Intégration du raisonnement sur la confiance pour la sécurité de OLSR

Asmaa Adnane ¹, Christophe Bidan ¹ and Ludovic Mé¹, Rafael de Sousa ²

¹Supélec, SSIR team (EA 4039)
²University of Brasília - LabRedes, supported by CNPq - Brazil

14th October 2008

A. Adnane, C. Bidan, L. Mé, R. de Sousa
Intégration du raisonnement sur la confiance pour la sécurité de OLSR
Plan

1. Introduction
2. Trust-Based Reasoning for OLSR
3. Simulation and results - Example
4. Conclusions and future works
Introduction

- Ad hoc route discovery and maintenance introduce specific security problems for routing protocols to prevent, detect or respond.
- Solutions to secure these routing protocols using some centralized units or trusted third-parties actually constrain the self-organization of ad hoc networks.
- For OLSR, we propose the integration of trust reasonings into each node behavior, so as to allow a self-organized trust-based control to help nodes to detect misbehavior attacks.
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 [2]

- $A$ trusts $B$ with respect to (doing) the action $cc$:

  $$A \ operatorname{trusts}_{cc}(B)$$

- $A$ trusts the recommendations of entity $B$ about the capacity of other entities to perform action $cc$:

  $$A \ operatorname{trusts}.\ operatorname{rec}_{cc}(B) \ where.\ operatorname{path}[S] \ when.\ operatorname{target}[R]$$
Characteristics of the OLSR protocol (1/2)

Flooding routing

OLSR routing

retransmitting nodes
Characteristics of the OLSR protocol (2/2)

- 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.
Notations

- $\text{MANET}$: the set of the whole MANET nodes.
- $\text{LS}_x$: Link Set.
- $\text{NS}_x$: Neighbor Set.
- $2\text{HNS}_x$: 2-Hop Neighbor Set.
- $\text{MPRS}_x$: MPR Set ($\text{MPR}_x \subseteq \text{NS}_x$).
- $\text{MPRSS}_x$: MPR Selection Set.
Validation process

- Validation of basic belief.
- Validation of MPR selection:
  - Validation of local view.
  - Validation of neighbors view.
In [3] authors present intrinsic properties of the protocol regarding the expected correct behavior in message processing and routing organization.

\[ (TC_Y)_Z \subseteq HELLO_Y \]

\[ X \in TC_Y \Rightarrow Y \in MPRS_X \]

\[ TC_Y = (TC_Y)_Z \]
Validation of basic belief (2/2)

In term of trust:

- HELLO and TC message of any neighbor must be consistent:
  \[ X \xleftarrow{HELLO_Y} Y, \ X \xleftarrow{TC_Y} Y, \ TC_Y \not\subseteq NS_Y \implies X \neg\text{trusts}(Y) \]

- Received TC must be consistent with local MPR selection:
  \[ X \xleftarrow{TC_Y} *, \ X \in TC_Y, \ Y \notin MPRS_X \implies X \neg\text{trusts}(Y) \]

- TC messages can not be modified before forwarding:
  \[ X \xleftarrow{TC_Y} Y, \ \exists m \in MPRS_Y, \ TC_Y \neq (TC_Y)_m \implies X \neg\text{trusts}(Y, m) \]
Validation of MPR selection

MPR Selection is a critical operation as it provides each node the access to the network. In our approach, after the MPR Selection each node should verify the two following points:

1. the nodes selected as MPR must behave correctly regarding the operations of broadcasting TC messages and forwarding TC messages and data packets originated by MPR selectors;
2. the local choices of MPRs by a node must be in accordance to global topology information received by this node.
Validation of the local view

- Consistency of the symmetric link:

\[ X \xrightarrow{HELLO_Y} Y, X \xleftarrow{HELLO_Z} Z, Z \in NS_Y \Rightarrow Y \in NS_Z \]

In term of trust:

Figure: False link advertised by Y or Z

\[ X \xrightarrow{HELLO_Y} Y, X \xleftarrow{HELLO_Z} Z, (Z \in NS_Y, Y \notin NS_Z) \]

or

\[ (Y \in NS_Z, Z \notin NS_Y) \Rightarrow X \neg \text{trusts}(Y, Z) \]
Supervising MPR behavior

MPR selection leads to the following expression:

\[ \forall Y \in MPRS_X : X \.trusts_{fw}(Y) \]

this trust relation is broken in the following situation:

- Checking TC message generation:
  \[ Y \in MPRS_X, (X \overset{TC}{\leftrightarrow} Y) \text{ or } (X \overset{TC}{\leftarrow} Y, X \not\in TC_Y) \Rightarrow X \neg\text{trusts}(Y) \]

- Checking data packet and TC message forwarding:
  \[ Y \in MPRS_X, (X \overset{TC}{\rightarrow} *, X \overset{TC}{\leftarrow} Y) \text{ or } (X \overset{DATA}{\rightarrow} *, X \overset{DATA}{\leftarrow} Y) \Rightarrow X \neg\text{trusts}(Y) \]
Validation of neighbor view (1/4)

If $A, B \in NS_X$ and $NS_A = NS_B$, then a common neighbor of $A$ and $B$ must not select both of them as MPRs:

$$NS_A = NS_B \Rightarrow MPRSS_A \cap MPRSS_B = \emptyset$$
Validation of neighbor view (2/4)

If $A, B \in NS_X$ and $NS_B \subset NS_A$, then $B$ should not be selected as MPR, all its neighbors will select $A$ as MPR, so $B$ should not generate a TC message:

$$NS_B \subset NS_A \Rightarrow MPRSS_B = \emptyset$$
Validation of neighbor view (3/4)

- If 2 neighbors, \(X\) and \(Y\), have the same neighbors (NS), they should also select the same MPRs:

\[
NS_X - \{Y\} = NS_Y - \{X\} \Rightarrow MPRS_X = MPRS_Y \text{ or } \\
\forall Z \in MPRS_X, \exists W \in MPRS_Y : NS_Z = NS_W
\]
In term of trust:

\[ X \overset{HELLO}{\leftrightarrow} A, X \overset{HELLO}{\leftrightarrow} B, NS_A \subseteq NS_B, \exists Z \in TC_A \cap TC_B \Rightarrow X \neg \text{trusts}(A, B, Z) \]
Implementation

- GlomoSim Simulator and the OLSR patch developed by the Niigata University.

- Several attack scenario:
  1. Attack 1: the attacker advertises wrong links information to be selected as the only MPR by target nodes in order to control its messages.
  2. Attack 2: The attacker does not advertise that it has been selected as MPR by another nodes.
  3. Attack 3: The attacker selected as MPR will not broadcast packets of target nodes.

- In the following, we discuss only results with 100 nodes using the first attack scenario.
Detection rate regarding only the concerned nodes by the attack
Figure: Network example: A is the attacker, T is the Target
Scenario of the attack (1/2)
Scenario of the attack (2/2)
Detection of the attack (1/5): Set of concerned nodes
Detection of the attack (2/5): The target

Inconsistencies between \((HELLO_A, HELLO_{N7}, HELLO_{N8}), (TC_A, HELLO_{N7}, HELLO_{N8})\) and \((NS_A, NS_{N2}, NS_{N20})\):
Detection of the attack(3/5): The faulty links

Inconsistencies between $HELLO_A$, $TC_A$ and $(NS_X, X \in \{7, 8, 9, 21, 22\})$: 

A. Adnane, C. Bidan, L. Mé, R. de Sousa
Intégration du raisonnement sur la confiance pour la sécurité de OLSR
Detection of the attack (4/5): The neighbors of faulty links

Inconsistencies between \((\text{TC}_A, \text{NS}_7, \text{NS}_8, \text{NS}_9)\) and \((\text{TC}_A, \text{NS}_{21}, \text{NS}_{22})\):
Detection of the attack (5/5): common neighbors

Inconsistencies between \((NS_A, NS_{N2}, NS_{N20})\):

[Diagram showing network with nodes and edges indicating inconsistencies]
Conclusions and future works

Conclusions

- Identification of trust-related properties.
- Each node is enabled to mistrust misbehaving nodes by correlation of received messages and deductions using the trust rules.
- MPR selection can be validated by exploiting trust properties and relations.
- The simulation using attack scenarios shows the effectiveness of using mistrust to detect some known attacks against OLSR.
Past (Future works) :-) !

- Trust-based reasoning in OLSR nodes can also be useful for routing table validation,
- Trust management module for OLSR without modifying the protocol.
- Measure the impact of trust-based reasoning on the protocol, not only to detect attacks, but to react and take measures to counter them, while preserving the auto-organization of the ad hoc environment.
Bibliography


This is the end ...

Intégration du raisonnement sur la confiance pour la sécurité de OLSR

Questions and remarks ?