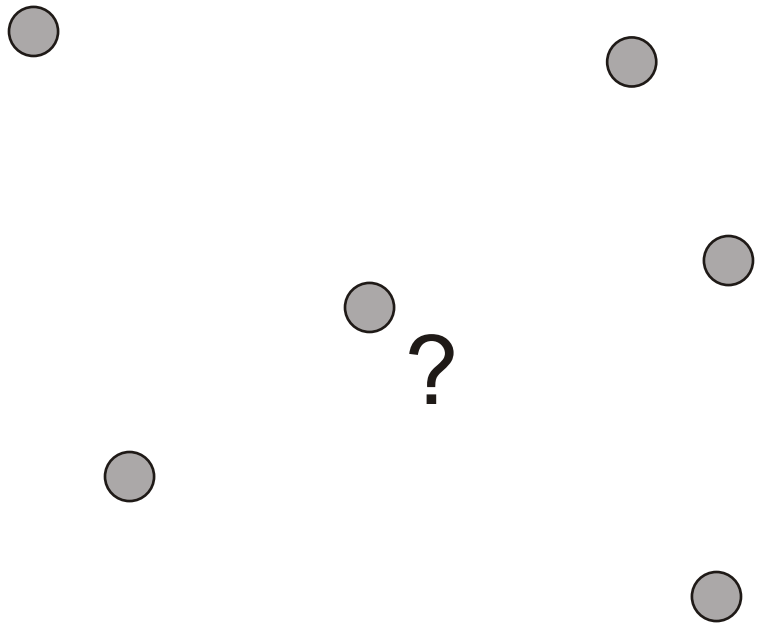
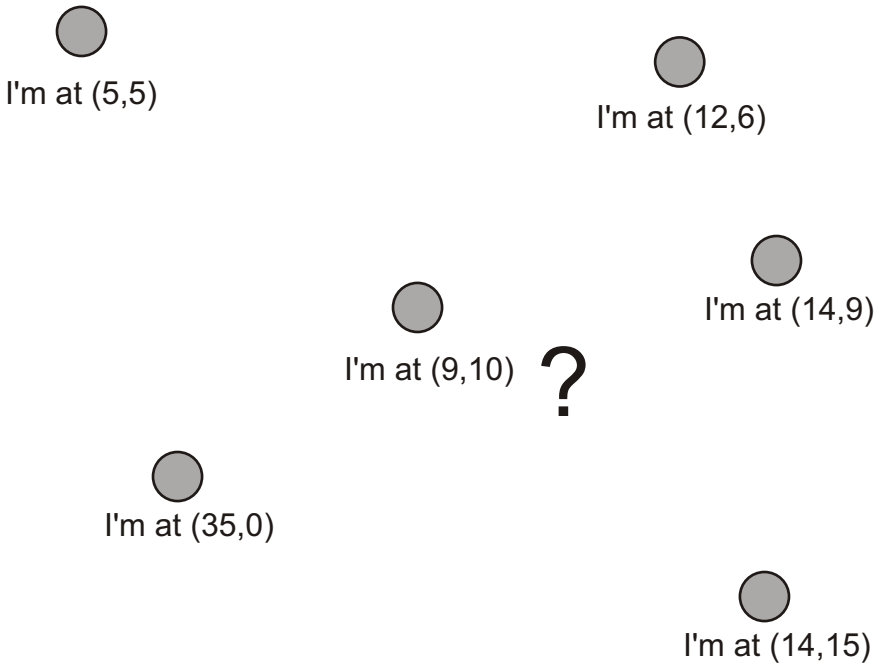
Secure Position Verification in Vehicular Networks Using Obfuscation

Ming-Yee Iu
Tutor: Maxim Raya

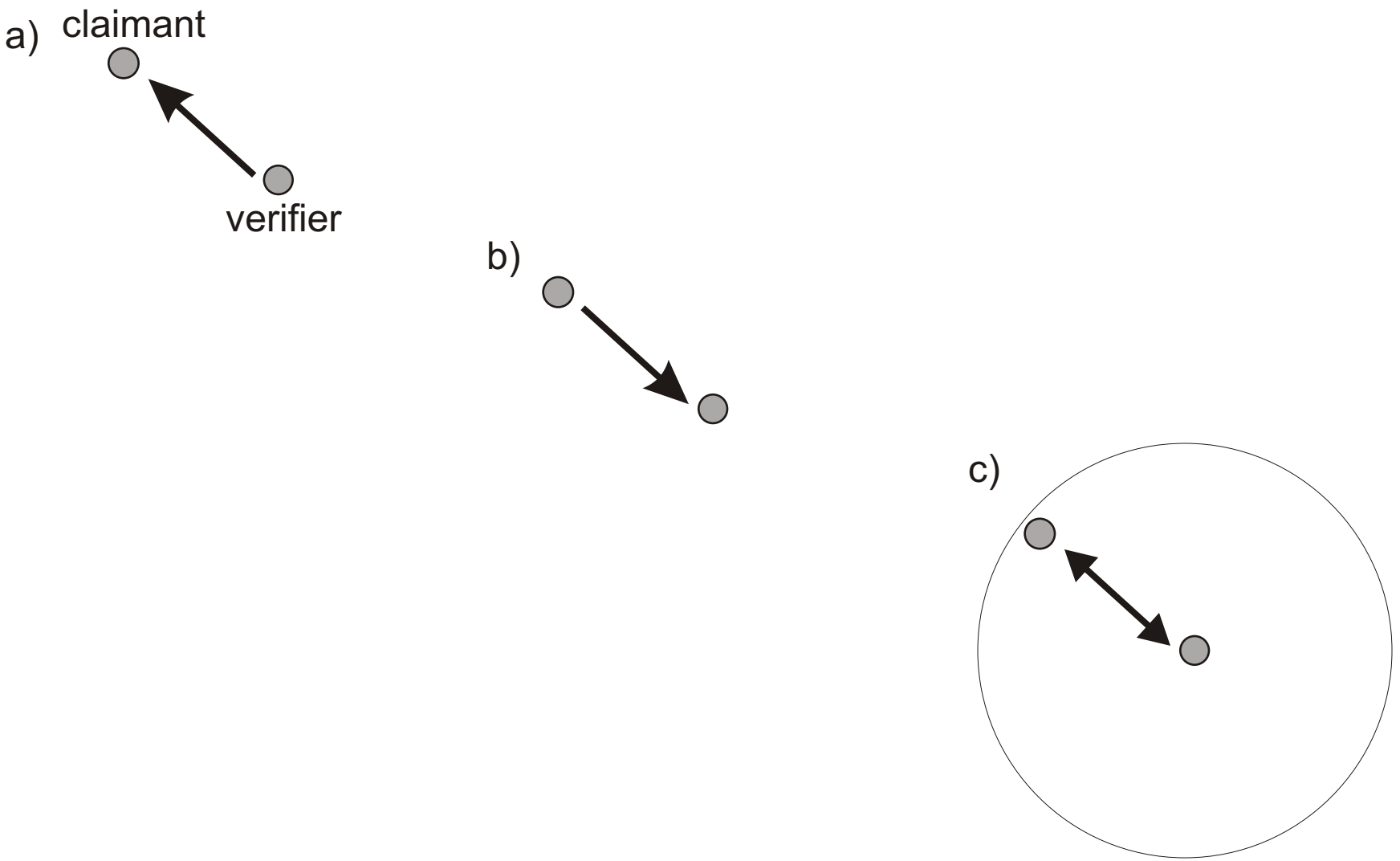
Secure Positioning



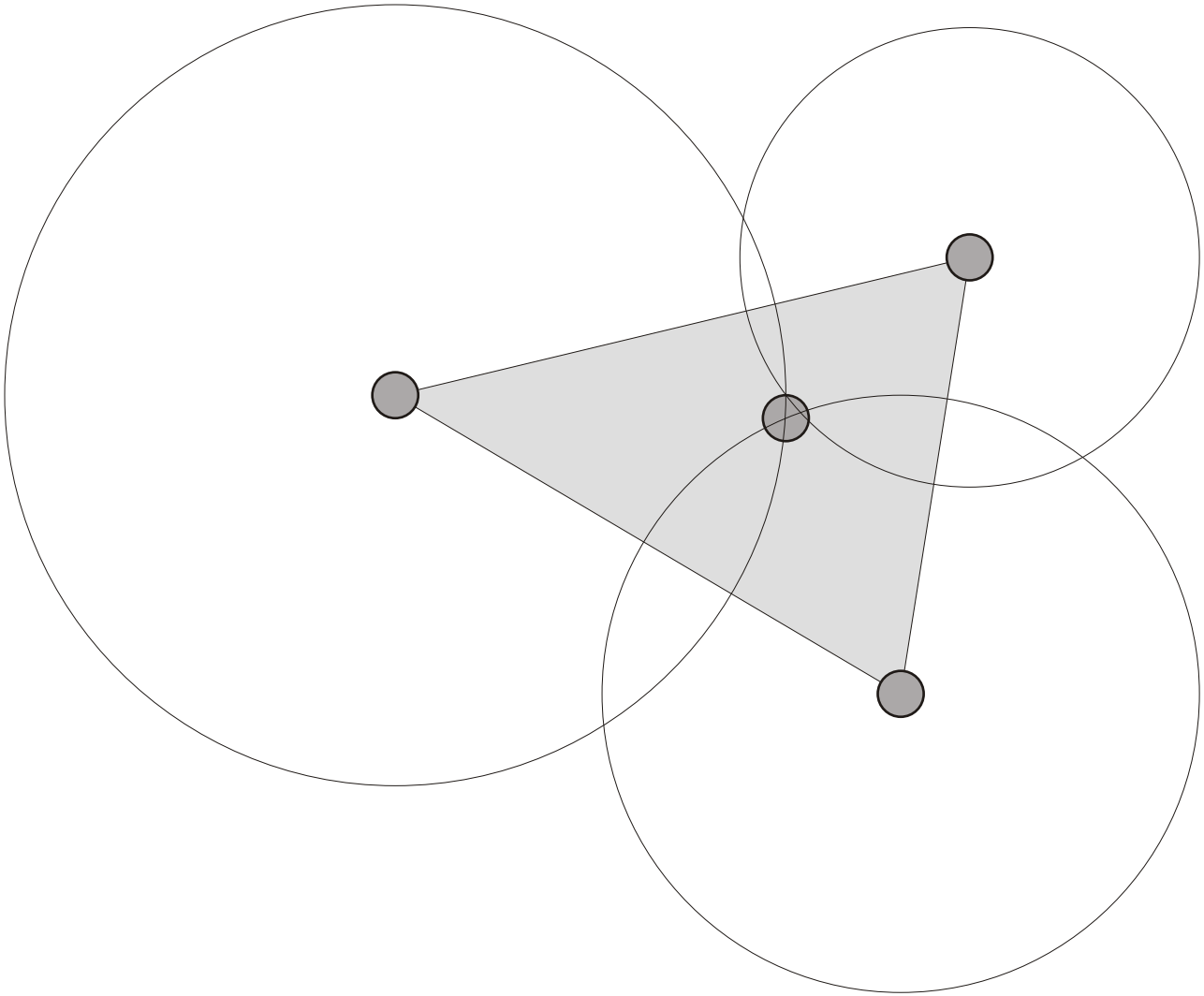
Secure Position Verification



Distance Bounding



Verifiable Multilateration

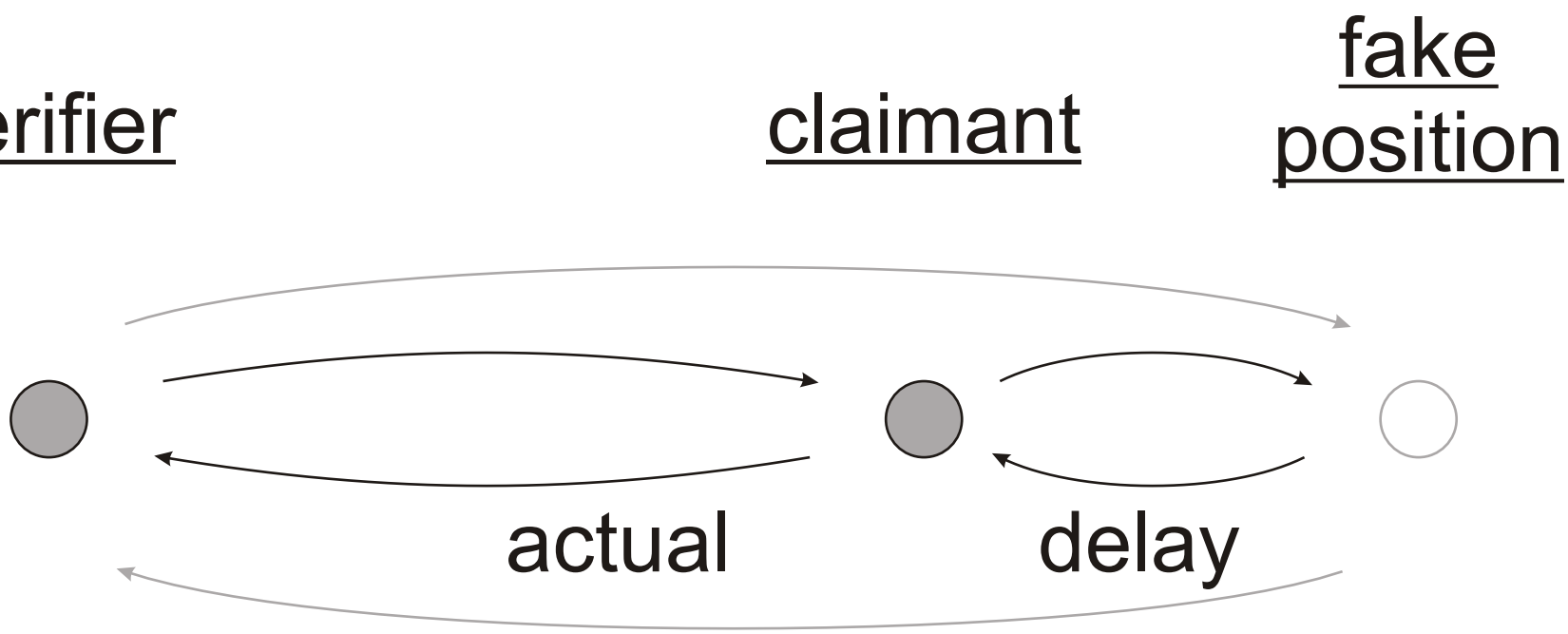


Secure Position Verification

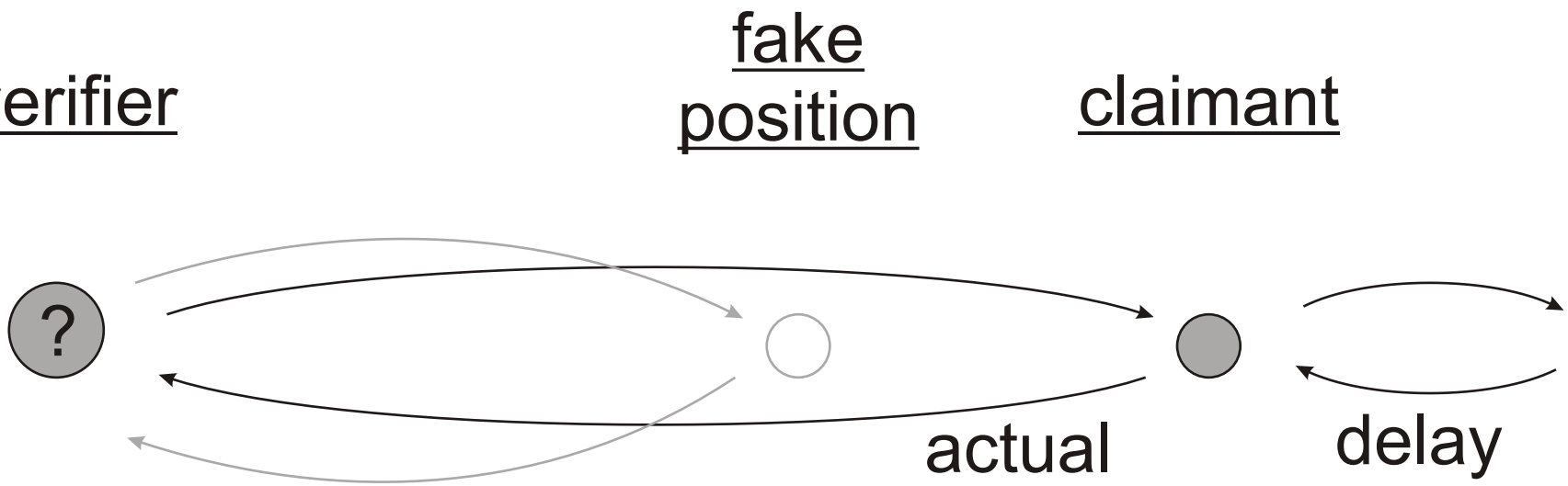
Secure positioning requires three nodes.

Can secure position verification be done with fewer?

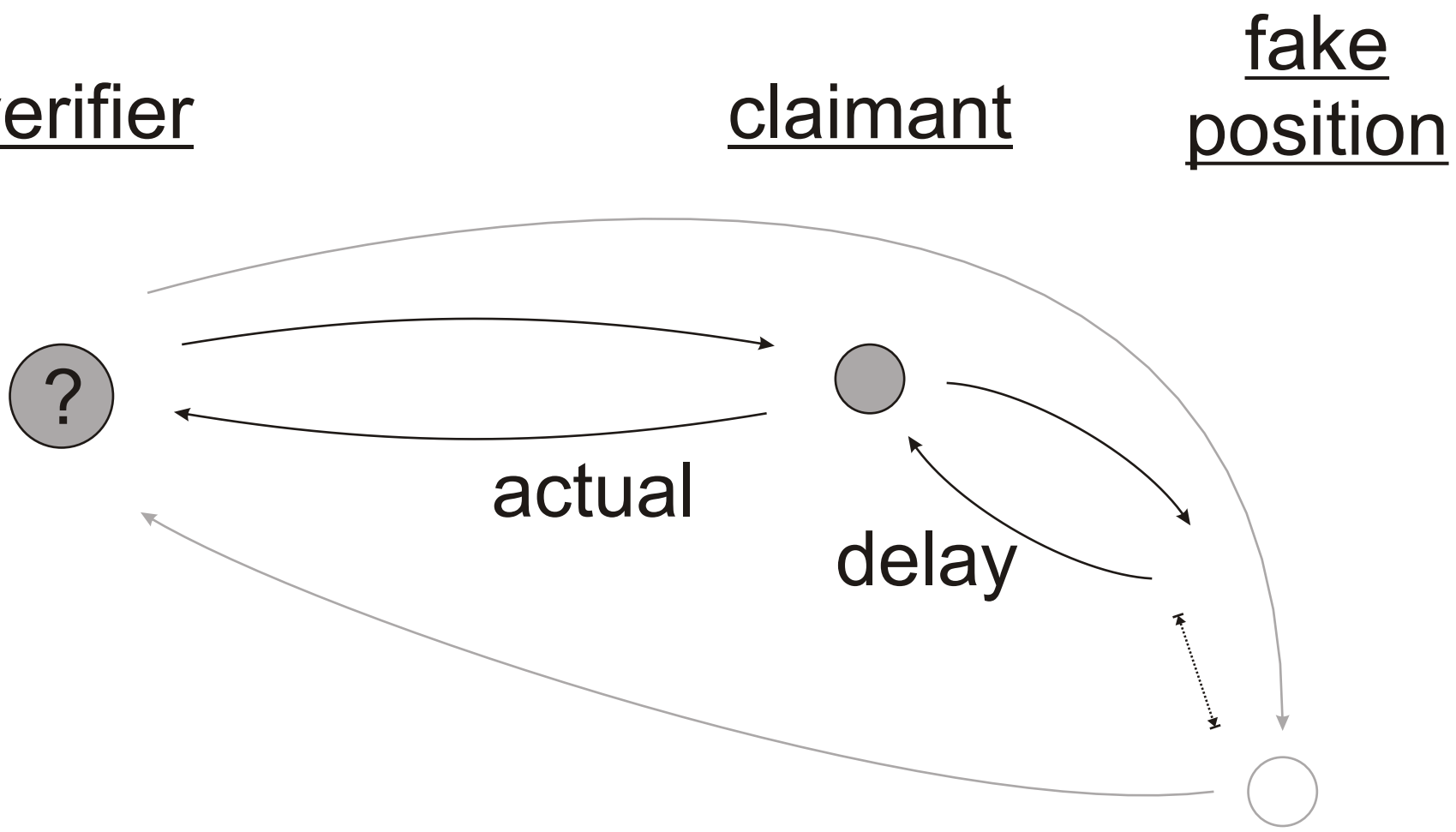
Cheating on Distance Bounding



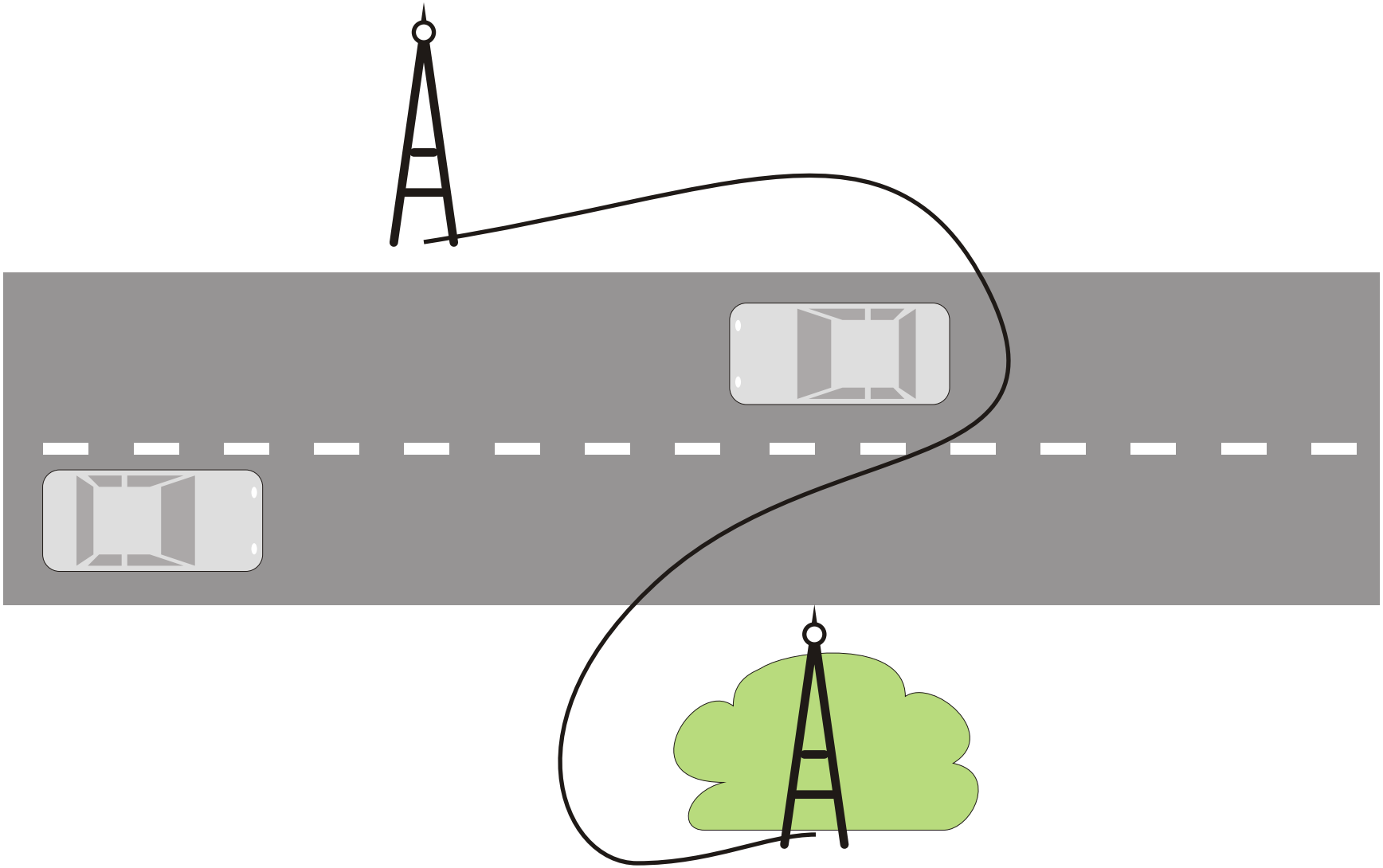
Cheating with Hidden Verifier



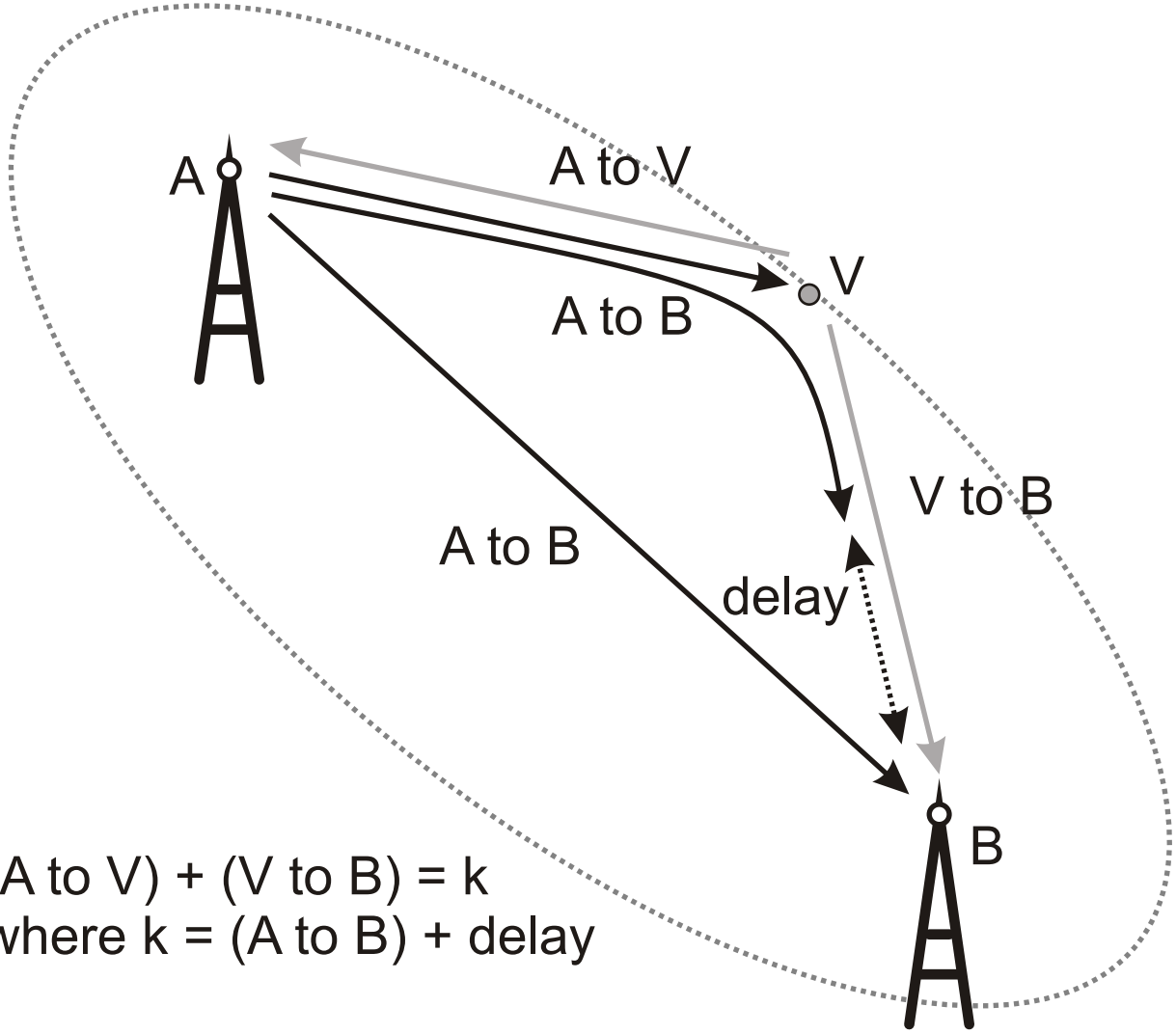
Cheating with Hidden Verifier



Infrastructure

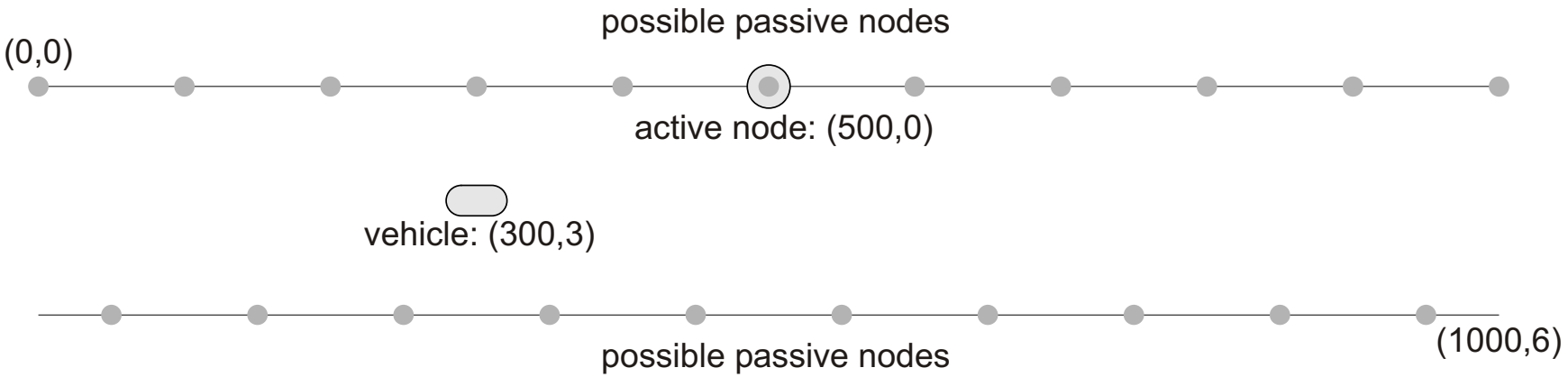


TDOA Ellipses



(A to V) + (V to B) = k
where k = (A to B) + delay

Simulation Configuration



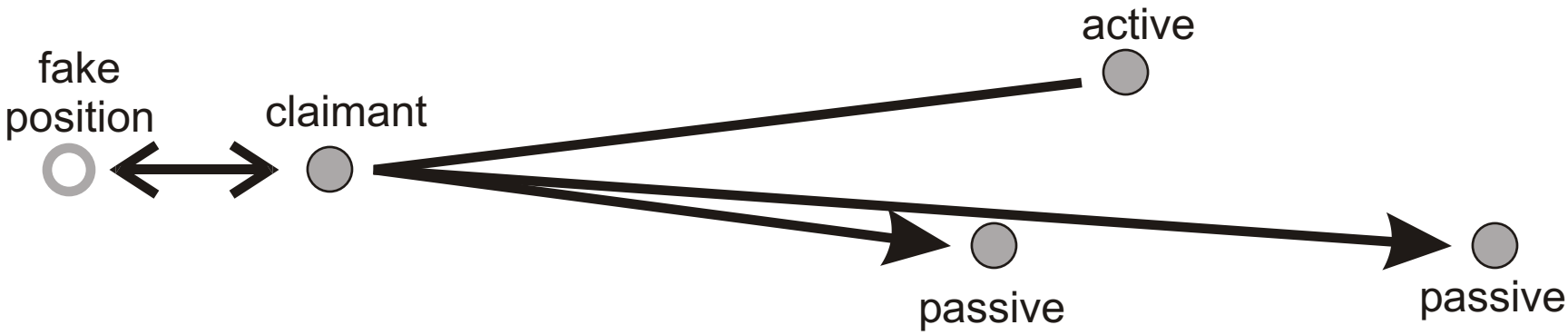
Initial Simulation

71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	95	28	28	28	28	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	95	28	28	28	28	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	95	28	28	28	28	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	100	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	95	28	28	28	33	33	33	33	33	33	33	33	33	33	33
71	71	71	71	71	71	95	28	28	28	33	33	33	33	33	33	33	33	33	33	33

With Active Checking

71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	95	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	95	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	95	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	100	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	95	0	0	0	0	0	0	0	4	4	4	4	4	4	4
71	71	71	71	71	71	95	0	0	0	0	0	0	0	4	4	4	4	4	4	4

The Problem



Passive Nodes Far from Road

0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	6	0	0
0	0	0	0	0	0	37	0	0	0	0	0	0	0	0	0	0	6	0	0
0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	6	0	0
0	0	0	0	0	0	93	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	87	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	6	0	0	6	0	0
0	0	0	0	0	0	12	0	0	0	0	0	0	0	0	6	0	0	6	0	0

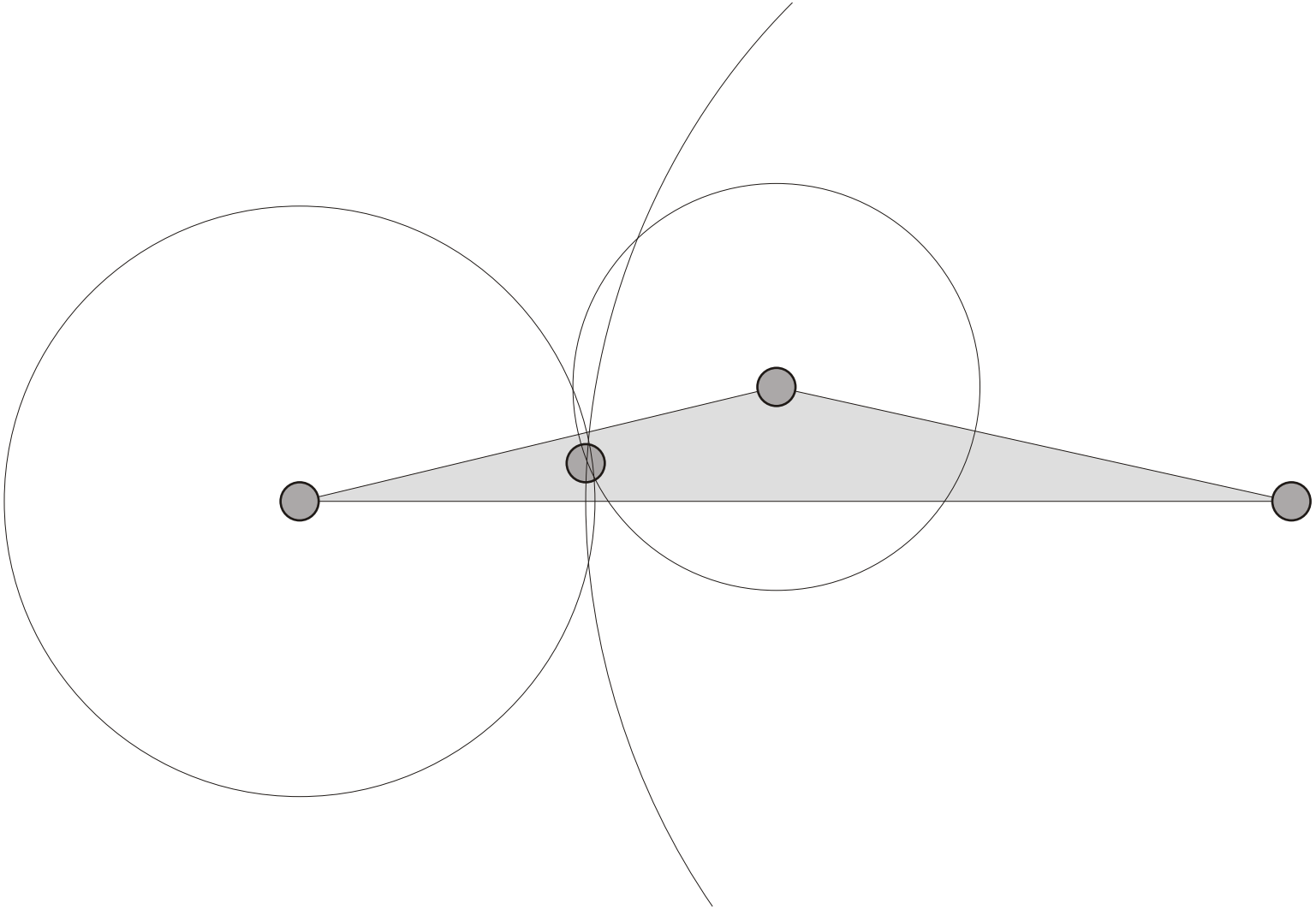
Zoomed In

6	12	12	12	12	18	18	25	25	25	31	31	37	50	50	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	12	12	12	18	18	18	25	25	31	31	37	50	50	37	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	6	6	12	12	12	18	18	25	31	31	37	50	56	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	6	6	6	6	12	12	18	18	18	31	43	50	62	68	93	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	6	6	6	12	18	25	37	37	50	68	93	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	6	6	12	18	25	31	43	50	62	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	6	6	12	18	25	31	43	50	68	93	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	6	6	6	12	18	25	25	37	50	62	75	87	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	6	6	6	12	12	18	18	31	37	43	50	56	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	6	6	6	12	12	12	18	18	25	25	31	37	43	50	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	6	12	12	12	18	18	25	25	25	31	37	43	50	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Active Node Far from Road Zoomed In

6	12	12	12	12	12	12	12	18	18	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	12	12	12	18	18	25	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	12	12	12	18	18	25	25	37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	12	12	12	18	18	25	25	37	56	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	12	12	18	18	25	25	31	56	81	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	18	18	18	25	31	37	50	62	75	100	100	68	0	0	0	0	0	0	0	0	0	0	0	0	0
12	12	12	12	12	18	18	25	31	37	43	50	56	68	100	100	93	37	0	0	0	0	0	0	0	0	0	0	0	0
12	12	18	18	18	18	25	31	37	37	43	50	50	50	56	100	93	37	31	0	0	0	0	0	0	0	0	0	0	0
12	12	18	18	25	25	31	31	37	37	43	37	37	31	12	0	6	25	31	25	25	0	0	0	0	0	0	0	0	0
12	18	18	25	25	25	31	31	31	31	25	18	6	0	0	0	0	6	18	25	25	18	0	0	0	0	0	0	0	0
18	18	25	25	25	25	31	31	25	18	12	0	0	0	0	0	0	0	6	12	18	18	18	0	0	0	0	0	0	0

Verifiable Multilateration Problems



Verifiable Multilateration Scenario

100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
~~100~~	~~100~~	~~100~~	~~100~~	~~100~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
~~100~~	~~100~~	~~100~~	~~100~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Vs. Stealth Nodes

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Verifiable Multilateration

100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
~~100~~	~~100~~	~~100~~	~~100~~	~~100~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
~~100~~	~~100~~	~~100~~	~~100~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Vs. Stealth Nodes

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Conclusion

With two nodes
- Can build a reasonable secure position verification system
- Side benefit: limited protection against collusion

With three nodes
- Can build a secure positioning system comparable to verifiable multilateration

Weaknesses
- Wired links
- Nodes far from road
- Nodes must be hidden