



Analysing the fairness of trust-based MANET protocols

I D Burke

M S Olivier

R P van Heerden

CSIR

our future through science

Overview

- What is a MANET and why is trust important in it?
- How does this relate to other scenarios of trust?
- Existing Protocols
- What affects trust in a MANET environment?
- Simulation Scenarios
- Results and Future work





What is a MANET and why does it need trust?

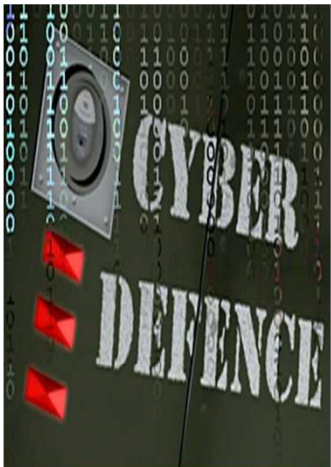
Mobile Adhoc Networks

- A collection of mobile nodes capable of sending and/or receiving wireless communications.
- Each node acts as a sender, receiver or intermediate
- This eliminates the need for centralised administration.
- Ideal for emergency rescue or military operations



Role of trust within a MANET

- The lack of centralised administration makes MANETs a target for network attacks and node misbehaviour.
- Each node has limited resources and by acting selfishly they can optimise their gain at the cost of the other network nodes, resulting in an iterative Prisoner's dilemma.





How does MANETs relate to other trust scenarios?

Trust scenarios in MANET compared to Online Trading

- Equations that do not accurately identify the current reputation of agents.
- Starting reputation is set too low, which acts as a barrier to new entries into the network.
- There is no incentive to rate peers.
- There is no ability to filter or search by reputation score.
- Use of a single general reputation system.
- Most systems have an unlimited memory.
 - A. Malaga





Existing Trust Protocols

Trusted Adhoc On-Demand Distance Vector Routing (TAODV)

- Trust based on: Belief, Disbelief and Uncertainty
- These values are formed based on past experiences.
- Nodes able to give opinion about other nodes based on trust chain.

$$\left\{ \begin{array}{l} b_B^A = \frac{p}{p+n+2} \\ d_B^A = \frac{n}{p+n+2} \\ u_B^A = \frac{2}{p+n+2} \end{array} \right.$$

$$\left\{ \begin{array}{l} b_C^{AB} = b_B^A b_C^B \\ d_C^{AB} = b_B^A d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A u_C^B \end{array} \right.$$

How

STEA

Trusted Energy Aware ADOV

- Introduces concept of Reliability by factoring in Battery power of node when assigning trust value.
- Uses various metrics to qualify node connection reliability. Such as number of packets per transmission interval and a similar trust scheme to that of TAODV

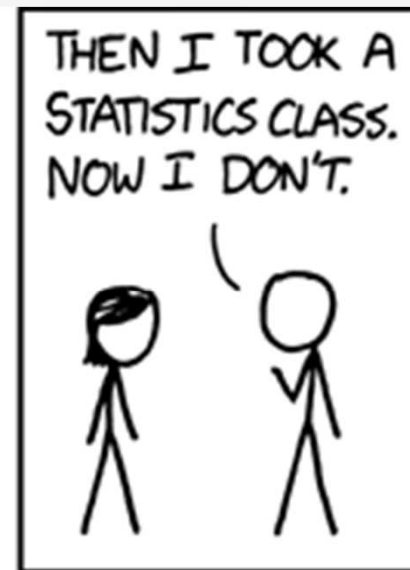
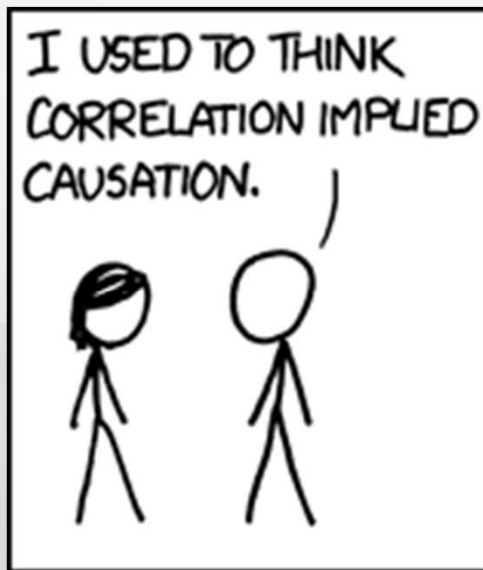




The big question: What actually affects trust?

Finding the cause of mistrust

- Node density
- Node Location
- Bad measurements/data
- Bad algorithms
- Node handover rate





Scenario selection



- Chose to investigate three very basic scenarios.
- The goal was to investigate
 - Trust build-up time
 - Treatment of new nodes to the network
 - The detection of marginally misbehaving nodes (Misbehave 10% of the time)



Results and future work

Comparison

- Scenario 1 (Trust buildup)
 - TAODV takes all transactions into account, hence it continues trusting node B long after node B no longer has the battery power to communicate to A
 - TEA-AODV on the other hand seems to be too strict, it values battery power more than actual capability to deliver data.



Comparison (2)

- Scenario 2 (New entrant)
 - TAODV only allows new entrant to act as relay after depletion of B's battery. This is unfair towards B.
 - TEA-AODV performs better. Traffic load is share more evenly between relay nodes.



Comparison (3)

- Scenario 3 (Slight misbehaviour)
 - TAODV picks up the misbehaviour, but due to misbehaviour node B is capable of achieving a higher transmission success rate due to higher battery power.
 - TEA-AODV. The misbehaving node actually benefits from misbehaving since its battery power usage is reduced and hence it can communicate for longer.



Future work

- Identify more micro scenarios which may lead to mistrust.
- Define new algorithm to address these issues.
- Test these scenarios with the new algorithm in large scale scenarios.



Questions

