Security Analysis of MANET in NS2

Giancarlo Pellegrino <gianko@trouge.net>

mWSF06
Mini Workshop on Security Framework 2006, Catania, December 12, 2006
"Security in Mobility"
I - Introduction

- MANETs;
- Basic network operations.

II - Security Analysis

- Background
  - Features hide lacks
  - Routing protocols
- Attacks
  - Passive attacks
  - Active attacks

III - Conclusions
Introduction
MANETs

MANET mean **Mobile Ad hoc NETwork** or **Multi-hop Ad hoc NETwork**

- It is a wireless open network;
- a temporary meshed network **formed by a collection of mobile nodes**;
- a fully self-organized network;
- not rely on any established infrastructure for the network initialization and operation;
- initially envisioned mainly for crisis situation (e.g. battlefield or rescue situation) ...
- ... subsequently (due to low-cost devices 802.11) for civilian applications (e.g. VANET)
Other features:

- **Multi-Hop**: due to limited transmission range;
- **Distributed approach**: lack of infrastructure to support network operation;
- **Dynamic topography**: MANET entities are mobile nodes;
- **Nodes cooperation**: basic operations are performed by whole community;
- **Peer-to-Peer (P2P) analogies**: that is a community, composed by peer entities (mobile nodes), which share a common resource (network services).
Basic network operations

Basic network(-level) operations

Basic operations are carried out using a distributed approach:

- **Packet forwarding**: e.g. a source node S send packets to a destination node D through a path \(<S, A, B, D>\). Nodes A and B will perform p.f. function to deliver packets.

- **Routing**: e.g. a source node S receive aid from community to discover a route to node D.
Security analysis
Background

The differences between MANETs and infrastructured networks make useless whole known network concept.

Inadaptability of:

• known “classic” routing protocols for wired networks;
• security systems which offers authentication, confidentiality, integrity and non-repudation.

Then MANETs describes a new network paradigm: Ad Hoc Paradigm.
Features hide lacks

• **lack of physical and network layer security**: vulnerabilities such as traffic subversion/redirection, network partition, spoofing etc...;

• **lack of a-priori trust**: mobile nodes are not part of any shared organization. Classical security mechanisms based on preestablished trust are not applicable;

• **lack of infrastructure**: other operation such as *Key Servers* and *Trusted Third Parties* (TTP) are not compatible with *Ad Hoc Paradigm*;

• **requirement for cooperation**: due both to lack of dedicated components for network operations.
Routing protocols

Families protocols:

- **Proactive**: use messages to populate RTs;
- **Reactive** (o On-Demand): don't use RTs;
- **Hybrid**;
- ...;

Routing protocols assumes collaboration between nodes: **lacks of security mechanisms**.
Routing protocols

Reactive protocol embody ad hoc networks features.

- **Ad hoc On-demand Distance Vector** (AODV - RFC3561) take benefit of dynamic Routing Table (RT) and Bellman-Ford algorithm;

- **Dynamic Source Route** (DSR): fully On-Demand, don't use RT but it has a Route Cache and SendBuffer to store outgoing packets. Main procedures: **Route Discovery** and **Route Maintenance**.
Attacks

MANETs vulnerabilities and lacks give rise to attacks at the network layer of the ISO/OSI stack.

- **Active attacks**: that requires energetic cost;
- **Passive attacks**: are perpetrated by nodes that do not cooperate to save battery life.

Node behaviours identify attacks...
Attacks

Behaviour node models

- **Collaborative model**: a node that behave properly executing both p.f. and routing functions;
- **Selfish model**: a node that misbehave to save its battery life. This node could disable p.f. and/or routing functions;
- **Malicious model**: a node that aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.
Passive attacks

Selfish node models

- **Type 1**: node does not perform the p.f. function;
- **Type 2**: node does not perform the routing function (DSR or AODV);
- **Type 3**: the node behaviour follows an energy model:
  - when \( E_{\text{max}} =< E_{\text{curr}} < T_1 \) node behaves properly;
  - when \( T_1 =< E_{\text{curr}} < T_2 \) node behaves as if it was a selfish node of type 1;
  - when \( T_2 =< E_{\text{curr}} < 0 \) node behaves as a selfish node of type 2.
Passive attacks

**ns2 components**

- **SelfishMobileNode**: new Otcl class representing selfish mobile nodes of type 1 or 2;

- **DSRAgent**: modified to perform selfish misbehaviours;
Passive attacks

Performance metrics

- **Throughput**: def. \( T = \frac{r_a}{g_a} \)
- **Overhead**: def. \( O = \frac{d_a + s_n}{g_a} \)

\( r_a \): tot. # of received packets at application layer
\( g_a \): tot. # of generated packets at application layer
\( d_a \): tot. # of lost packets at application layer
\( s_n \): tot. # of sent packets at network layer
Passive attacks

Simulations in NS2

6 families of simulations depicted by:

- **Density**: low = 20 nodes, high = 60 nodes;
- **Mobility**: low = 2 m/s, high = 15 m/s
- **Selfishness**: type 1 or type 2

Parameters:

- nodes deployed over an 800 by 800 flat meter space;
- percentage $p$ of selfish nodes takes values from $p=0\%$ to $p=50\%$;
- random waypoint model;
- constant bit rate; packets size = 512bit; packet rate = 1 packet/s
- protocols: IEEE 802.11, IP, UDP and CBR
Passive attacks

Launcher and analyser

Launcher:
- gived the family, for each percentage $p$ build 40 different MANET models;
- 19Gb of trace files;
- produced about 5,400 different models of MANET.

Analyser:
- calculate $T$, $O$, $r_T$ and $r_O$ (radius of confidence interval at 95%)
- produce graphs.
Passive attacks

Results (1/3)

Throughput type 1:
• degrades by 60% when 50% of the modes mishbehave;
• node mobility and density have a negligible influence on the measurements.
Passive attacks

Observations (1/3)

\[ T = \frac{r_a}{g_a} \]

Linear regression from 0% to ~60%
Passive attacks

Results (2/3)

Throughput type 2:
- with low density degrades by ~40% when 50% of the nodes misbehaves;
- node density improve network throughput.
Passive attacks

Observations (2/3)

\[
T = \frac{r_a}{g_a}
\]

1) Linear regression from 0\% to ~40\% with low density and low mobility
2) Improve with high density and high mobility
Passive attacks

Results (3/3)

Overhead type 1 & 2:

- degrades slowly when $p$ increase
- nodes density and mobility increases # of packets inside the network
Passive attacks

Observations (3/3)

\[ O = \frac{d_a + s_n}{g_a} \]

- \( O < 2 \) => for each packet sent by CBRAgent there are at the worst 2 packets
- \( O > 1 \) => simulations reach the term while there are still packets in SendBuffer.
Active attacks

Smashing the MANET for fun and profit

Def: attack carried out in order to withhold the normal network operation by compromising the routing protocol.

Classification:

- Threats using modification: due to lack integrity checks;
- Threats using impersonation (a.k.a. spoofing attacks): due to lack of authentication at network/datalink layer;
- Threats using fabrication;
Active attacks

Redirection with modified sequence number

In AODV any node may divert traffic:

- S send a RREQ to its neighbours (A) for destination D
- A forward RREQ to X and B
- X unicast a false RREP to A containing an higher `dest_sequence_num` for D

Then X belong to shortest path from S to D
Active attacks

Denial of Service with modified source routes

In DSR states routes in data packet:
- suppose that D hear C, and B hear X
- S send data for destination D using source route <S, A, X, B, C, D>
- A forward packets to X
- X alter source route <S, A, X, B, C, D> in <S, A, X, B, D>
- B send a RRER (link broken) to source S
- X drop RRER
Active attacks

Forming loops by spoofing

In AODV may happen:

1. X learn the topology by listening;
2. X move closer to B and change its MAC address in S's ... 
3. ... X send RREP to B that contains a hop count to E less than the one sent by C
4. (3) X move closer to C and change its MAC address in B's ...
5. ... X send RREP to C that contains a hop count to D lower than the one sent by E

Then E is isolated.
Active attacks

Falsifying RRER messages in AODV and DSR

• Suppose node S has a route to D: <S, A, B, C, D>
• a malicious node X can launch DoS attack against D by sending RRER messages to A spoofing node B
Conclusions
Conclusions

Passive attacks:
• Necessary and sufficient condition is cooperation between nodes;
• The network performance severely degrade when a large percentage of node do not cooperate in p.f. function;
Then: need to enforce collaboration between nodes

Active attacks:
• Routing protocols do not care of security aspect;
Then:
• Need of securing routing protocol;
• Need of authentication mechanism to prevent spoofing attack;
• Need of integrity of routing messages;
MANETs:

- represent a challenging scenario for researchers;
- will play an important role in society and economy.

TODO:

- carry out studies upon impact of selfishness of type 3;
- recuring routing function;
- ...
The end

References:

- Giancarlo Pellegrino, relatore Prof. Ing. Salvatore Riccobene - “Analisi basata su simulazione delle prestazioni delle reti MANET in ns2” - Progetto finale;
- The Network Simulator, http://www.isi.edu/nsnam/ns
- P. Michiardi - “Mécanismes de sécurité et de coopération entre noeuds d'un réseaux mobile ad hoc” - Ph. D. thesis;