

AREX: An Adaptive System for Secure Resource Access

Brent Lagesse
Mohan Kumar
Matthew Wright

Department of Computer Science Engineering
The University of Texas at Arlington

Example

How do I get to the conference?

Turn left and go 3 km

Turn right and go 1 km



What is the problem?

- Malicious peers
 - Serve faulty resources
 - DoS
 - Violate privacy
- Benign peers may be unreliable
- In this context, security means being able to get what we want, when we want it

Reputation

- Advantages

- Many mechanisms are effective against small number of attackers

- Disadvantages

- Fails when most peers are malicious
- Susceptible to startup attacks and one-time attacks
- Performance degrades when assumptions about factors such as connectivity or mobility do not hold

System Goal

- Using reputation is difficult in some situations
 - Uncertain/Malicious systems
 - Systems with intermittent connectivity
 - Systems with peers that are very sensitive to attack

- Goal: Provide protection for peers in systems where reputation performs poorly by not relying on other peers for information

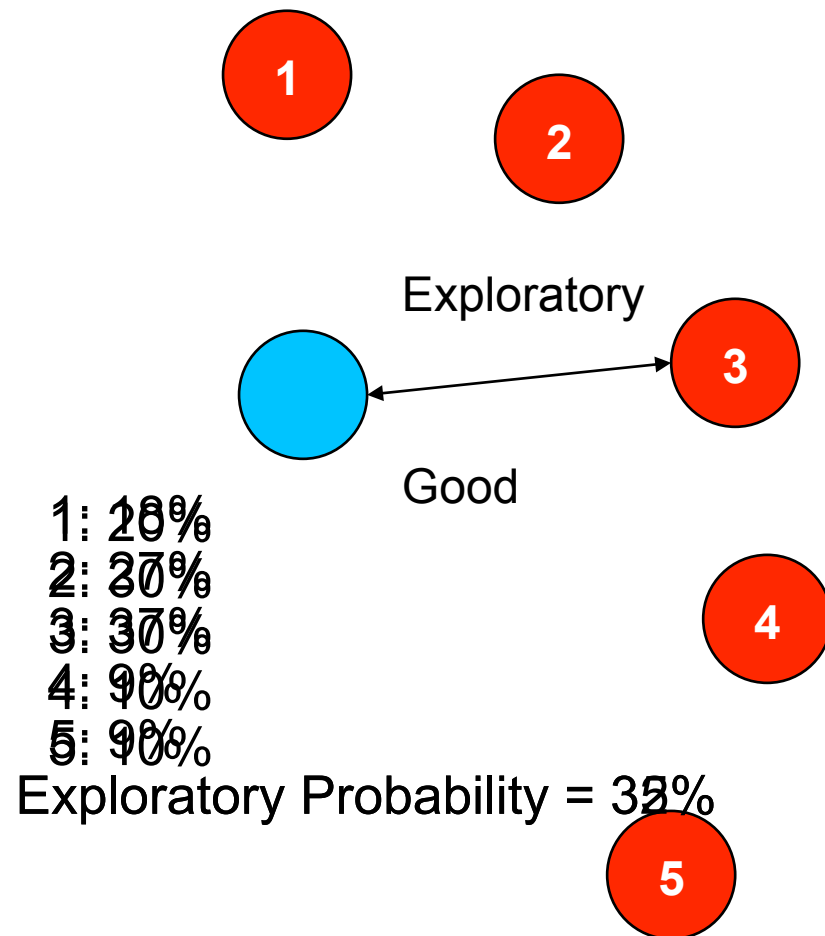
Resource Exploration

- Intermixes “Exploratory” messages with real requests
- Exploratory messages are indistinguishable to the attacker from real requests
- The response to exploratory messages can be easily verified by the sender to see if an attack occurred
 - Example: Asking a peer to solve a computationally intense problem for which I already have the solution
- Exploratory messages help discover which peers are malicious without being damaged by an attack

Adaptive Resource EXploration

- Implements the Resource Exploration strategy
 - Resource Exploration randomly tests the resources provided by peers
- Creates an incentive for peers to provide resources rather than attack
- Designed to operate efficiently against both strategically malicious peers and with benign peers

Overview of AREX



- 1) AREX peer randomly selects the peer to communicate with
- 2) AREX peer randomly chooses whether to explore or access
- 3) AREX peer evaluates the response
- 4) AREX peer readjust strategy based on response

How do we decide the selection rate and exploration rate?

Computing Selection Rate

- Keep track of known peers
- Assign each a value based on previous experience
- Calculate the selection probability based on value
- **Alpha** – Amount to increase after a good interaction
- **Beta** – Amount to decrease after an attack

Computing Selection Rate

Alpha = 2 Beta = 1

Event	Peer 1	Peer 2	Peer 3	Peer 4	Peer 5
Initial Round	0	0	0	0	0
	20.00%	20.00%	20.00%	20.00%	20.00%
Peer 2 returns good resource	0	2	0	0	0
	14.28%	42.86%	14.28%	14.28%	14.28%
Peer 4 returns good resource	0	2	0	2	0
	11.11%	33.33%	11.11%	33.33%	11.11%
Peer 2 returns bad resource	0	1	0	2	0
	12.50%	25.00%	12.50%	37.50%	12.50%
Peer 5 returns good resource	0	1	0	2	2
	10.00%	20.00%	10.00%	30.00%	30.00%
Peer 2 returns good resource	0	3	0	2	2
	8.33%	33.33%	8.33%	25.00%	25.00%

Computing Exploratory Rate

- Set up as a 2 player game
 - AREX peer vs. the rest of the system
- Initial Exploratory rate computed as if attacker is optimal and omniscient
- Exploratory rate adapts in reaction to opponent actions
- Always trying to maximize expected utility

		P2	
		Explore	Request
P1	Attack	C_{Ben} C_{Disc} C_{Ben}	C_{Ben} B_{Mal} C_{Ben} C_{Vic}
	Serve	C_{Ben} C_{Ben}	C_{Ben} C_{Ben} B_{Acc}

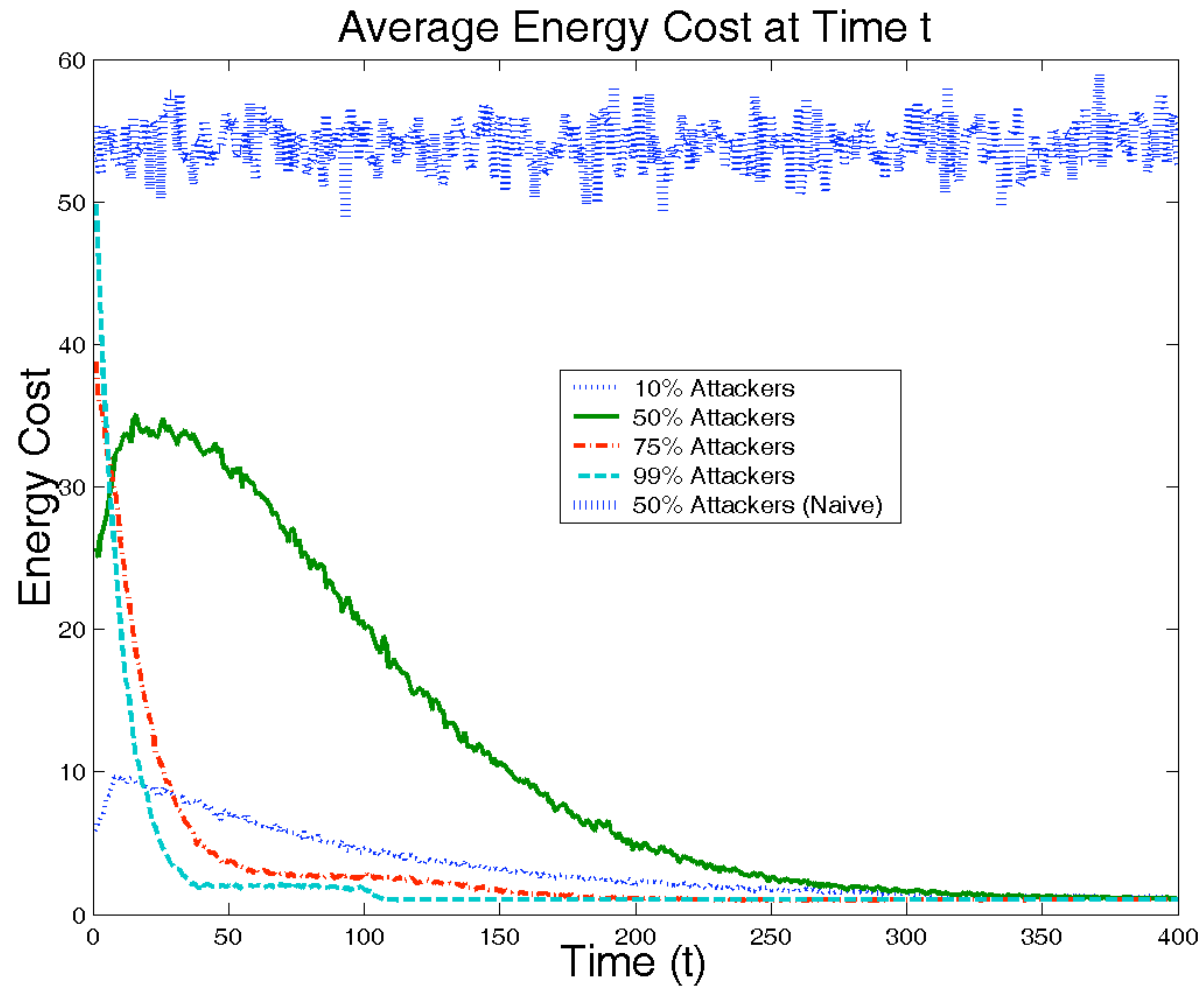
Simulation Setup

- Random Graph P2P Network
- Number of Peers – 1000
- Average Benign Peer Reliability – 95%
- Execution Time – 1000 iterations
- Attack Rate of Malicious Peers – 100%
- One request per time-step from the AREX peer

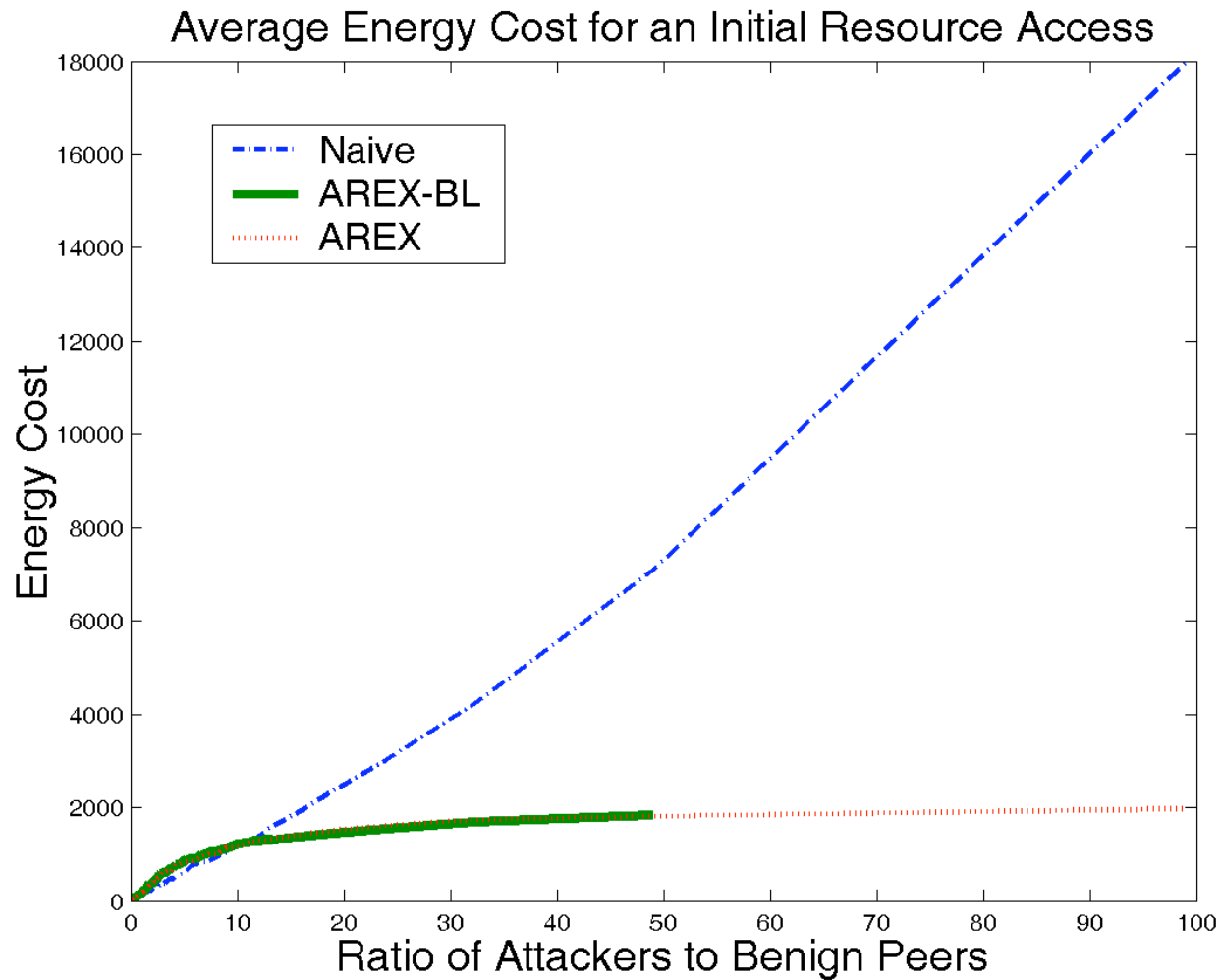
System Participation	1
Victim	100
Malicious Action	0
Discovered as an Attacker	1

Access	120
Successful Attack	100

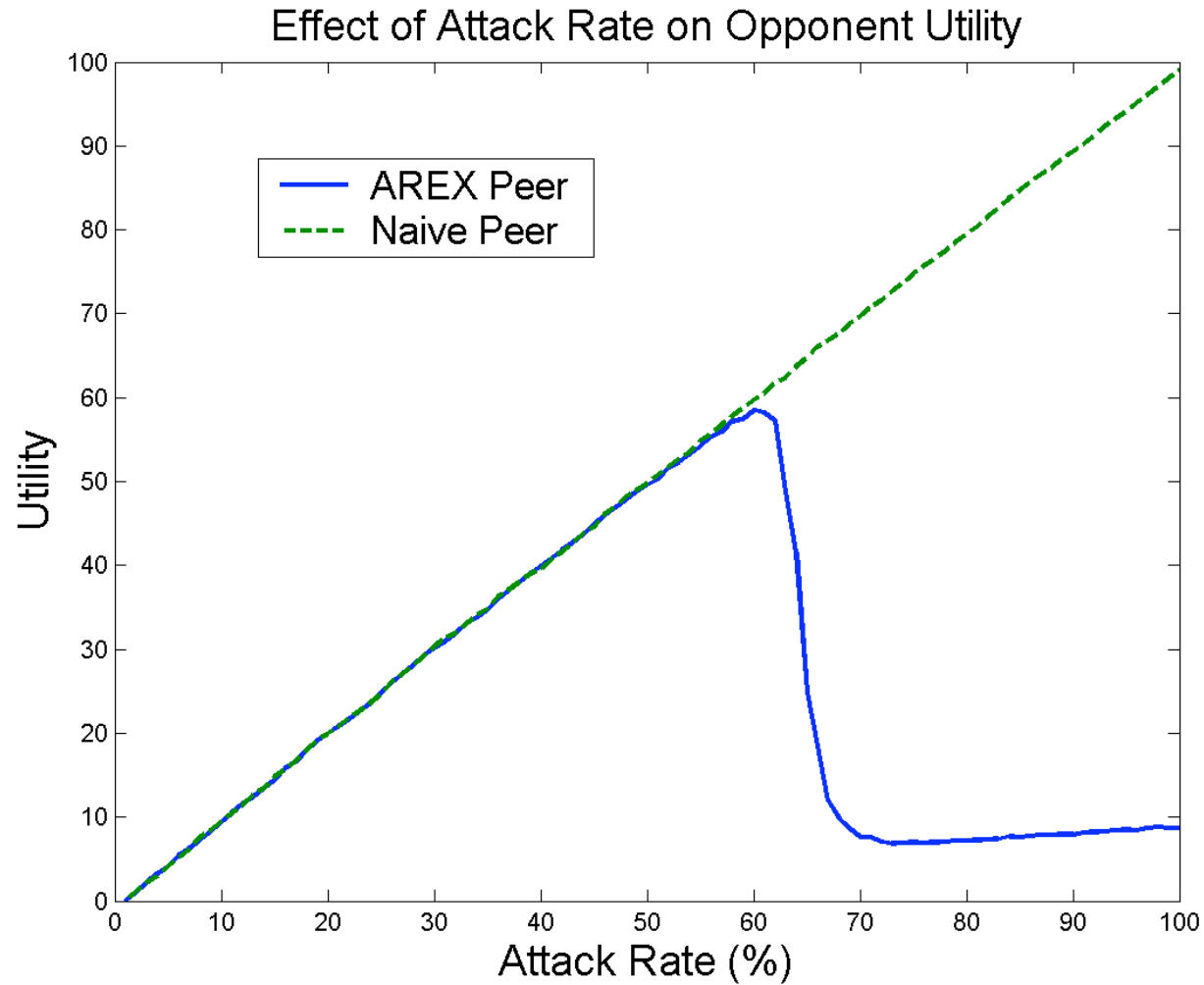
Adaptation over Time



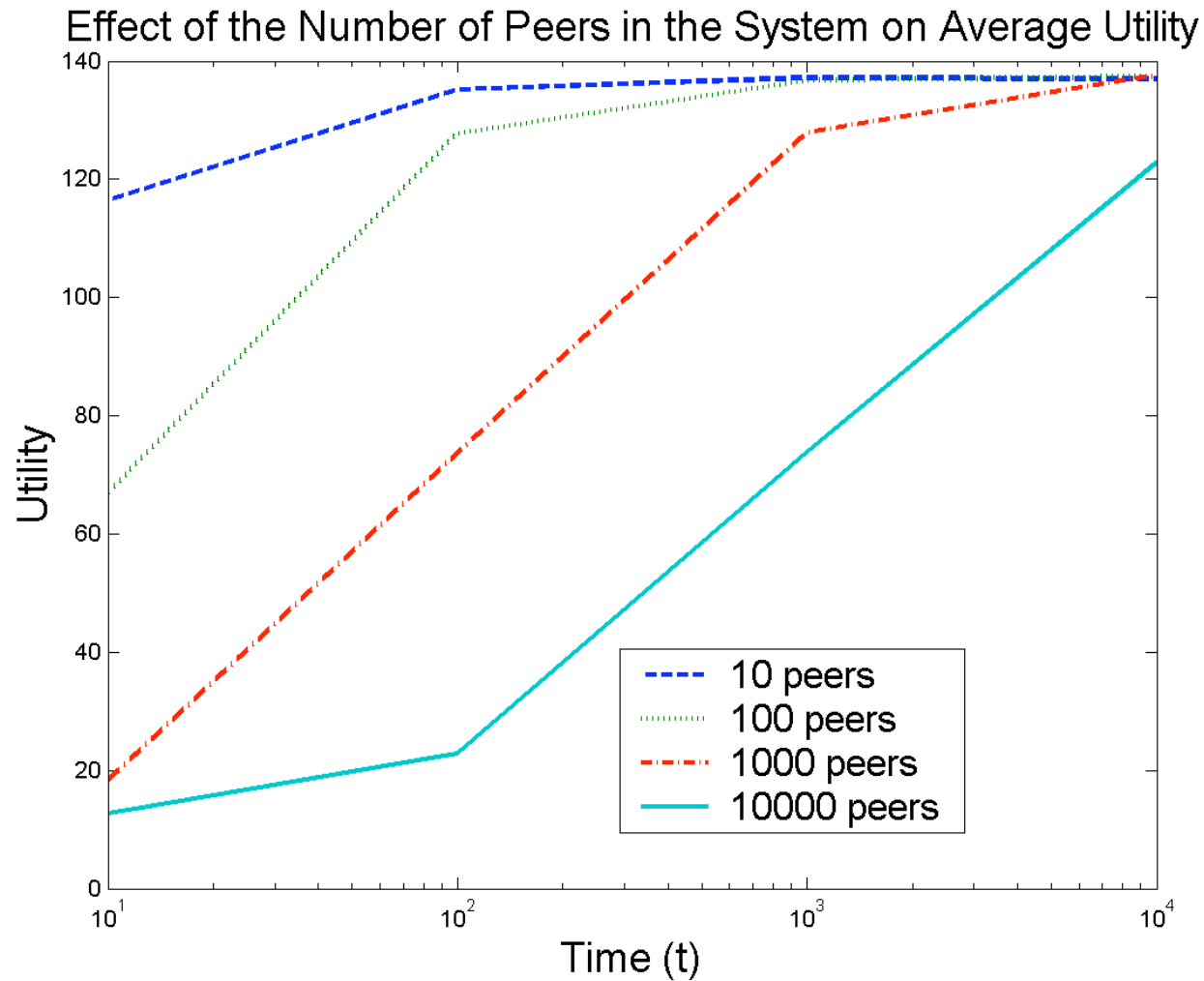
Initial Cost



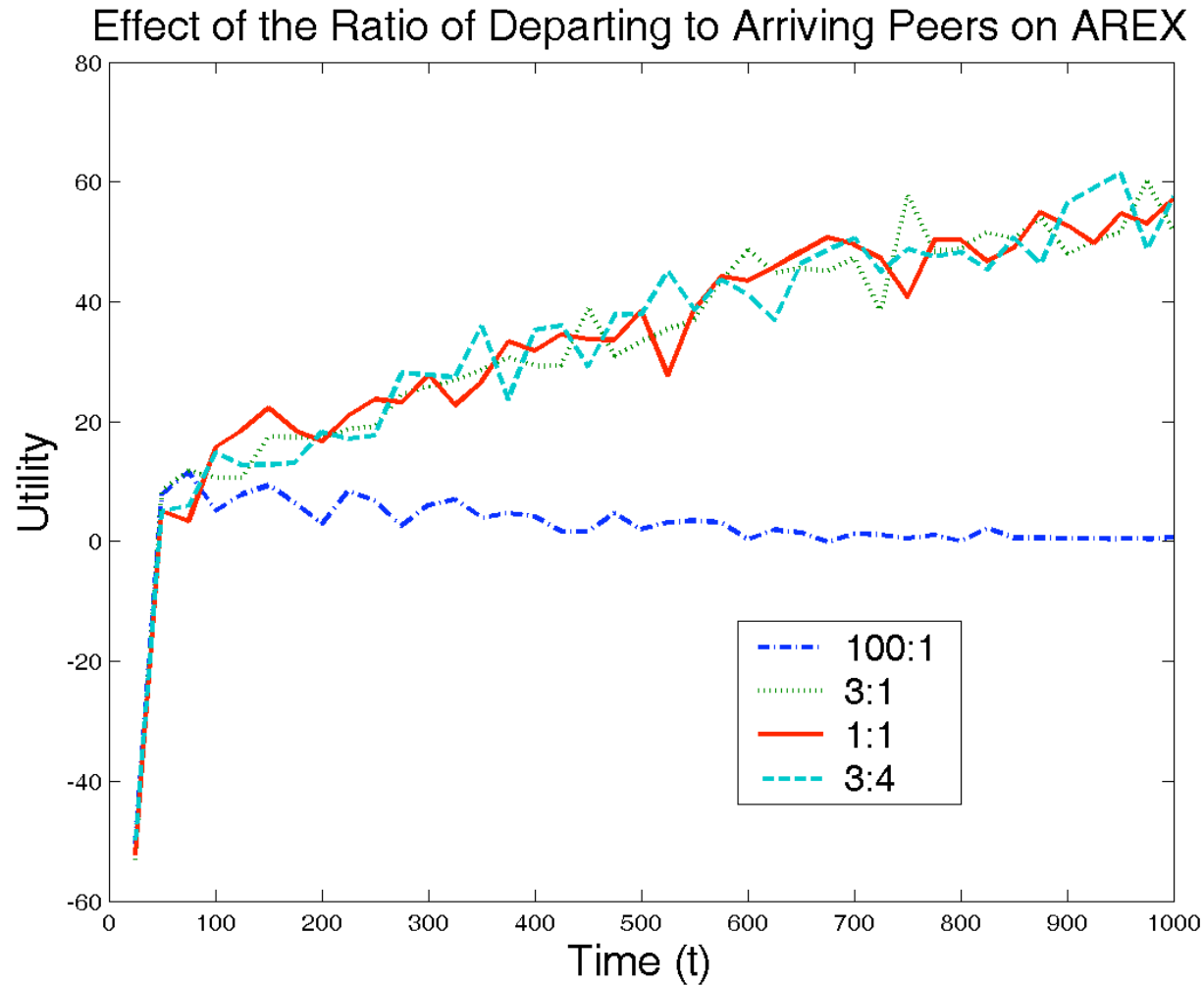
Effect on Attackers



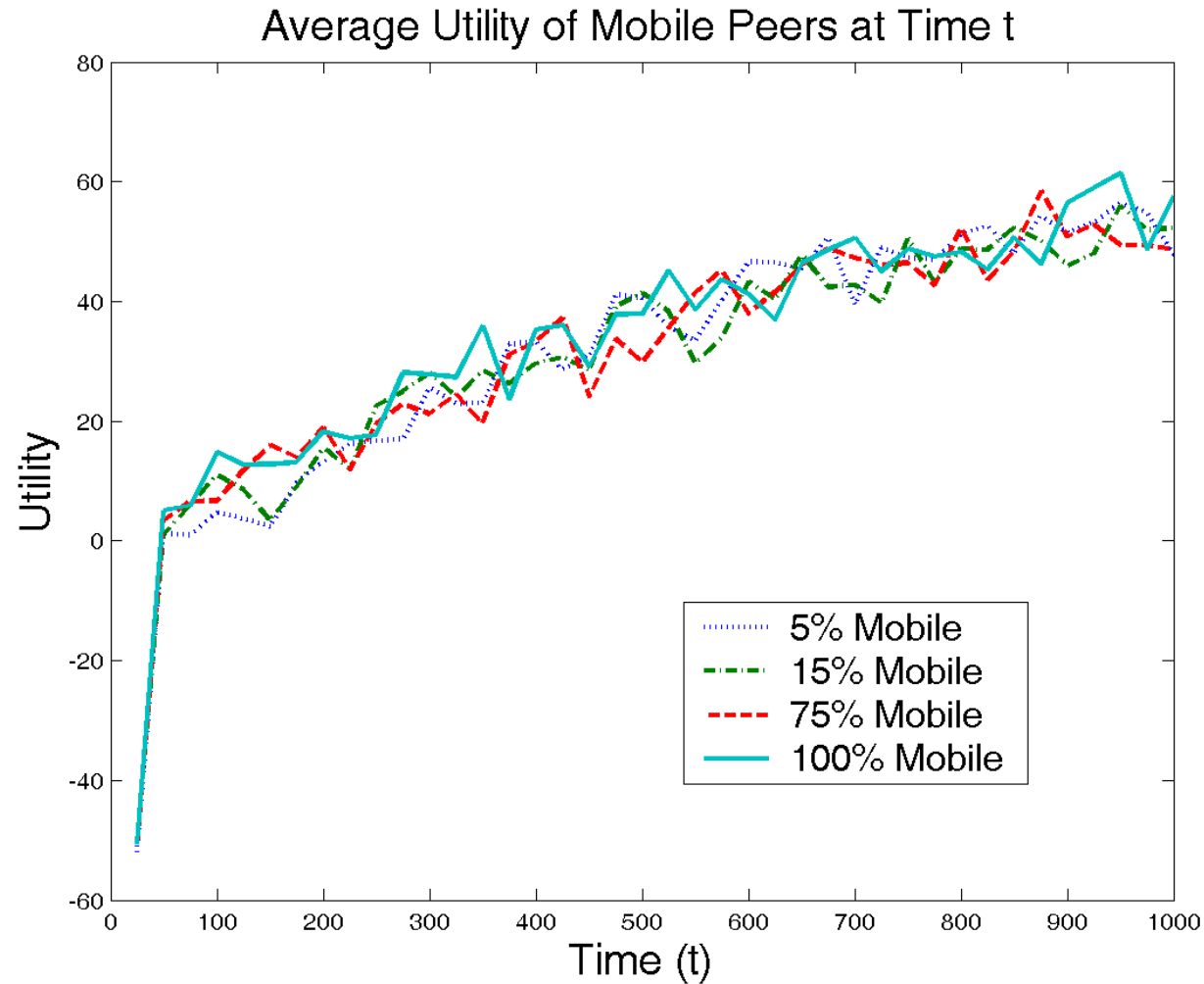
System Size



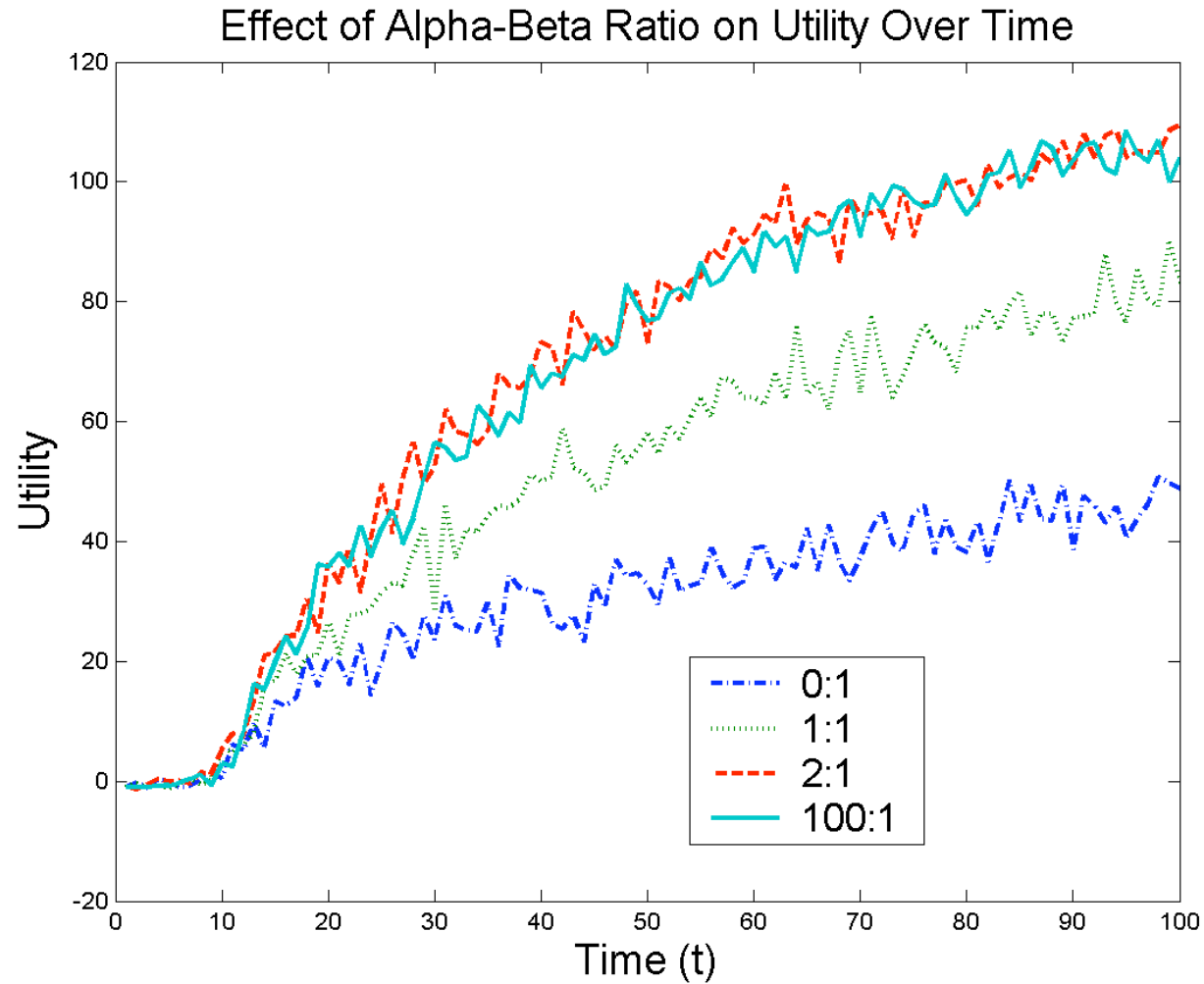
Effect of Dynamicity



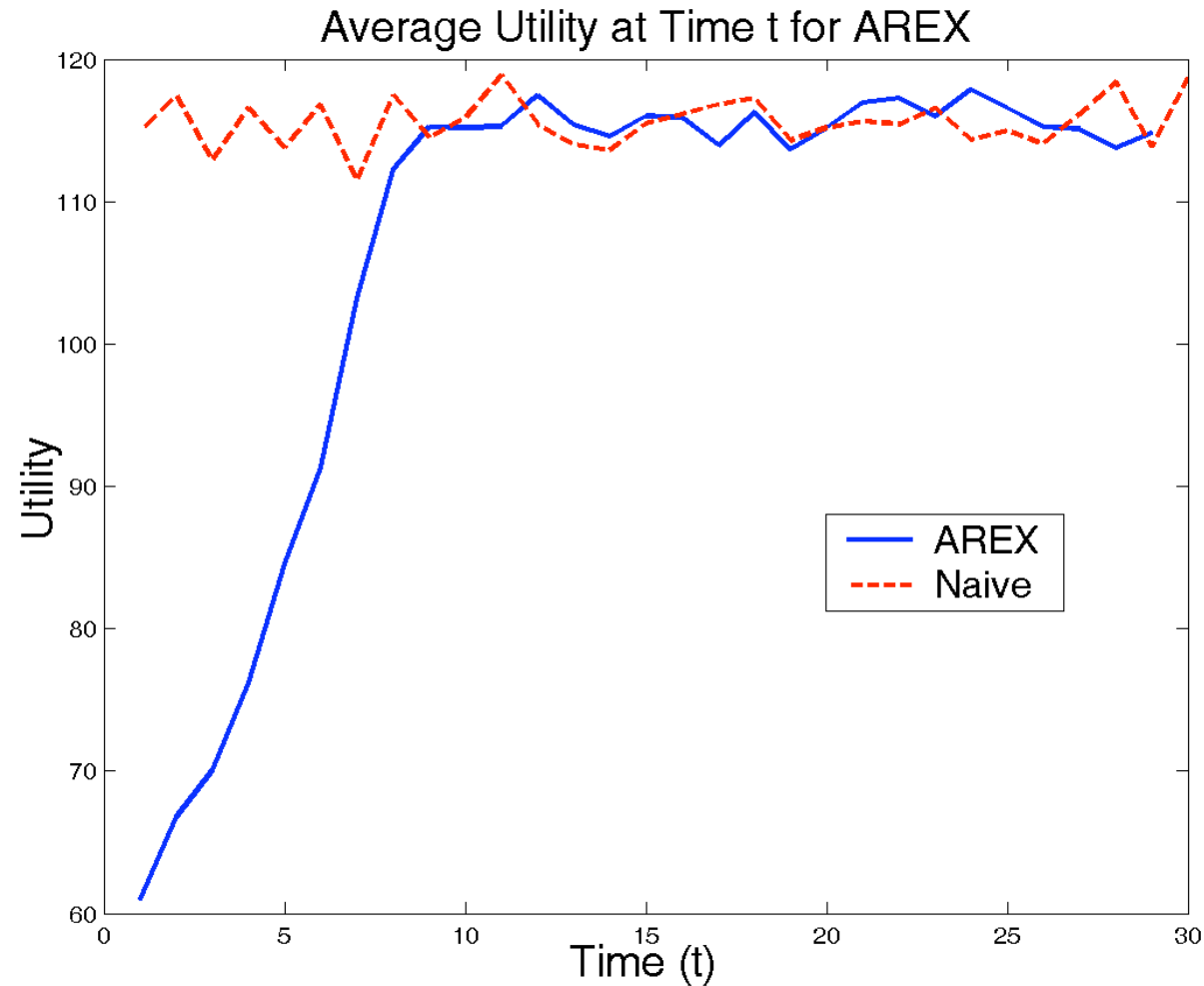
Mobility



Reaction speed



Adaptation to a Benign Environment



Key Contributions of AREX

- Tolerance to inadvertent errors by benign peers
- Approximation of a Nash equilibrium in a dynamic and uncertain system
- Adaptation of Nash equilibrium to optimize utility against non-optimal malicious peers

Example

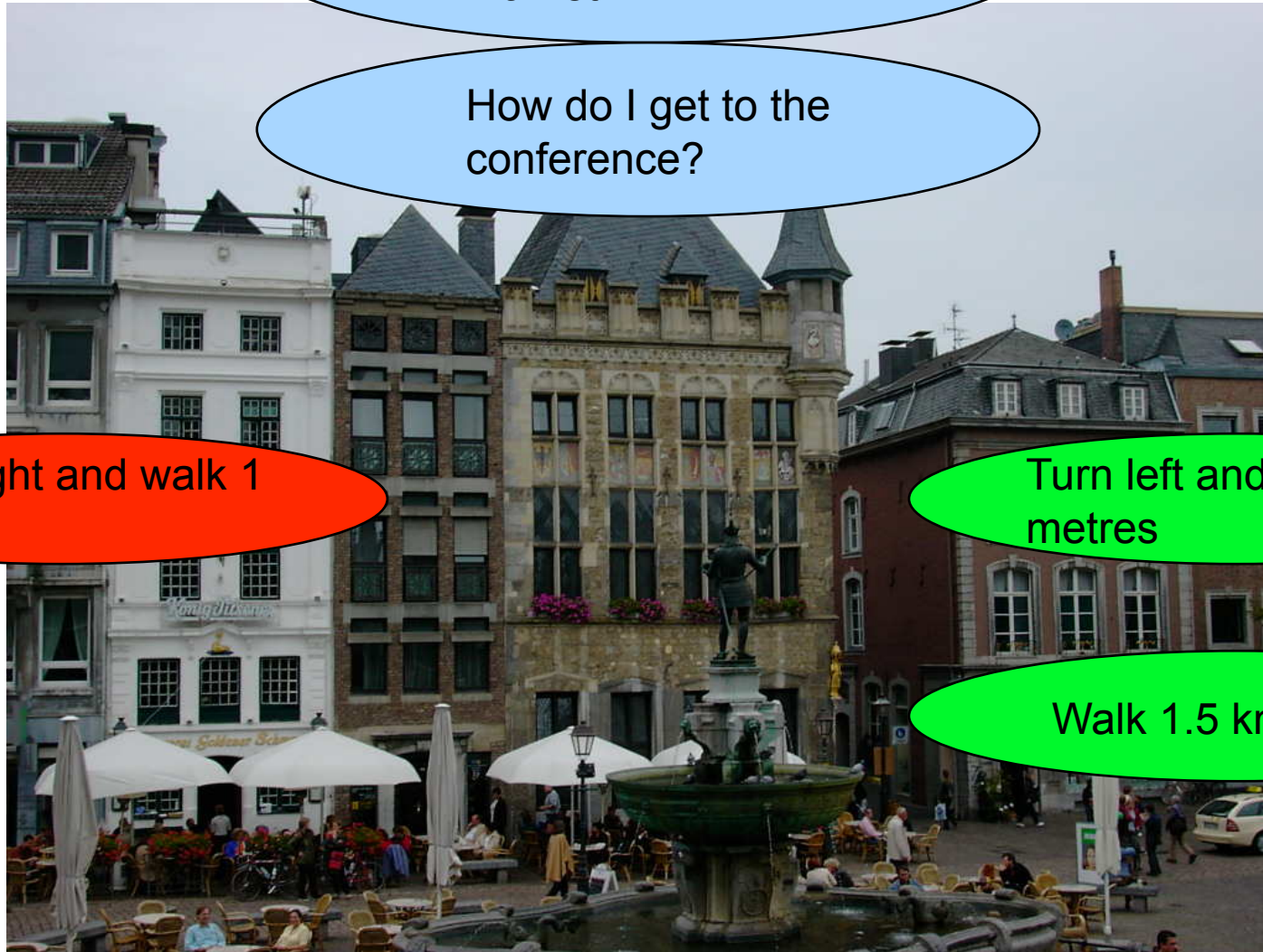
How do I get to the market?

How do I get to the conference?

Turn right and walk 1 km

Turn left and walk 500 metres

Walk 1.5 km ahead



Conclusions

- AREX is designed for hostile and uncertain environments, but also adapts quickly to benign environments
- AREX balances the trade-off between exploration and utilization of resources

	Reputation	AREX
Start up attacks in uncertain environments	No defense	Reduces effectiveness by testing peers
Frequent Disconnections	Cannot exchange information well	Does not rely on information exchange
One-time attacks	Cannot combat	Reduces effectiveness by testing peers