Analysis of the implicit trust within OLSR

Asmaa Adnane ¹, Rafael de Sousa ², Christophe Bidan ¹ and Ludovic Mé ¹

¹Supélec, équipe SSIR (EA 4039), ²University of Brasília - LabRedes

29 Mars 2007
Plan

1. Introduction
2. Implicit trust within OLSR
3. Applying trust to mitigate OLSR vulnerabilities
4. Conclusions/future works
5. Bibliography
Research on trust/trust management - Timeline

- (1993) R. Yahalom, B. Klein, and T. Beth. Formalism for explicit expressions of trust relationships
- (1994) S. Marsh. Basic definitions, computational trust model
- (2002) A. Jsang and R. Ismail/L. Mui. Computational models connecting reputation, trust and reciprocity
- Many other recent relevant works/authors
Notion of trust

- The fact that an entity A trusts an entity B in some respect means that
  - A believes that B will behave in a certain way and perform some action in certain specific circumstances
  - A actually believes that B has the potential to carry out the related tasks competently and honestly
- Different types/classes of trust depending on action/circumstance
- Direct and derived (by means of recommendations) trust relationships
Trust specification language [3]

- $A$ trusts $B$ with respect to (doing) the action $cc$
  
  $A$ trusts$_{cc}(B)$

- $A$ trusts the recommendations of entity $B$ about the capacity of other entities to perform action $cc$
  
  $A$ trusts$_{rec_{cc}}(B) when. path[S] when. target[R]$
Characteristics of the OLSR protocol

- **Proactive link-state routing protocol**, with a flooding mechanism to diffuse link state information
- **Multi-point relays (MPRs)** are selected nodes that forward messages during the flooding process
- **HELLO messages**
  - Sent periodically by a node to advertise its links
  - Allow a node to establish its view of the 2-hop neighborhood, then MPR selection
- **TC messages**
  - Convey the topological information necessary for computing routes
  - Periodically broadcast by MPRs advertising link state to symmetric neighbors
Mental state of each OLSR node

- **MANET**: the set of the whole MANET nodes
- **$LS_x$**: Link Set
- **$NS_x$**: Neighbor Set
- **2HNS$_x$**: 2-Hop Neighbor Set
- **$MPRS_x$**: MPR Set ($MPR_x \subseteq NS_x$)
- **$MPRSS_x$**: MPR Selection Set
- **$TS_x$**: Topology Set
- **$RT_x$**: Routing Table
Implicit trust construction within OLSR (1/2)

- OLSR reasoning is aimed at calculating the routing table, a behavior that implies thereafter the implicit use of trust relationships between nodes.
- The only criterion for this reasoning is the distance between the nodes.
- The information related to trust is obtained, but not used for the ensuring cooperations, nor to improve the operation of the protocol.
Implicit trust construction within OLSR (2/2)

Analysis steps

- Discovering the neighborhood
- MPR selection
- MPR Signaling
- Computing the routing table
A node (X) starts to build its view of the neighborhood with the reception of HELLO messages.

Received HELLO messages allow the node to detect asymmetrical links with each neighbor (Y).

Then, node X modifies its mental state about its trust in node Y:

\[ X \xleftarrow{HELLO} Y, \ X \notin LS_Y \implies X \neg \text{trusts} (Y) \]

So, node X now knows Y but does not trust it yet, because X is not sure that Y operates as specified by OLSR.
Discovering the neighborhood (2/3)

- Being an agent generally trustful [2], $X$ diffuse HELLO messages that can be received by $Y$
- If $Y$ acts according to the protocol, it sends back HELLO messages informing that it has a link with $X$
- Again, node $X$ changes its mental state to reflect a new situation of trust :

$$X^{HELLO} \leftrightarrow Y, \ X \in LS_Y \Rightarrow X \ trusts_{ID\cup NI}(Y)$$

- Now, node $X$ knows and trusts node $Y$
The trust relation is seen as symmetrical, since $Y$ is expected to behave in the same way as $X$:

\[
X \stackrel{HELLO}{\leftrightarrow} Y \Rightarrow X \text{ trusts}_{ID\cup NI}(Y)
\]

\[
Y \stackrel{HELLO}{\leftrightarrow} X \Rightarrow Y \text{ trusts}_{ID\cup NI}(X)
\]

- This symmetrical relation is the base for future decisions regarding MPR selection.
- Also, indirectly, this trust relation determines the calculation of the routing tables.
MPR Selection (1/2)

- The only criterion for MPR selection by a node $X$ is the number of symmetrical neighbors of a candidate node $Y$.
- The MPR selection imply that $X$ trusts only its neighbors selected as MPR for routing:

$$\forall \ Y \in MPRS_X : X \ \text{trusts}_{fw}(Y) \quad (1)$$

- Consequently, the nodes in $MPRS_X$ are required to recommend to $X$ the routes to the distant nodes:

$$\forall \ Z \in MANET : X \ \text{trusts}_{rec_{fw}}(Y) \ \text{when.path}[MPRS_Y] \ \text{when.target}[Z] \quad (2)$$
As the nodes $MPRS_Y$ themselves trust other MPRs, the route from $X$ to $Z$ is expressed by the predicate:

$$route_{Y_1 \rightarrow Y_n} = Y_1, ..., Y_n \text{ with } Y_{i+1} \in MPRS_{Y_i}$$

This allows the expression of the general rule of trust recursivity for the routing within OLSR:

$$\forall Z \in MANET : \quad X \text{ trusts} . rec_{fw}(Y) \quad \text{when} . path[route_{Y \rightarrow Z}] \quad \text{when} . target[Z] \quad (3)$$
MPR Signaling

- The calculation of $MPRSS_X$ allows a node $X$ to discover information about the trust that other nodes place on itself.
- Node $X$ allows the nodes of its $MPRSS$ to use its resources for routing (access trust)

$$X \text{ trusts}_{at} (Y)$$

- Node $X$ trusts $Y$ for advertising (delegation trust) that $X$ is a MPR

$$X \text{ trusts}_{dt} (Y)$$
Computing the routing table (1/2)

- Each node $X$ selects the shortest path to reach any other node $Z$ passing through a selected MPR $Y$
- This calculation will allow $X$ to trust $Y$ for the routing towards $Z$

$$T = (Z, Y, N, I)$$ is a tuple of $RT_X$

$$\forall T \in RT_X \Rightarrow X \text{ trusts}_{fw-Z}(Y)$$
Computing the routing table (2/2)

- The selection of $Y$ as MPR by $X$ for routing towards a node $Z$ implies that $X$, not only trusts $Y$ for routing (1), but also trusts the choices of the routes made by $Y$ (3).
- Actually, there is a chain of this indirect trust relation between $X$ and any relay forwarding the packets to $Z$.
- This sequence expresses the transivity of MPR recommendations in OLSR:

$$X \; trusts.rec_{fw-Z}^* (Z) \; when.target[Z] \; when.path[Z] \; (4)$$
Implicit trust within OLSR

- The routing table is calculated so that there is only one route towards each destination, and each selected route is the shortest among the routes starting from MPR nodes.
- After computing the distances to destinations, the node will place more trust in those nodes which offer the shortest paths towards the destinations (4).
- The inherent risk in the choice of only one route towards any destination is to choose, as router, a corrupted or misbehaving node.
Fabrication of HELLO message

A- Steps of attack

1: HELLO_B, LS_B = {A, C, att}
2: HELLO_A, LS_A = {B, att},
3: HELLO_att, LS_att = {A, B, C, x}
Consequences of the attack

- The attacker acquires the trust of A and B which will choose it as MPR for routing towards any node Z, without having a proof of the existence of a path between the attacker and Z

\[ A \text{ trusts}_{fw}(att) \quad \text{and} \quad B \text{ trusts}_{fw}(att) \]

- So, A will select the attacker to route towards C:

\[ A \text{ trusts}_{rec}(att) \quad \text{when} \cdot \text{path}[\text{route}_{att \rightarrow C}] \quad \text{when} \cdot \text{target}[C] \]

- As \( route_{attacker \rightarrow C} \) is not the shortest path, the nodes A and B should mistrust the information provided in the HELLO message
Trust-based detection of the attack (1/2)

- After the attack, B is still a MPR of C and will broadcast TC messages advertising C as symmetric neighbor.
- Trust-based reasoning from the point of view of A will lead to contradictory conclusions:
  - By receiving a TC message from B, A will deduce:
    \[ A \xleftarrow{TC} B, \quad NS_B = \{A, \text{att}, C\} \Rightarrow \exists Z \in NS_B : B \in MPRS_Z \]
  - After receiving a TC message from the attacker, A will also deduce:
    \[ A \xleftarrow{TC} \text{att}, \quad NS_{att} = \{A, B, C, X\} \Rightarrow \exists Z \in NS_{att} : \text{att} \in MPRS_Z \]
Trust-based detection of the attack (2/2)

- To discover the node which selected B as MPR, A reasons by elimination on the set $NS_B$
  - $B \notin MPRS_A$ and $[NS_B - \{att\}] \subset [NS_{att} - \{B\}]$
  - So, it was not the attacker which selected B as MPR, but C:
    \[ B \in MPRS_C \Rightarrow C \text{ trusts}_{fw-A}(B) \] (5)

- Moreover, as the neighborhood of B is a subset of the attacker’s, C should use att as MPR for routing towards A:
  \[ att \in MPRS_C \Rightarrow C \text{ trusts}_{fw-A}(att) \] (6)

- So, there is **contradiction between 5 and 6**, because OLSR specifies that a node should use only one route to a destination
Conclusions and future works

Conclusions

- OLSR generates information about trust between nodes
  - nodes firstly cooperate and gather trust related information, without any validation
  - nodes implicitly deduce information about the other nodes in which they have to trust
- Trust can be an additional criterion for MPR selection and routing table calculation
- Mistrust-based control can be set up to detect suspect behavior
Future works

- Simulation of trust-reasoning OLSR nodes
- Evaluation of possible trust metrics for OLSR
- Extension of OLSR using trust rules for MPR selection and routing table calculation
- Distributed trust management module for OLSR


Analysis of the implicit trust within OLSR

Questions and remarks?