The Maude-NPA GUI:

Installation and user manual

January 2012

Sonia Santiago

Carolyn L. Talcott

Santiago Escobar

Catherine Meadows

José Meseguer

INDEX

1. INTRODUCTION

This document describes the prototype version of the Graphical User Interface (GUI) of the Maude-NRL Protocol Analyzer (Maude-NPA) and gives instructions for its installation and use.

The aim of this graphical user interface is to give the user a complete animation of the Maude-NPA search tree generation process which she can control at will.

This document is organized as follows. In Section 2 we provide the instructions to install the Maude-NPA GUI package. Section 3 describes all the features of the Maude-NPA GUI, explaining step by step how the GUI can be used. Finally, in Section 4 you will find some further information and useful links.

Throughout this manual, we assume a minimum acquaintance with the Maude-NPA tool. The Maude-NPA GUI uses Maude-NPA version 2.0. We refer the user to the Maude-NPA manual that is available online at http://maude.cs.uiuc.edu/tools/Maude-NPA

2. INSTALLATION

The Maude-NPA requires the Graphviz library to be installed on your computer. We have succesfully tested the Maude-NPA GUI on Graphviz versions 2.20.2 and 2.24.0. For Mac OS X 10.5 or Mac OS X 10.6, please, download and install the Graphviz library from the following web site:

www.graphviz.org/Download.php

Note that there is no binary installation package for Mac OS X 10.4. Instead, you should download the source files from the following link:

www.graphviz.org/Download_source.php

and build the library manually.

The current version of the Maude-NPA GUI works on Mac OS X 10.4, Mac OS X 10.5 and Mac OS X 10.6, and is available online at:

www.dsic.upv.es/grupos/elp/Maude-NPA_GUI

For installation, just unpack the package at the desired directory. The Maude-NPA tool is already included into this package.

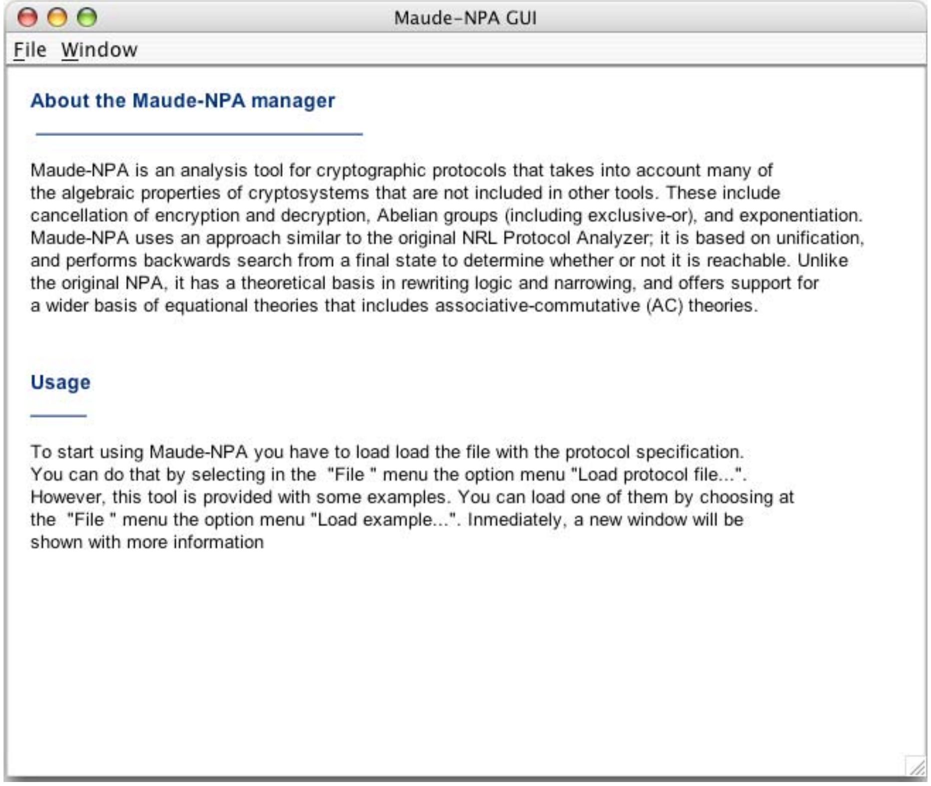
3. USER MANUAL

3.1. How to launch the tool

In order to start using the Maude-NPA GUI you have to enter into the directory where you installed the Maude-NPA GUI. In this directory there is an executable file called *start* which sets some necessary environment variables and launches the tool. To execute this file just double click on it or type in the following command line:

```
./start
```

After doing this, the window shown in Figure 1 will appear:



About the Maude-NPA manager

Maude-NPA is an analysis tool for cryptographic protocols that takes into account many of the algebraic properties of cryptosystems that are not included in other tools. These include cancellation of encryption and decryption, Abelian groups (including exclusive-or), and exponentiation. Maude-NPA uses an approach similar to the original NRL Protocol Analyzer; it is based on unification, and performs backwards search from a final state to determine whether or not it is reachable. Unlike the original NPA, it has a theoretical basis in rewriting logic and narrowing, and offers support for a wider basis of equational theories that includes associative-commutative (AC) theories.

Usage

To start using Maude-NPA you have to load load the file with the protocol specification. You can do that by selecting in the "File " menu the option menu "Load protocol file...". However, this tool is provided with some examples. You can load one of them by choosing at the "File " menu the option menu "Load example...". Inmediately, a new window will be shown with more information

Figure 1 . Main window of the Maude-NPA GUI

This window contains some information about the Maude-NPA tool and some basic instructions to start using this GUI.

3.2. How to load a protocol

The next step the user may want to do is loading a protocol specification to start its analysis. The Maude-NPA GUI allows the user to load his or her own protocol specification from his or her file system but it also provides some predefined protocol specifications. We recommend the user to start using one of these example protocols to become familiar with the Maude-NPA GUI.

For both, loading her protocol or a predefined protocol, click on on the "*File*" menu option and select *"Load protocol specification…"* or "*Load predefined protocol…"*, as Figure 2 shows.

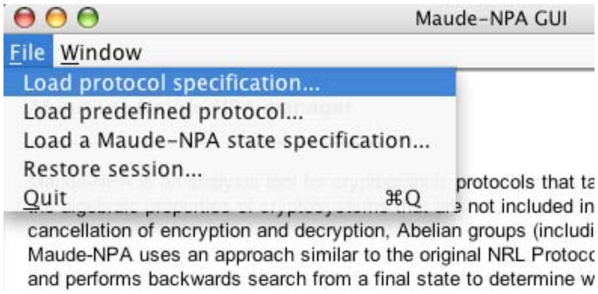
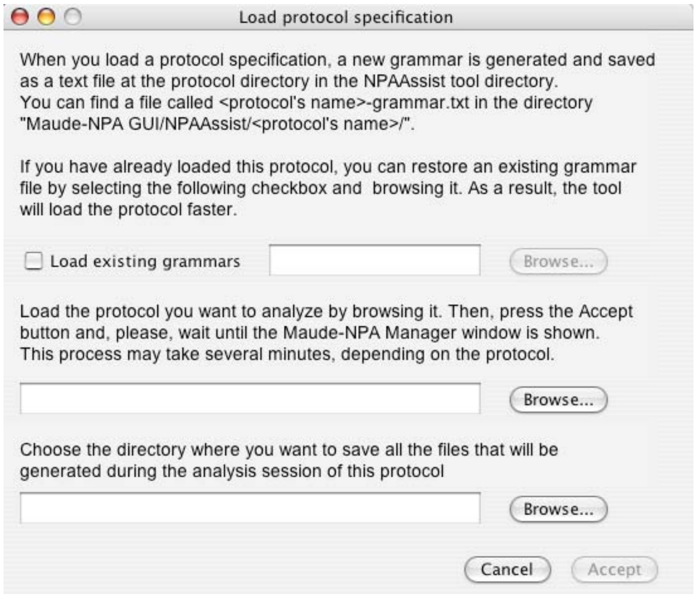

Maude-NPA GUI
File
Window
Load protocol specification...
Load predefined protocol...
Load a Maude-NPA state specification...
Restore session...
Quit
⌘Q
protocols that ta
not included in
cancellation of encryption and decryption, Abelian groups (includi
Maude-NPA uses an approach similar to the original NRL Protocc
and performs backwards search from a final state to determine w

Figure 2: Menu option to load a protocol specification

Both options are explained in more detail in Sections 3.2.1 and 3.2.2 below.

3.2.1. How to load a protocol file from the user file system

When the user chooses to load a protocol specification file from her system, a new window (see Figure 3), is shown:



When you load a protocol specification, a new grammar is generated and saved as a text file at the protocol directory in the NPAAssist tool directory.
You can find a file called <protocol's name>-grammar.txt in the directory "Maude-NPA GUI/NPAAssist/<protocol's name>/".

If you have already loaded this protocol, you can restore an existing grammar file by selecting the following checkbox and browsing it. As a result, the tool will load the protocol faster.

□ Load existing grammars

Load the protocol you want to analyze by browsing it. Then, press the Accept button and, please, wait until the Maude-NPA Manager window is shown.
This process may take several minutes, depending on the protocol.

Choose the directory where you want to save all the files that will be generated during the analysis session of this protocol

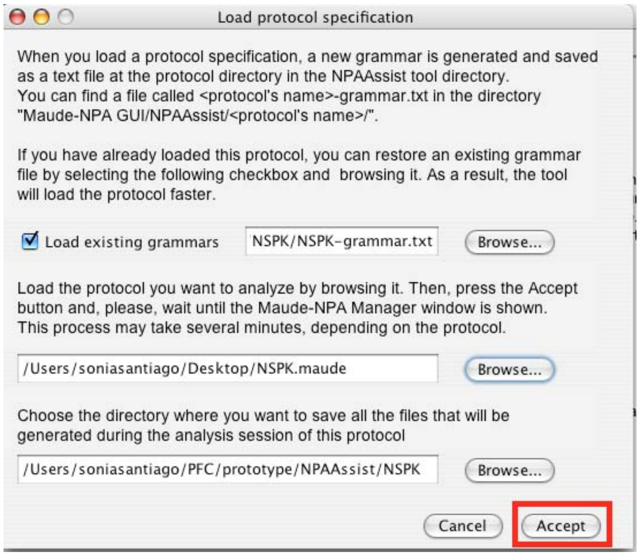
Figure 3: Window to load a file with a protocol specification

For each protocol, Maude-NPA generates a set of auxiliary data structures called "grammars". Since their generation can take from a few seconds to several minutes, the user can save the grammars and load them later without generating them again. The option *"Load existing grammar"* and its associated *"Browse"* button allow that. The file containing the grammars is stored at a folder associated to the current protocol (see below) using the file name *"<protocol name>-grammars.txt".* Note that a new grammar file must be generated after any modification of the protocol specification.

The next step is selecting the protocol file from the user's file system. This can be done by clicking on the second *"Browse…"* button.

The user can change the folder for temporal files associated to the current protocol. This folder is set by default to a folder with the protocol name and it is located at the NPAAssist directory of the Maude-NPA GUI installation.

Once the user has selected the file, the grammars and the temporal folder, she can press the *"Accept"* button (see Figure 4). If the tool has to generate the grammars associated to the protocol, a message will be shown to the user. After generation, a new window (see Section 3.3) is shown up.



Load protocol specification

When you load a protocol specification, a new grammar is generated and saved as a text file at the protocol directory in the NPAAssist tool directory.
You can find a file called <protocol's name>-grammar.txt in the directory "Maude-NPA GUI/NPAAssist/<protocol's name>/".

If you have already loaded this protocol, you can restore an existing grammar file by selecting the following checkbox and browsing it. As a result, the tool will load the protocol faster.

☑ Load existing grammars NSPK/NSPK-grammar.txt

Load the protocol you want to analyze by browsing it. Then, press the Accept button and, please, wait until the Maude-NPA Manager window is shown. This process may take several minutes, depending on the protocol.

/Users/soniasantiago/Desktop/NSPK.maude

Choose the directory where you want to save all the files that will be generated during the analysis session of this protocol

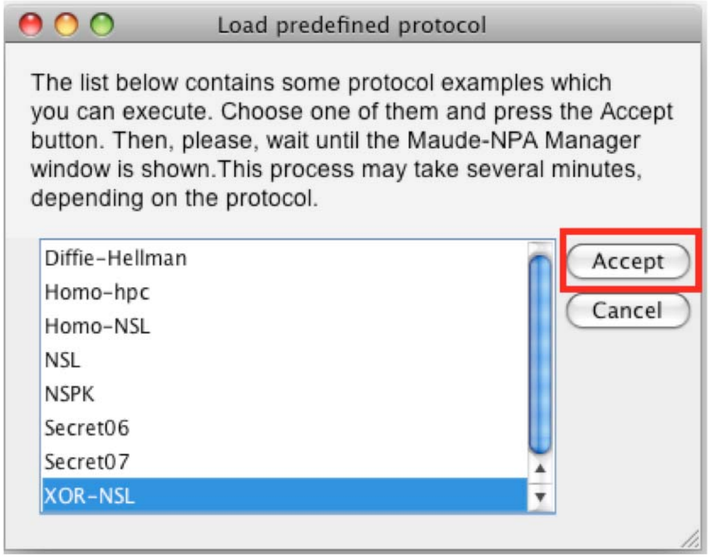
/Users/soniasantiago/PFC/prototype/NPAAssist/NSPK

Figure 4: An example of how to load a protocol specification

3.2.2. How to load a predefined example protocol

When the user decides to load a predefined protocol specification and selects the "*Load predefined protocol…"* submenu option, a new window (see Figure 5) is displayed. This window contains a list of the predefined protocols. The user has to select one of these list elements.

Finally, the user has to press the *"Accept"* button and wait a few seconds until a new window (see Section 3.3) is opened.



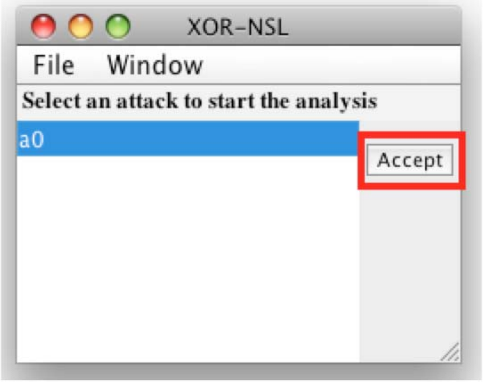
The list below contains some protocol examples which you can execute. Choose one of them and press the Accept button. Then, please, wait until the Maude-NPA Manager window is shown.This process may take several minutes, depending on the protocol.

- Diffie-Hellman
- Homo-hpc
- Homo-NSL
- NSL
- NSPK
- Secret06
- Secret07
- XOR-NSL

Figure 5: Window to load a predefined protocol

3.3. How to select an attack and generate the protocol search tree

In a protocol specification, more than one attack state can be described. After loading a protocol, the user has to choose the concrete attack state she wants to analyse. In the Maude-NPA GUI this is done in a window entitled with the protocol's name, as Figure 6 shows.

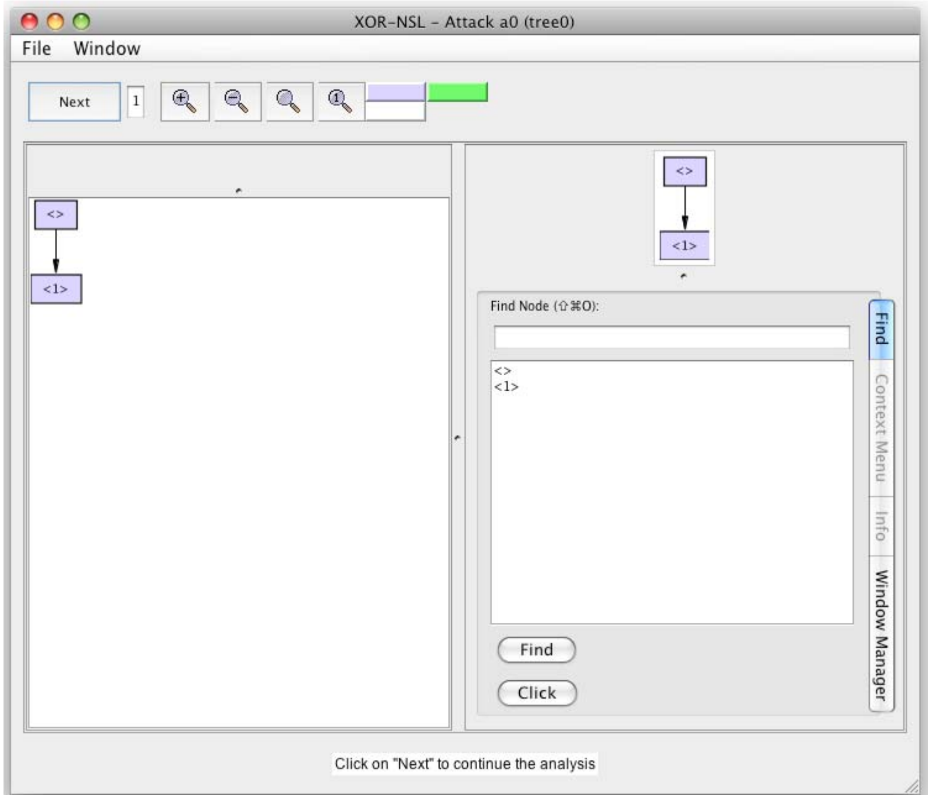


Select an attack to start the analysis

a0

Figure 6: Window to select a concrete attack

The user has to select the concrete attack and press the *"Accept"* button. The protocol's attacks are collected from the Maude-NPA specification file: we refer the reader to the Maude-NPA manual for details. A few seconds later, a new window, shown in Figure 7, is opened. This window displays graphically the first two levels of the search space generated by Maude-NPA.



Click on "Next" to continue the analysis

Figure 7: Window that shows the initial search space

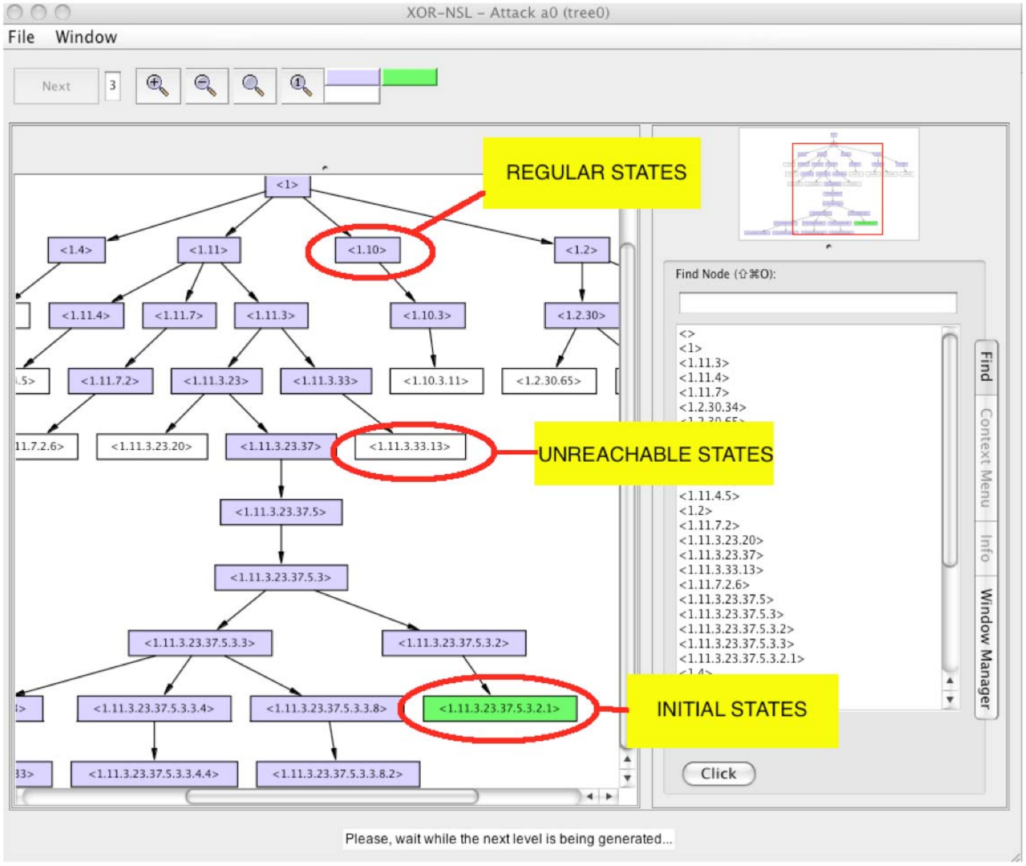
3.4. Graphical representation of a protocol search tree

This section gives a brief explanation about the window that displays the search tree and the features it provides.

At the left side of the window there is a big frame which will display the search tree, i.e. the graphical representation with the shape of a tree of the search space generated by the Maude-NPA during its analysis of the protocol. Each node of the tree represents a state generated during the backwards search. The state background color is lavender if it is a regular state and green if it is an initial state, i.e., a solution state. If a state has no children (predecessor states), its corresponding node at the search tree is painted in white color. Figure 8 shows the search space for the XOR-NSL protocol when an initial state is found.

On the top of this window there is a tool bar with a button called "*Next*" which will allow the user to generate one or more levels of the tree (see

Section 3.4.1 for further information) and some buttons to zoom in on the tree image. There is also a color key which explains the meaning of each background color of the search tree.



Please, wait while the next level is being generated...

Figure 8: Search tree representation of the NSPK protocol analysis

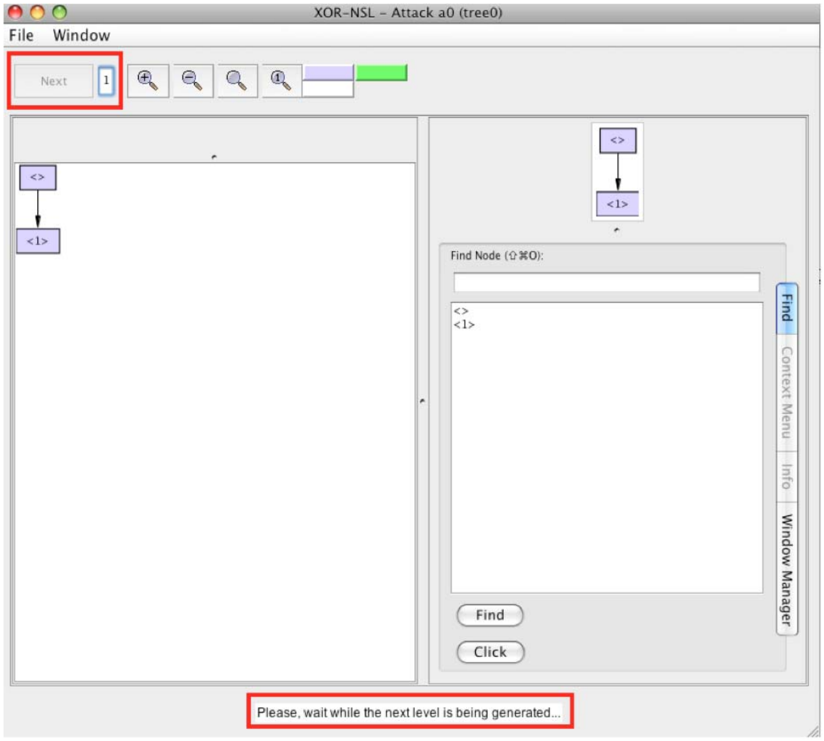
There is a thumbnail picture placed at the top right corner of the frame which shows the entire search space tree. The user can navigate through it to focus in one part of the tree.

At the bottom of the right part of the window there is an area with a list of all the tree states and some buttons which will allow the user to find a specific state at the tree (see Section 3.4.2 for further information). There is also a tab on this area called *"Window Manager",* in which all the windows related to a Maude-NPA GUI session will be listed (see Section 3.4.4 for more detailed information).

3.4.1. How to generate one or more search tree levels

Initially, the protocol search tree is displayed with the first two node levels. In the first level there is only one node, called the *"root node",* which is a dummy node. Indeed, the root node does not correspond to any Maude-NPA state. The second level of the search tree contains the attack states that we are going to use for the backwards analysis of the protocol.

The user can generate more one level by clicking on the *“Next”* button (see Figure 9). After clicking it, the message *“Please, wait while the next level is being generated”* appears at the message area in the bottom part of the window.



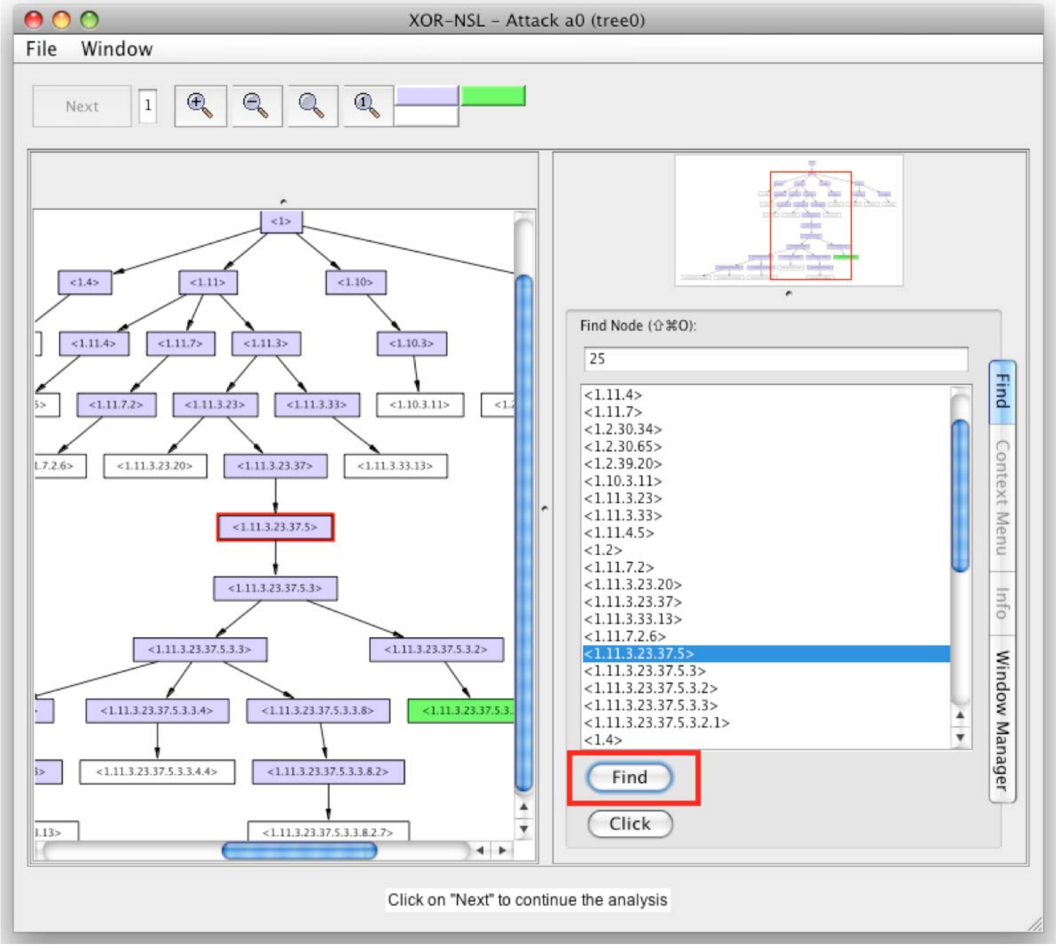
Please, wait while the next level is being generated...

Figure 9: How to generate one more level of the search space tree

Moreover, the user can generate more than one level by typing the desired number of backwards analysis steps at the text box place besides the *“Next”* button. When an initial state is found or the analysis has finished, a pop-up window will be showed, telling so to the user. In both cases, the user should only press the *“Accept”* button to close the pop-up window. If the analysis has finished the text of the message area is also updated, reporting to the user about that fact.

3.4.2. How to find any specific state in the search tree

At the right bottom corner of the window there is a list of the state labels. The user can find any specific state in the tree by doing double-click on any of the list elements or by selecting one of them and then pressing the *"Find"* button placed below the list, as Figure 10 shows. The selected state will appear highlighted in red color and the picture of the search tree will be centered on this state, if necessary.



Find Node (⇧⌘O): 25

<1.11.4>
<1.11.7>
<1.2.30.34>
<1.2.30.65>
<1.2.39.20>
<1.10.3.11>
<1.11.3.23>
<1.11.3.33>
<1.11.4.5>
<1.2>
<1.11.7.2>
<1.11.3.23.20>
<1.11.3.23.37>
<1.11.3.33.13>
<1.11.7.2.6>
<1.11.3.23.37.5>
<1.11.3.23.37.5.3>
<1.11.3.23.37.5.3.2>
<1.11.3.23.37.5.3.3>
<1.11.3.23.37.5.3.2.1>
<1.4>

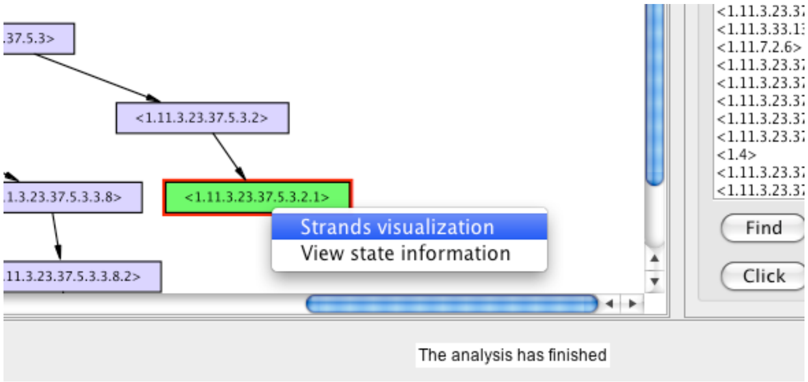
Click on "Next" to continue the analysis

Figure 10: How to find any specific state of the search tree

3.4.3. View state information

For each state, Maude-NPA provides the following blocks of information: (i) the current strands, (ii) the intruder knowledge, (iii) the sequence of messages, and (iv) some additional data. There is a contextual menu associated to each node of the search tree, which is activated with a right-click, as shown in Figure 11. This contextual menu allows the user to consult any of the four blocks of information or to obtain a graphical representation of the strands and the intruder knowledge information given by Maude-NPA. Let us explain both visualization capabilities.

Graphical Visualization. If the user selects the *“Strands visualization”* option of the contextual menu, a new window will appear, showing the graphical representation of a Maude-NPA state. For the graphical display of state strands we followed the original graphical representation of strands shapes, but modified to represent the Maude-NPA specific features, such as the notion of time. Figure 12 shows the graphical representation of a Maude-NPA state.



The analysis has finished

Figure 11: Contextual menu associated to a tree’s state

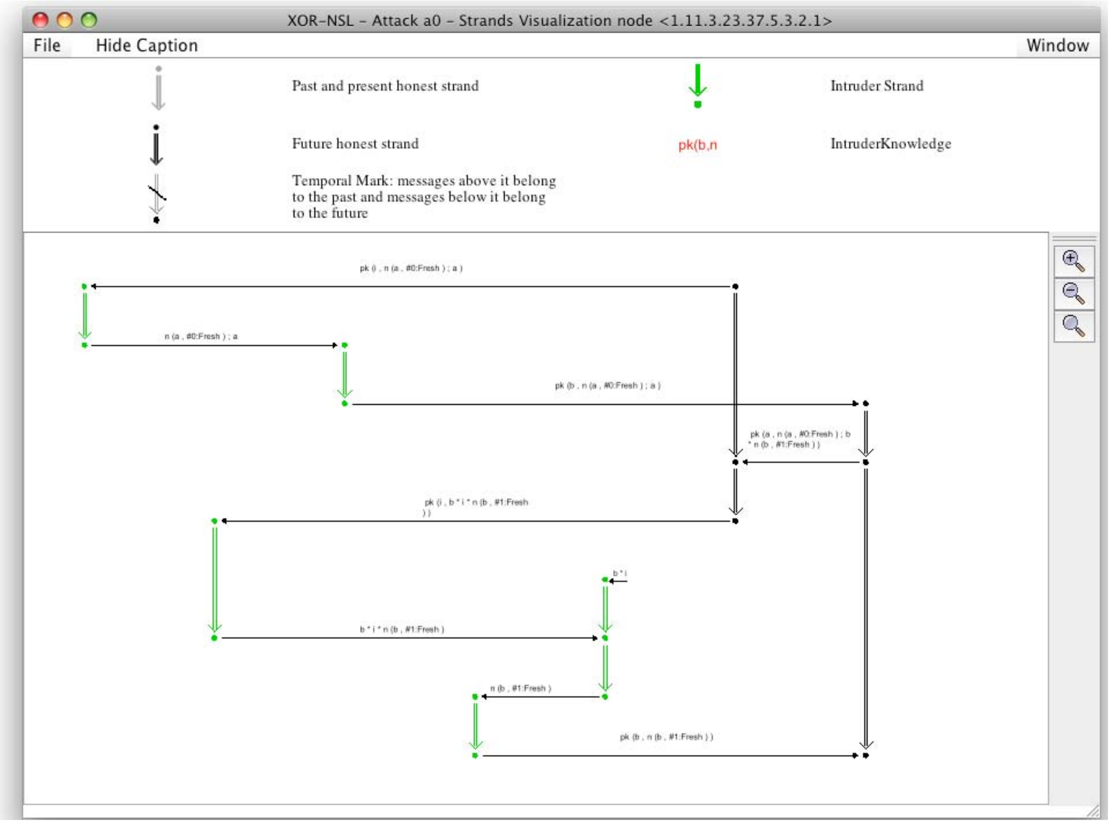

XOR-NSL - Attack a0 - Strands Visualization node <1.11.3.23.37.5.3.2.1>
File
Hide Caption
Window
Past and present honest strand
Intruder Strand
Future honest strand
pk(b,n
IntruderKnowledge
Temporal Mark: messages above it belong to the past and messages below it belong to the future
pk (i , n (a , #0:Fresh) ; a)
n (a , #0:Fresh) ; a
pk (b , n (a , #0:Fresh) ; a)
pk (a , n (a , #0:Fresh) ; b * n (b , #1:Fresh))
pk (i , b * i * n (b , #1:Fresh))
b * i
b * i * n (b , #1:Fresh)
n (b , #1:Fresh)
pk (b , n (b , #1:Fresh))

Figure 12: Graphical representation of a Maude-NPA state

For the graphical representation of a state, a strand is drawn as a vertical sequence of dots connected between them by a double vertical line. Each dot corresponds to an input or output message in the strand and is also called a node. In the Maude-NPA both, intruder and honest principals behaviors, are represented with strands and, thus, shown in the graphical representation. To differentiate between an intruder and an honest strand, we use *grey* and *black* for honest strands and green for intruder strands. The aim of having two colors for honest strands is to represent the notion of time: grey color for the past and present, and black color for the future. The vertical bar used in Maude-NPA for denoting the time position is here represented by a slanting line.

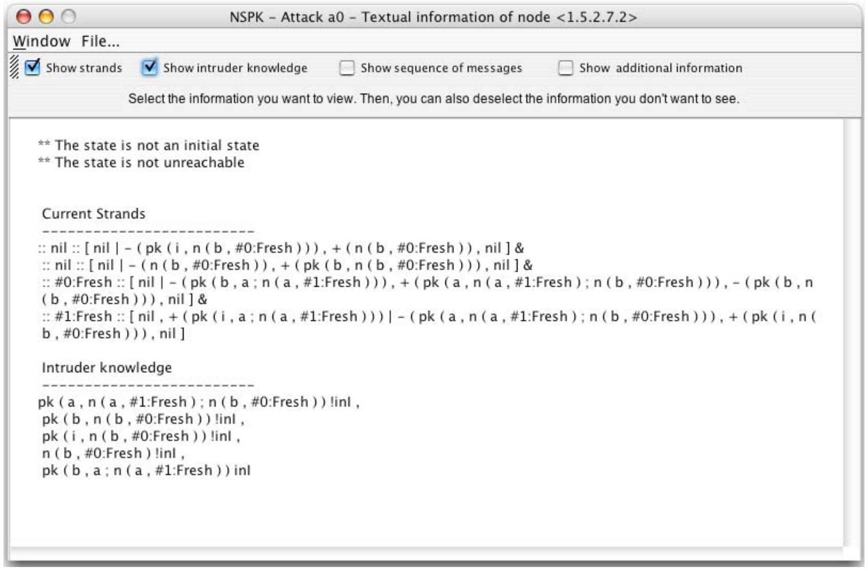
The intruder knowledge is integrated into the graphical representation by using different colors for the messages attached to each node. We use *red* if the message is known by the intruder and *black* if the message is not known. For messages that do not yet belong to a concrete strand, we use a single dot instead of a vertical sequence of dots.

The menu option *"File -> Save picture",* available in the left part of the menu bar, allows the user to save the picture of the state as an image file. Once the user clicks on this menu option, she is requested to choose the location where she wants to save the image.

Textual Visualization. When the user chooses the *“View state information”* option of the contextual menu, a new window, shown in Figure 13, is opened too. In the top side of this window there is a set of “checkbox” elements. Each one of these “checkbox” elements is associated to each type of specific information that Maude-NPA obtains for each state, i.e. there is a “checkbox” associated to the current strands information, another one that corresponds to the intruder knowledge, and so on. The Maude-NPA tool will always show, before this information, two lines of text, indicating whether the state is an initial state or not, and whether it has been proved unreachable by the Maude-NPA or not.

The user can choose the concrete information that she wants to see by selecting the corresponding “checkbox” elements. This information will be represented in a textual way. If the user does not yet want to see any concrete information that is currently being displayed, she should just unselect the concrete “checkbox”.

The menu option *“File -> Save…”,* available in the left part of the menu bar, allows the user to save the selected information of the state in a text file. Once the user clicks on this menu option, she is requested to choose the location where she wants to create the text file with the selected information of the state.


NSPK – Attack a0 – Textual information of node <1.5.2.7.2>
Window File...
☑ Show strands
☑ Show intruder knowledge
□ Show sequence of messages
□ Show additional information

Select the information you want to view. Then, you can also deselect the information you don't want to see.

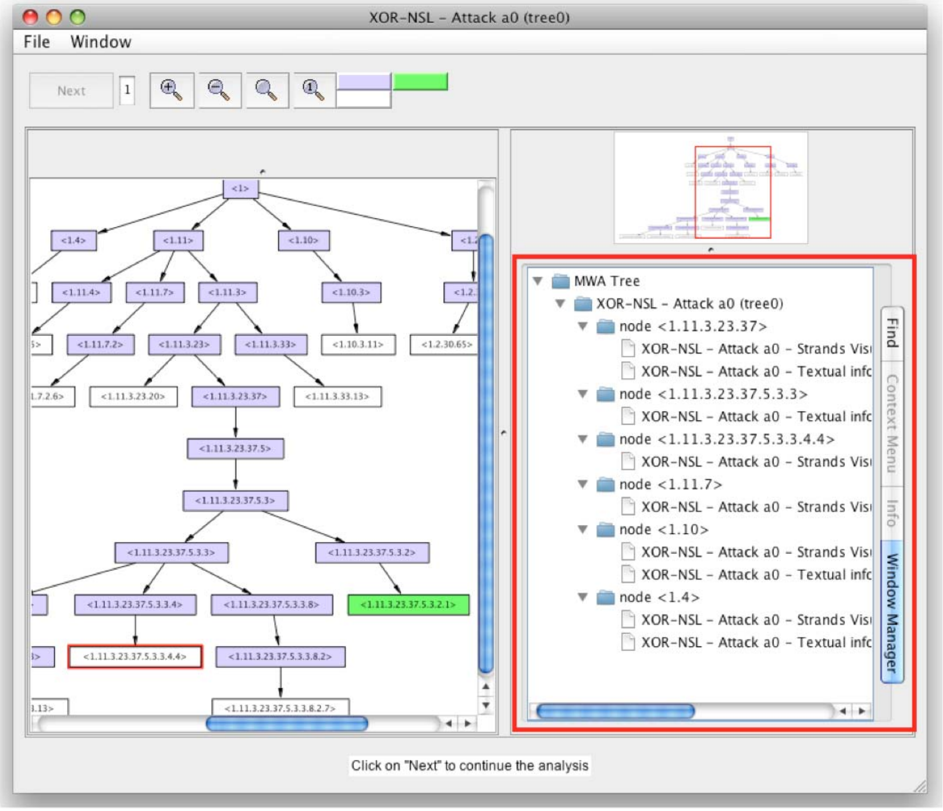
```
** The state is not an initial state
** The state is not unreachable


 Current Strands
 -------------------------
:: nil :: [ nil | - ( pk ( i , n ( b , #0:Fresh ) ) ) , + ( n ( b , #0:Fresh ) ) , nil ] &
 :: nil :: [ nil | - ( n ( b , #0:Fresh ) ) , + ( pk ( b , n ( b , #0:Fresh ) ) ) , nil ] &
 :: #0:Fresh :: [ nil | - ( pk ( b , a ; n ( a , #1:Fresh ) ) ) , + ( pk ( a , n ( a , #1:Fresh ) ; n ( b , #0:Fresh ) ) ) , - ( pk ( b , n
 ( b , #0:Fresh ) ) ) , nil ] &
 :: #1:Fresh :: [ nil , + ( pk ( i , a ; n ( a , #1:Fresh ) ) ) | - ( pk ( a , n ( a , #1:Fresh ) ; n ( b , #0:Fresh ) ) ) , + ( pk ( i , n (
 b , #0:Fresh ) ) ) , nil ]

 Intruder knowledge
 -------------------------
pk ( a , n ( a , #1:Fresh ) ; n ( b , #0:Fresh ) ) !inI ,
 pk ( b , n ( b , #0:Fresh ) ) !inI ,
 pk ( i , n ( b , #0:Fresh ) ) !inI ,
 n ( b , #0:Fresh ) !inI ,
 pk ( b , a ; n ( a , #1:Fresh ) ) inI
```

Figure 13: Textual representation of a Maude-NPA state

3.4.4. The window manager

As Section 3.4.3 says, for each stateof the search tree, two windows can be opened through the contextual menu associated to it. Moreover, the user may explore different states of the search space tree to compare the information of several states at the same time. This means that the user may have many opened windows, so that it is necessary to manage all of them in some way. In order to solve this problem, the Maude-NPA GUI offers to the user a window manager, which is available at the area in the right bottom corner of the window that shows the representation of the search tree. The user only has to click on the tab with title *"Window Manager"* to see a list with all the active windows associated to each state of the search tree, as Figure 14 shows.

Whenever the user wants to bring to the front an active window, she must click on the corresponding "Window Manager" item.



- MWA Tree
  - XOR-NSL – Attack a0 (tree0)
    - node <1.11.3.23.37>
      - XOR-NSL – Attack a0 – Strands Visi
      - XOR-NSL – Attack a0 – Textual infc
    - node <1.11.3.23.37.5.3.3>
      - XOR-NSL – Attack a0 – Textual infc
    - node <1.11.3.23.37.5.3.3.4.4>
      - XOR-NSL – Attack a0 – Strands Visi
    - node <1.11.7>
      - XOR-NSL – Attack a0 – Strands Visi
    - node <1.10>
      - XOR-NSL – Attack a0 – Strands Visi
      - XOR-NSL – Attack a0 – Textual infc
    - node <1.4>
      - XOR-NSL – Attack a0 – Strands Visi
      - XOR-NSL – Attack a0 – Textual infc

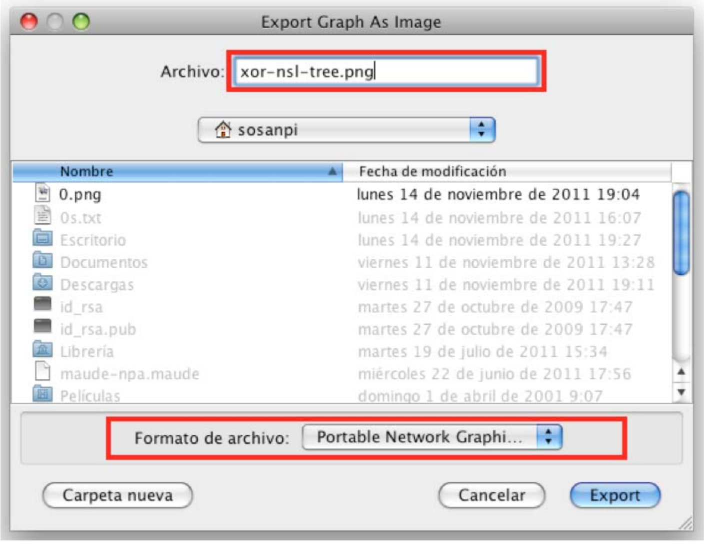
Click on "Next" to continue the analysis

Figure 14: The "Window Manager"

3.4.5. Exporting a search tree as an image

The search tree displayed by the Maude-NPA GUI can be exported as an image, more specifically as a file either in the Encapsulated PostScript (.eps) format or in the Portable Network Graphics (.png) format. This option is available in the menu option *"File -> Export Image".*

To export the tree as an image the user has to select the correponding file format (.eps or .png), choose the directory where he or she wants to export the image and write the name of the file (**including its extension**), as shown in Figure 15.



Archivo: xor-nsl-tree.png

sosanpi

Nombre	Fecha de modificación
0.png	lunes 14 de noviembre de 2011 19:04
0s.txt	lunes 14 de noviembre de 2011 16:07
Escritorio	lunes 14 de noviembre de 2011 19:27
Documentos	viernes 11 de noviembre de 2011 13:28
Descargas	viernes 11 de noviembre de 2011 19:11
id_rsa	martes 27 de octubre de 2009 17:47
id_rsa.pub	martes 27 de octubre de 2009 17:47
Librería	martes 19 de julio de 2011 15:34
maude-npa.maude	miércoles 22 de junio de 2011 17:56
Películas	domingo 1 de abril de 2001 9:07

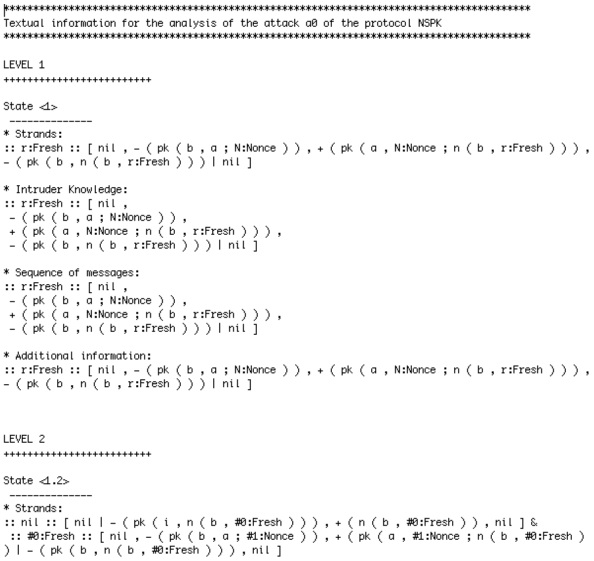
Formato de archivo: Portable Network Graphi...

Figure 15: Exporting the search tree as an image

3.4.6. Saving the search tree information as a text file

The Maude-NPA GUI also allows the user to save the information of the search tree into a text file, in a similar way as the textual information of a Maude-NPA state is shown to the user but for all the states of each generated level. This feature is available in the menu option *"File -> Save search tree information …".*

The user simply has to choose where she wants to save the text file. The tool will automatically generate a ".txt" file containing all the information in the directory selected by the user. In Figure 16 we provide an example of how this text file looks like.



```
****************************************************************************************
Textual information for the analysis of the attack a0 of the protocol NSPK
****************************************************************************************

LEVEL 1
+++++++++++++++++++++++++

State <1>
 --------------
* Strands:
:: r:Fresh :: [ nil , - ( pk ( b , a ; N:Nonce ) ) , + ( pk ( a , N:Nonce ; n ( b , r:Fresh ) ) ) ,
- ( pk ( b , n ( b , r:Fresh ) ) ) | nil ]

* Intruder Knowledge:
:: r:Fresh :: [ nil ,
 - ( pk ( b , a ; N:Nonce ) ) ,
 + ( pk ( a , N:Nonce ; n ( b , r:Fresh ) ) ) ,
 - ( pk ( b , n ( b , r:Fresh ) ) ) | nil ]

* Sequence of messages:
:: r:Fresh :: [ nil ,
 - ( pk ( b , a ; N:Nonce ) ) ,
 + ( pk ( a , N:Nonce ; n ( b , r:Fresh ) ) ) ,
 - ( pk ( b , n ( b , r:Fresh ) ) ) | nil ]

* Additional information:
:: r:Fresh :: [ nil , - ( pk ( b , a ; N:Nonce ) ) , + ( pk ( a , N:Nonce ; n ( b , r:Fresh ) ) ) ,
- ( pk ( b , n ( b , r:Fresh ) ) ) | nil ]


LEVEL 2
+++++++++++++++++++++++++

State <1.2>
 --------------
* Strands:
:: nil :: [ nil | - ( pk ( i , n ( b , #0:Fresh ) ) ) , + ( n ( b , #0:Fresh ) ) , nil ] &
 :: #0:Fresh :: [ nil , - ( pk ( b , a ; #1:Nonce ) ) , + ( pk ( a , #1:Nonce ; n ( b , #0:Fresh )
) | - ( pk ( b , n ( b , #0:Fresh ) ) ) , nil ]
```

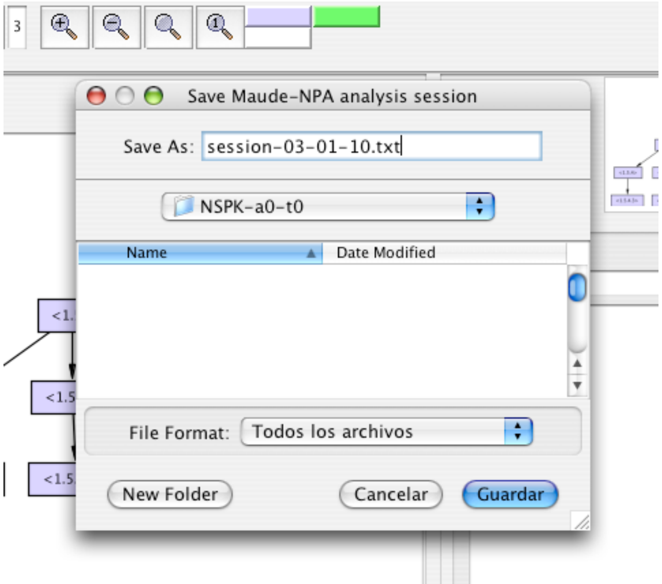
Figure 16: Text file with the saved information of a search tree

3.5. Saving and restoring an analysis session

Sometimes, the analysis of a protocol with the Maude-NPA GUI can take a lot of time. For this reason, the Maude-NPA GUI allows the user to save an analysis session, i.e. to save the search tree levels already generated during the current analysis session that she is performing in such a way that, later, she can continue that analysis session from the point where that session was saved, without having to start the analysis from scratch and without having to generate the grammars associated to the protocol specification.

More specifically, saving an analysis session in the Maude-NPA GUI involves writing relevant data of the session in a text file given by the user. However, note that this action must be performed when the tool is not generating a new level of the search tree.

In order to save an analysis session, the user must select, in the window that shows graphically the search tree, the menu option *"File -> Save Session…".* Then, she is required to select the directory and the name of the text file where the current analysis session will be saved (see Figure 17). Once the user has specified the text file, the Maude-NPA GUI will automatically write in this text file the necessary data of the current analysis session.



Save As: session-03-01-10.txt

NSPK-a0-t0

File Format: Todos los archivos

Figure 17: Saving an analysis session in the Maude-NPA GUI

Regarding to restoring an analysis session, the Maude-NPA GUI just requires the user to select the text file where that session was previosly saved. Then, the tool starts an analysis session with the data that was saved in this text file so that the user can continue executing the analysis of a protocol from the last level that was generated in the saved session.

The user can restore a previously saved session by selecting the menu suboption *"File -> Restore Session…"* in the main window of the Maude-NPA GUI, as Figure 18 shows.

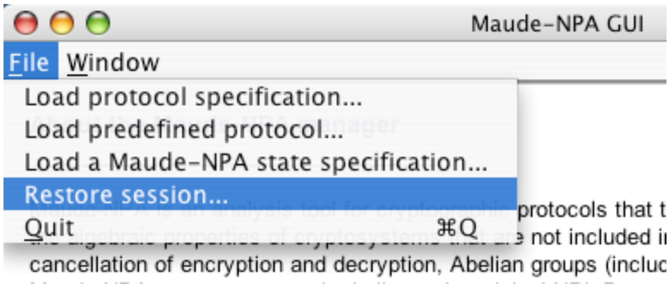
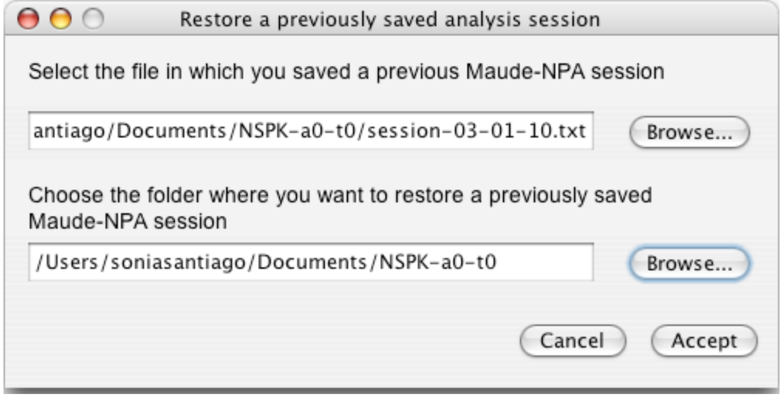

Maude-NPA GUI
File
Window
Load protocol specification...
Load predefined protocol...
Load a Maude-NPA state specification...
Restore session...
Quit
⌘Q
protocols that t
not included i
cancellation of encryption and decryption, Abelian groups (incluc

Figure 18: Menu suboption to restore an analysis session

Once the user has selected the corresponding menu suboption to restore an analysis session, a new window is shown to the user (see Figure 19). This window requires the user to select (i) the file where a previous analysis session was saved and (ii) the folder for temporal files associated to this protocol. By default, the Maude-NPA GUI sets this temporal folder to a new folder (created automatically) whose name is the name of the file (without the extension) where the session was saved and that is allocated at the NPAAssist directory of the Maude-NPA GUI installation. The user can choose any directory, except the one where the predefined protocols of the Maude-NPA GUI are allocated. When these two fields have been filled in by the user, she has to press the *"Accept"* button and a new window will display the search tree with all the levels that were previously generated during the analysis session that has been restored.



Restore a previously saved analysis session

Select the file in which you saved a previous Maude-NPA session

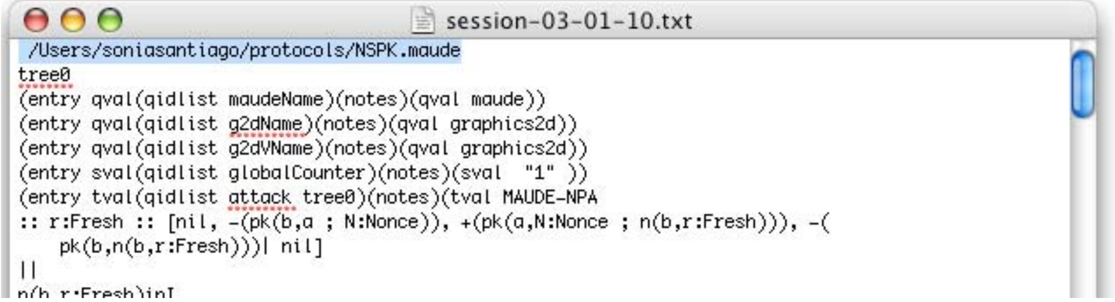
antiago/Documents/NSPK-a0-t0/session-03-01-10.txt

Choose the folder where you want to restore a previously saved Maude-NPA session

/Users/soniasantiago/Documents/NSPK-a0-t0

Figure 19: Window to restore a previously saved analysis session

When restoring a previously saved analysis session, the Maude-NPA GUI needs the file that contains the specification of the protocol that is being analyzed to be in the same directory where it was allocated during the analysis session that was saved. If this file has been removed from this location, the user can either copy it again in that directory or modify manually the text file in which the analysis session was saved. In the second case, the user must replace the first line of the text file (that contains the old location of the file with the specification of the protocol) with the new directory where it is allocated, as Figure 20 shows.



session-03-01-10.txt

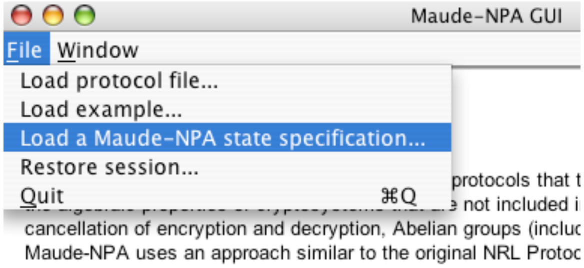
```
 /Users/soniasantiago/protocols/NSPK.maude
tree0
(entry qval(qidlist maudeName)(notes)(qval maude))
(entry qval(qidlist g2dName)(notes)(qval graphics2d))
(entry qval(qidlist g2dVName)(notes)(qval graphics2d))
(entry sval(qidlist globalCounter)(notes)(sval  "1" ))
(entry tval(qidlist attack tree0)(notes)(tval MAUDE-NPA
:: r:Fresh :: [nil, -(pk(b,a ; N:Nonce)), +(pk(a,N:Nonce ; n(b,r:Fresh))), -(
    pk(b,n(b,r:Fresh)))| nil]
||
n(b,r:Fresh)inI
```

Figure 20: Modifying manually the file where a session was restored to update the path to the file that contains the specification of a protocol

3.6. Loading the specification of a Maude-NPA state

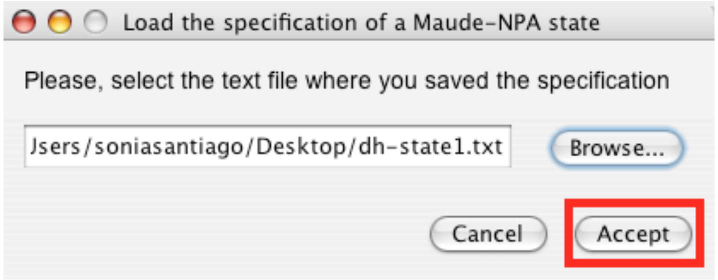
The Maude-NPA GUI allows the user to obtain the graphical and textual representation of any Maude-NPA state, not only the ones that have been generated by the GUI. This feature is very useful and allows users to keep apart textual copies of states and display them as explained in Section 3.4.3.

The user can load a file with the specification of a Maude-NPA state by selecting the menu suboption *“File -> Load a Maude-NPA state specification…”* in the main window of the Maude-NPA GUI, see Figure 21. As a result, a new window (see Figure 22) will be opened. In this window, the user has to browse her file system to select the file that contains the state specification. Once this has been done, the user must click on the *“Accept”* button.



protocols that t
e not included i
cancellation of encryption and decryption, Abelian groups (incluc
Maude-NPA uses an approach similar to the original NRL Protoc

Figure 21: Menu suboption to load a file with the specification of a concrete Maude-NPA state

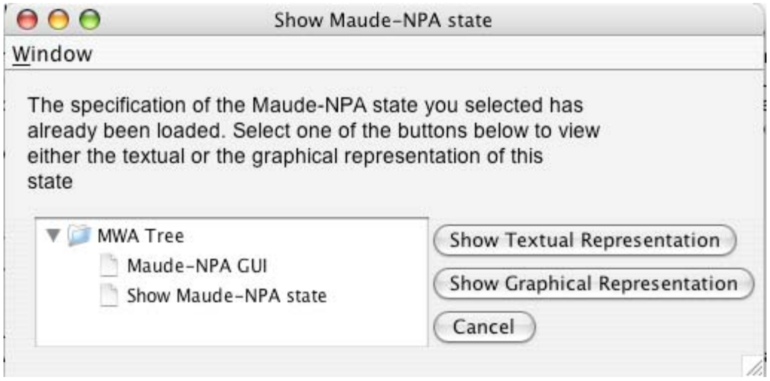


Please, select the text file where you saved the specification

Jsers/soniasantiago/Desktop/dh-state1.txt

Figure 22: Window to load the file that contains the specification of a Maude-NPA state

After clicking on the *“Accept”* button, the Maude-NPA GUI will open a new window (see Figure 23). This window allows the user to view both the textual and the graphical representations of the Maude-NPA state, by clicking on the buttons *“Show Textual Representation”* or *“Show Graphical Representation”* respectively.



The specification of the Maude-NPA state you selected has already been loaded. Select one of the buttons below to view either the textual or the graphical representation of this state

Figure 23: Window to show both the textual and the graphical representation of the Maude-NPA state

3.7. Shortcuts to start or to restore an analysis session

Once a protocol specification has been loaded with the Maude-NPA GUI, the user can analyze it again without having to load the protocol again, even if she has changed the protocol specification. In principle, the file that contains the protocol specification must be allocated in the same directory where it was placed when it was loaded for the first time. However, as we will see later, if the user has changed the location of this file, she can modify manually one of the configuration files.

When a protocol specification is loaded for the first time, the Maude-NPA GUI generates and executes automatically some configuration files, which are created into the protocol folder selected by the user. More specifically, these files are:

- start-generateGrammar
- start-restoreGrammar
- startup-generateGrammar.txt
- startup-restoreGrammar.txt
- load-npa-assist-generateGrammar.maude
- load-npa-assist-restoreGrammar.maude

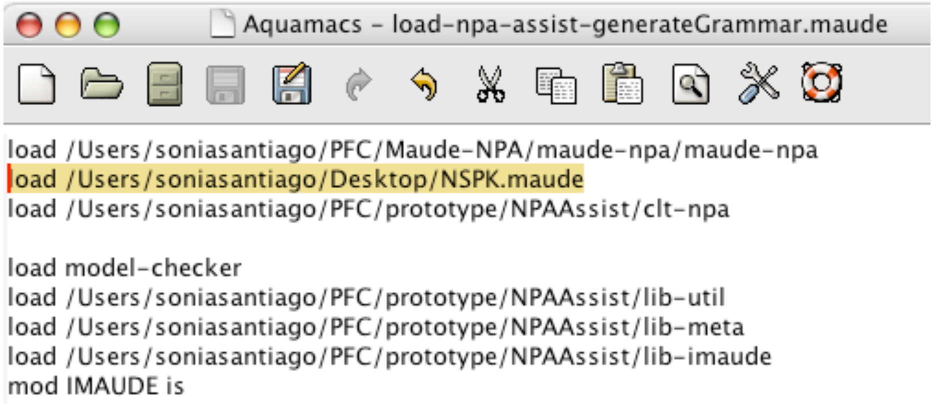
These files (plus the following three) are also created when the user restores a previously saved analysis session:

- start-restoreSession
- startup-restoreSession.txt
- load-npa-assist-restoreSession.maude

With these files, the user can restore again an analysis session without having to launch the Maude-NPA GUI again.

The configuration files whose name starts with *"load-npa-assist"* are the ones that specify the path to the file which contains the protocol specification.

Therefore, if the user has changed the location of this file (with respect to the directory where it was allocated during the saved session), she must edit the second line of the corresponding *"load-npa-assist…"* file and replace the path that is specified with the new one (see Figure 24).



```
load /Users/soniasantiago/PFC/Maude-NPA/maude-npa/maude-npa
load /Users/soniasantiago/Desktop/NSPK.maude
load /Users/soniasantiago/PFC/prototype/NPAAssist/clt-npa

load model-checker
load /Users/soniasantiago/PFC/prototype/NPAAssist/lib-util
load /Users/soniasantiago/PFC/prototype/NPAAssist/lib-meta
load /Users/soniasantiago/PFC/prototype/NPAAssist/lib-imaude
mod IMAUDE is
```

Figure 24: Modifying manually one of the configuration files to update the path to the file that contains the protocol specification

Files start-generateGrammar, start-restoreGrammar and start-restoreSession allow to start the analysis of a protocol in different ways. Before using these files, please, set them as executable files by typing the following commands in the command line:

```
chmod +x start-generateGrammar
chmod +x start-restoreGrammar
chmod +x start-restoreSession
```

Then, to start the analysis of a protocol execute any of these files by typing in the command line:

```
./start-generateGrammar
./start-restoreGrammar
./start-restoreSession
```

The execution of the first command will generate a new grammar for the protocol specification and save it in the protocol folder. This command is the one that must be used whenever the user has modified the protocol specification.

If a protocol specification has not been modified, the user can execute the second command which will make the Maude-NPA GUI start a new protocol analysis session reusing a grammar file that was previously generated and saved into the protocol folder.

The third command can be executed to restore a previously saved analysis session. In this case, the Maude-NPA GUI will reuse the grammar file that was generated during the saved analysis session. This means that the protocol specification of the saved session cannot be modified.

After the execution of the first two commands, the window to select one of the attacks of the procotocol is shown to the user. If the user executes the third command, the Maude-NPA GUI will display the window with the graphical representation of the search tree with all the levels already generated of the restored session.

4. FURTHER INFORMATION

This document contains the most detailed information about how to install and use the Maude-NPA GUI. However, if you would like to read some more specific information about this GUI, please visit the *"Documentation"* section at the Maude-NPA GUI homepage at

www.dsic.upv.es/grupos/elp/Maude-NPA_GUI

You can also obtain specific information about the Maude-NPA tool at its homepage, whose link is maude.cs.uiuc.edu/tools/Maude-NPA/. In this website, publications and other references about the Maude-NPA are available. Furthermore, the user can download the latest version of the Maude-NPA from the "Downloads" section.

If you are interested in implementing graphical interfaces for formal reasoning tools, you might like to visit the InterOperability Platform Homepage at:

http://jlambda.com/~iop/

and the Interactive Maude homepage at:

www.csl.sri.com/users/clt/IMaudeWeb/

These two frameworks have been used to implement the Maude-NPA GUI.

In case you have any other question or doubts, or if you would like to report any bug you experience while using the Maude-NPA GUI, please do not hesitate to contact Sonia Santiago at ssantiago@dsic.upv.es .