Mobile ad hoc networks Various problems and some solutions

Humayun Bakht
School of Computing and Mathematical Sciences
Liverpool John Moores University
Email: humayunbakht@yahoo.co.uk
Main Focus

- **Problems**
  - We will see what are some of the important problems in MANET

- **Importance**
  - We will discuss their importance i.e. why do we need a solution of these problems?

- **Solutions**
  - I will highlight some of the possible solutions to these problems.

- **What I will not discuss is routing**
Some problems

- Security
- Routing (will not discuss)
- Hidden terminal problem
- Bandwidth
- Power limitation
- Corroboration of mobile devices
  - One final point all of these problems are related to the unique art of network formation of Mobile ad-hoc networks (MANET)
Protecting data transformation in mobile ad-hoc networks is an important aspect to be seen.

Parties within the network want their communication to be secure.

At present MANET do not have any stick security policy.

This could possibly lead active attackers to easily exploit or possibly disable mobile ad-hoc network.
Security 1

- Mobile ad-hoc networks are highly dynamic i.e. topology changes and link breakage happen quite frequently.
- We need a security solution which is dynamic too.
- Any malicious or misbehaving nodes can create hostile attacks.
- These types of attack can seriously damage basic aspects of security, such as integrity, confidentiality and privacy of the node.
Security 2

- Some of the main security requirements of MANET
  - Certain discovery
    - route should always be found if it exits between two nodes.
  - Isolation misbehaving nodes
    - misbehaving nodes should always be identified and isolated from routing
  - location privacy
    - protection of information about node location and network structure
Security 3

- Types of attacks
- Passive attack
  - Passive attack do not disturb the operation of MANET and attacker tries to steal/discover valuable information by listening to the network traffic.
- Active attack
  - Active attack injects arbitrary packets and tries to disrupt the network operation
  - The main aim of such attacks is to limit the availability gain authentication or attract packets destined for other nodes.
Security 4

- At present Security goal in mobile ad-hoc networks are gained through cryptographic mechanisms.
- Example of some of the cryptographic mechanisms are public key encryption or digital signature.
- These mechanisms are backed by centralized key management.
- Trusted Certificate Authority (CA) provides public key certificate to mobile nodes in order to develop mutual trust between nodes.
- However, Chances are any disturbance with Certificate authority can easily affect the security of the entire network.
Corroboration of mobile devices in mobile ad-hoc networks

- Each node in MANET relies on others to forward data packets to the other nodes in the network.
- Some of the reasons why mobile nodes in ad-hoc networks would prefer not to cooperate are
- One important thing
  - In MANET Nodes establish ad hoc structure in one of two cases
Corroboration of mobile devices in mobile ad-hoc networks

- **Case 1**
  - to reach those destinations that would either require a significant amount of transmission energy using single hop communication

- **Case 2**
  - When transmission flow is not possible without routing the traffic through other nodes.
  - In both cases nodes spend energy without receiving any direct benefit
corroboration of mobile devices in mobile ad-hoc networks 2

- If a node only considers its own short term live period then it may not choose to participate within the network.

- Concept of introducing measure for corroboration of mobiles devices into the architecture of MANET becomes one of the important issues.

- Please note here I am not discussing about localization of mobile nodes for which we have number of different
corroboration of mobile devices in mobile ad-hoc networks 3

- This problem is out of the focus of our project, however I have proposed two solution to tackle this issue.
- A node can volunteer itself as an administrative node.
- Number of measure could be taken to identify self-fish node.
- Such as we may include a specific header identifies each participating nodes.
- Each of the nodes on the way to the destination require to remove this header before forwarding it to its next hop.
- In this way if any of the link found missing could be treated as a self-fish nodes.
- You may think, this link could also be taken as broken link, then how can we differentiate in between the two.
- Obviously if the node is active and receiving and forwarding only those packet which are of interest to it.
- Could easily be identified.
Corroboration of mobile devices in mobile ad-hoc networks

- The system could be reboot and the node could be banned from there.
- Second option is to make use of global positioning systems.
- This GPS system can force small number of mobile devices to be fixed in a small region. Through this type of strategy we can possibly track down self-fish node.
Corroboration of mobile devices in mobile ad-hoc networks

- One benefit: GPS enables not only the use of position centric methods of addressing and routing.
- One drawback: GPS scheme make use of extra equipments to localize various nodes to route packets across the network.
Finally

- I am stopping here due to time limitation. However, I have intention to cover rest of the problems and discuss their solutions, off-course if time permits.
- Please drop me email at humayunbakht@yahoo.co.uk
- You can also read some of my articles on this subject:
  - A focus on the challenges of mobile ad hoc networks at http://www.computingunplugged.com/issues/issue200408/00001346001.html
  - Importance of secure routing in MANET at http://www.computingunplugged.com/issues/issue200408/00001327001.html
Questions time

- Questions ?