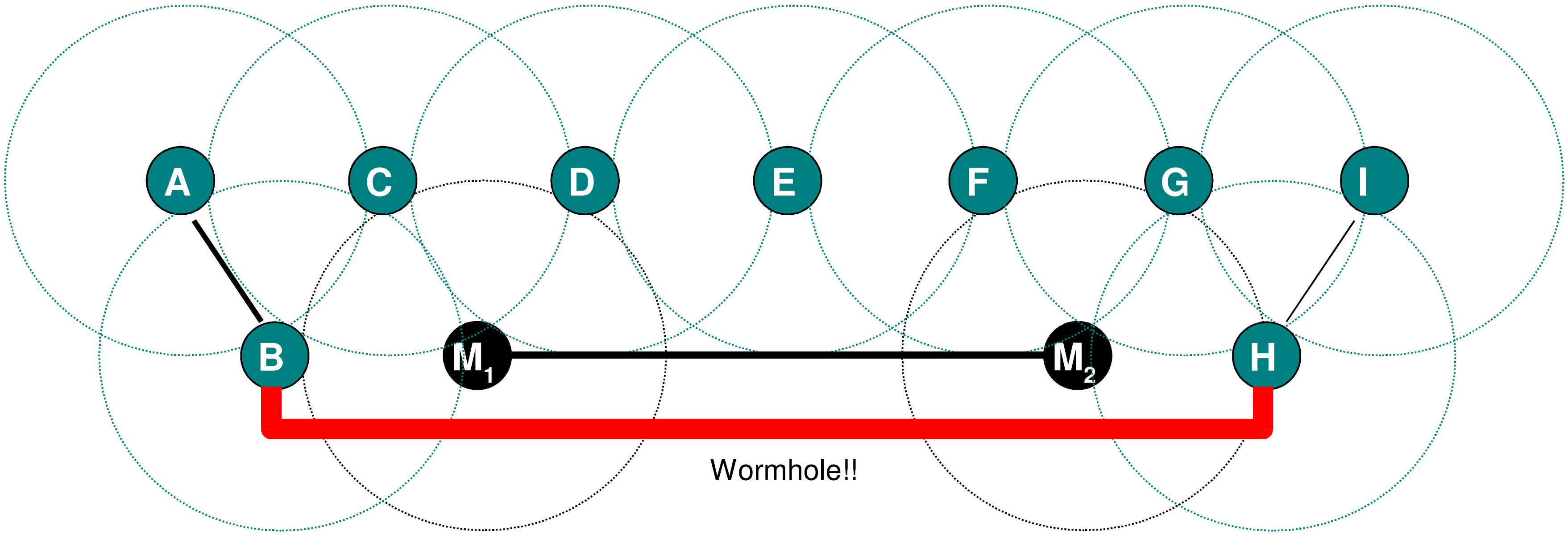


The paper doesn't say at what point of the routing process their neighbor verification process should be performed

My guess is that it is meant to be performed periodically so that every node constantly has a fresh list of its neighbors.

In this case when H receives a RREQ from B it can state that B is a false neighbor since it is not included in the "neighbor list" of H

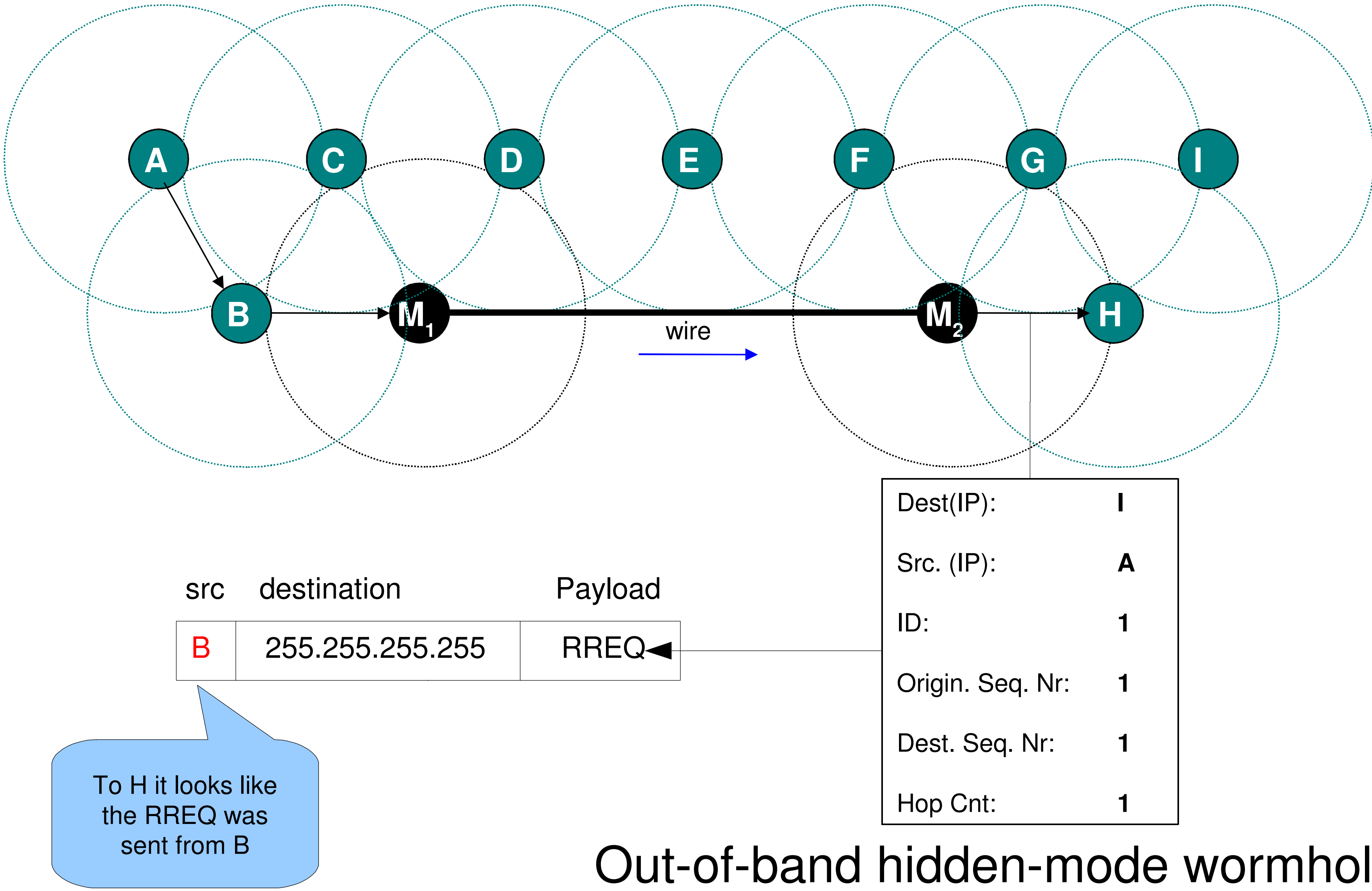
Wormhole countermeasure proposal: "IEEE paper"



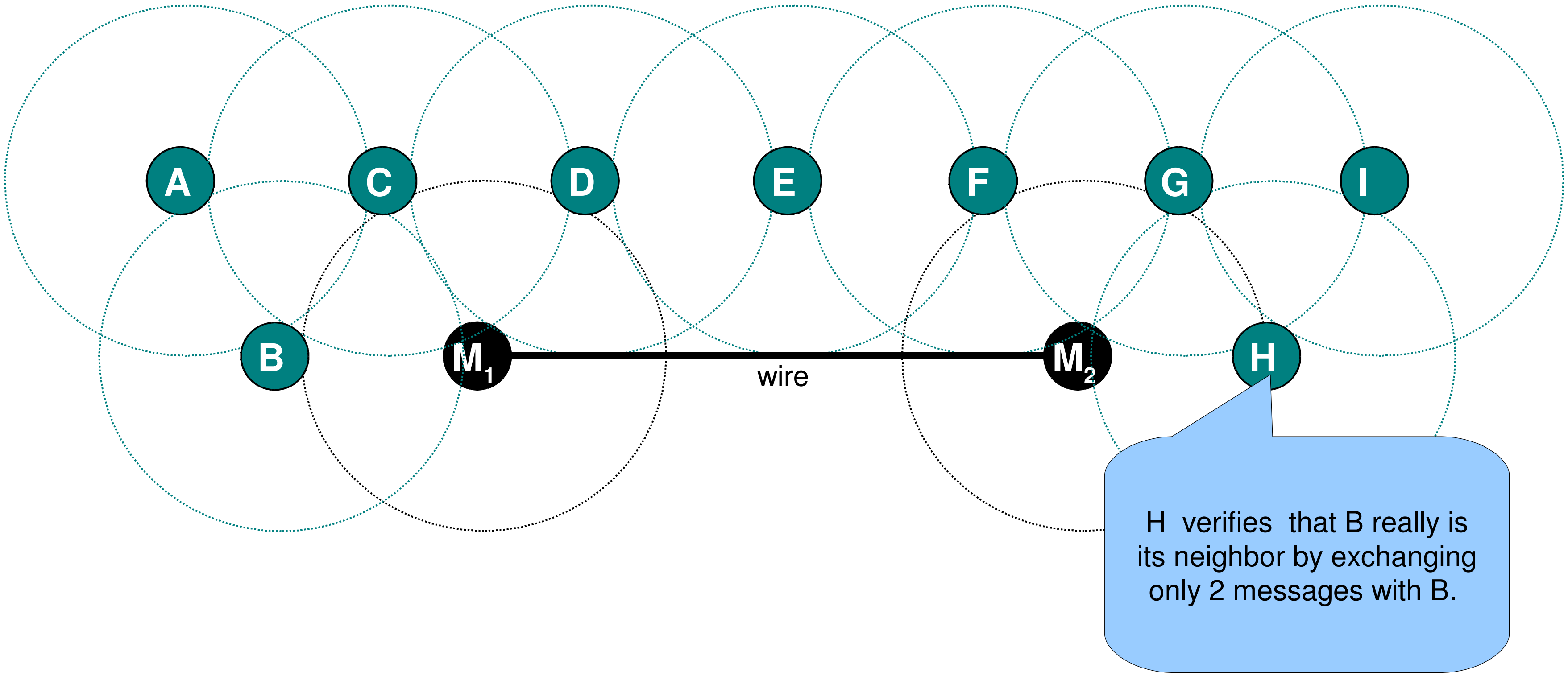
Another option could perhaps be to perform a modified version of the proposed neighbor verification process during route discovery.

When a node receives a RREQ it will verify if the sender of the RREQ is a real neighbor. If the RREQ is sent from a false neighbor the RREQ would be discarded

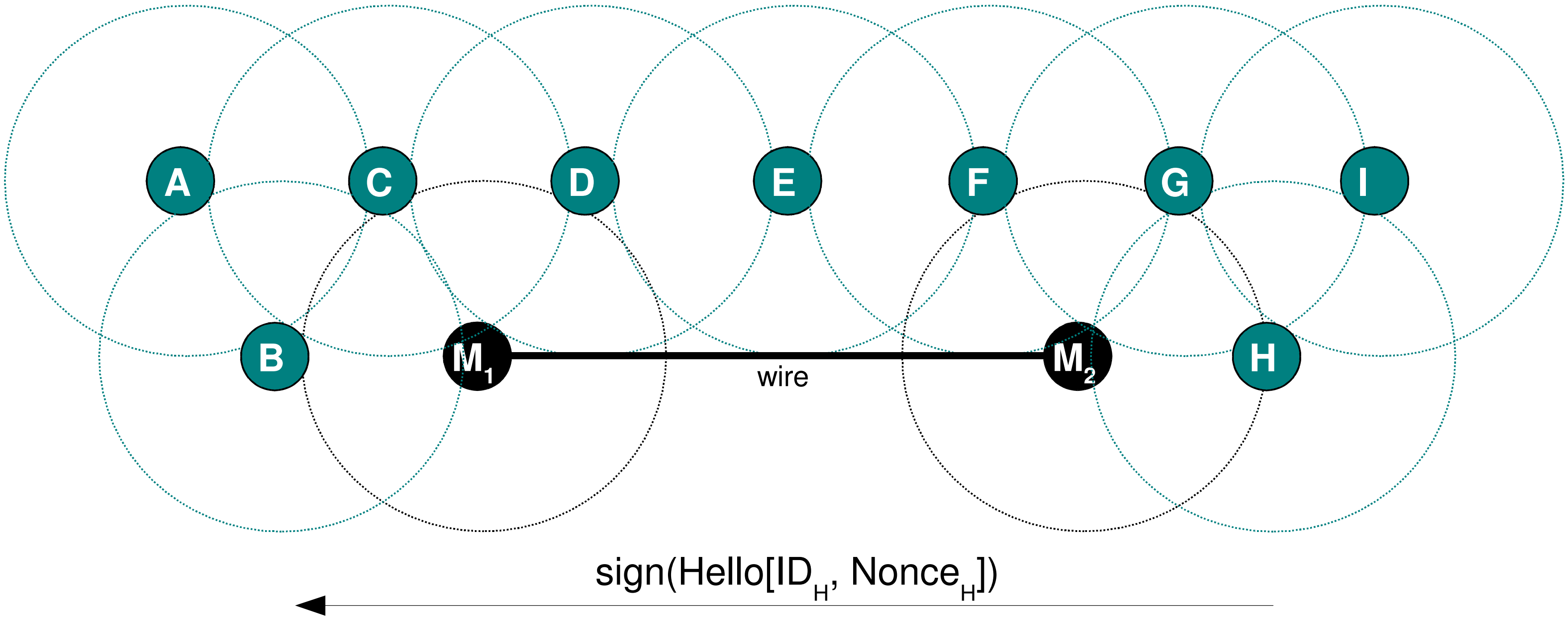
Wormhole countermeasure proposal: “IEEE paper”



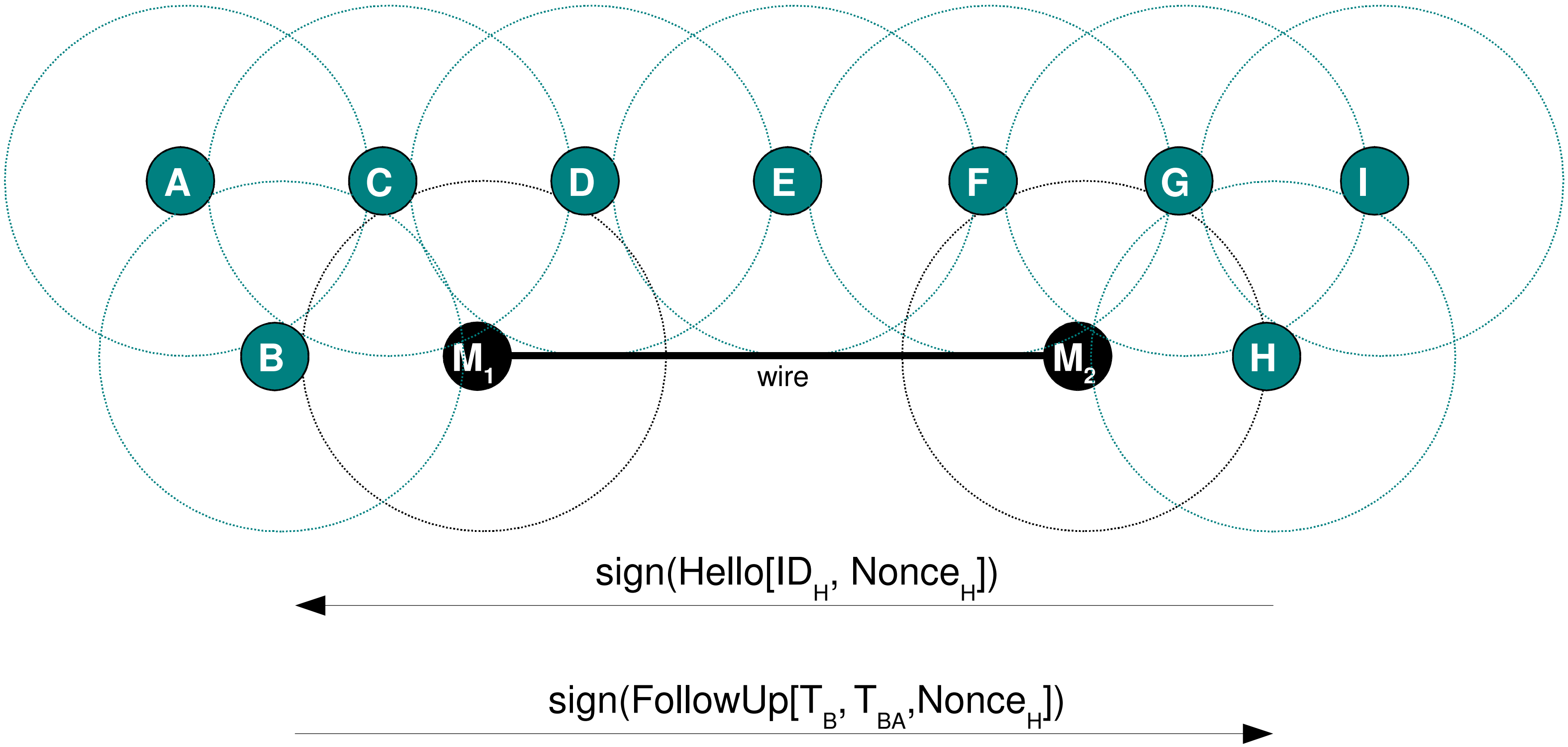
Out-of-band hidden-mode wormhole



Out-of-band hidden-mode wormhole



Out-of-band hidden-mode wormhole

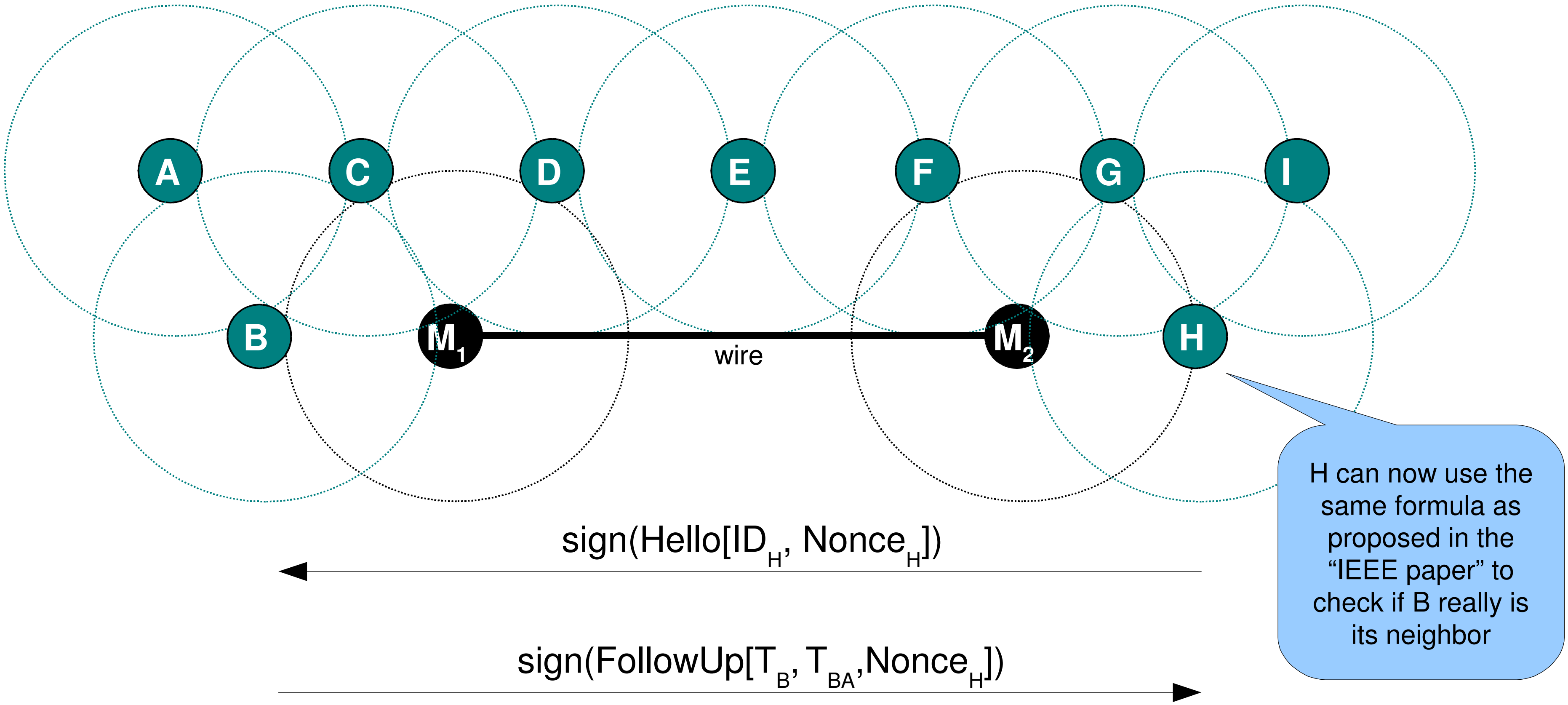


T_B = The time when B sends the Follow-UP, measured by B

T_{BA} = The time when B received the hello from H, measured by B

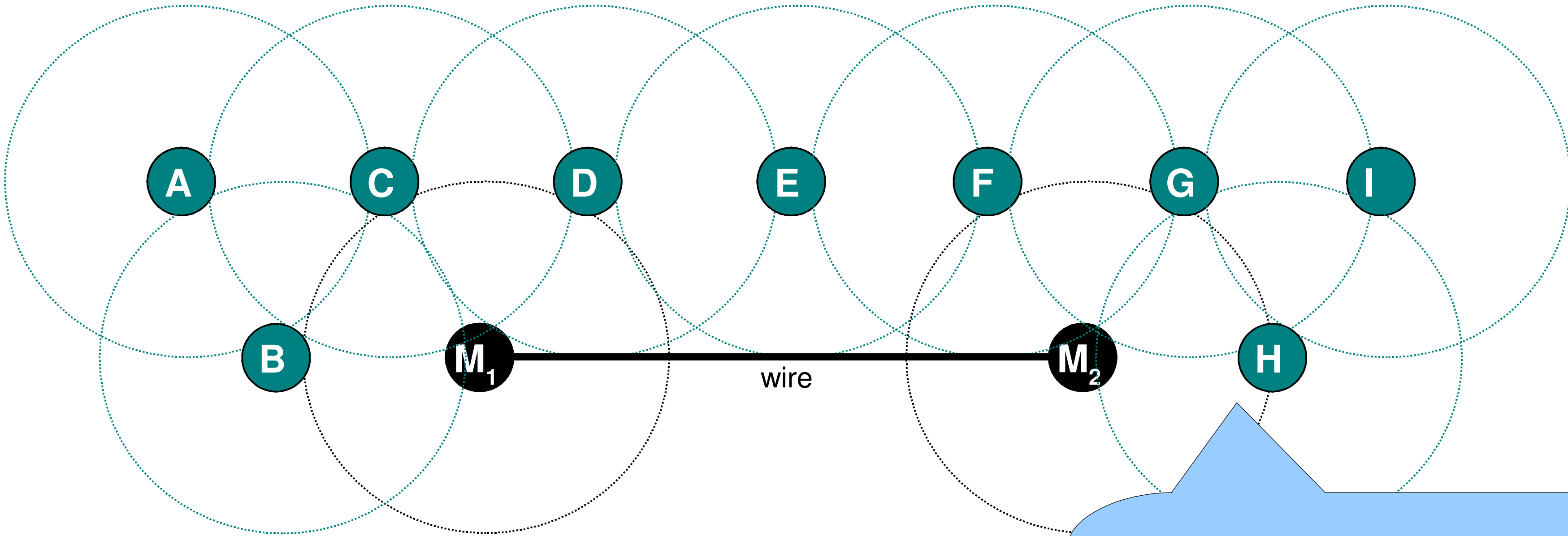
Out-of-band hidden-mode wormhole

Out-of-band hidden-mode wormhole



T_B = The time when B sends the Follow-UP, measured by B

T_{BA} = The time when B received the hello from H, measured by B



$$\frac{(T_{AB} - T_A) - (T_B - T_{BA})}{2} \times C <= T_{max}$$

T_B = The time when B sends the Follow-Up, measured by B

T_{BA} = The time when B received the hello from H, measured by B

T_A = The time when A sent the hello, measured by A

T_{AB} = The time when A received the Follow-Up from H, measured by B

T_{max} = The maximum transmission range

Out-of-band hidden-mode wormhole