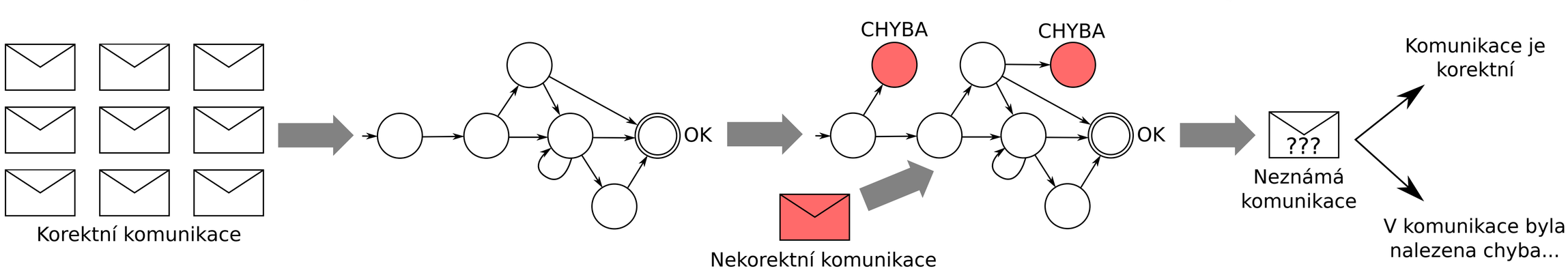
POLOAUTOMATICKÁ DIAGNOSTIKA SÍŤOVÝCH PROTOKOLŮ

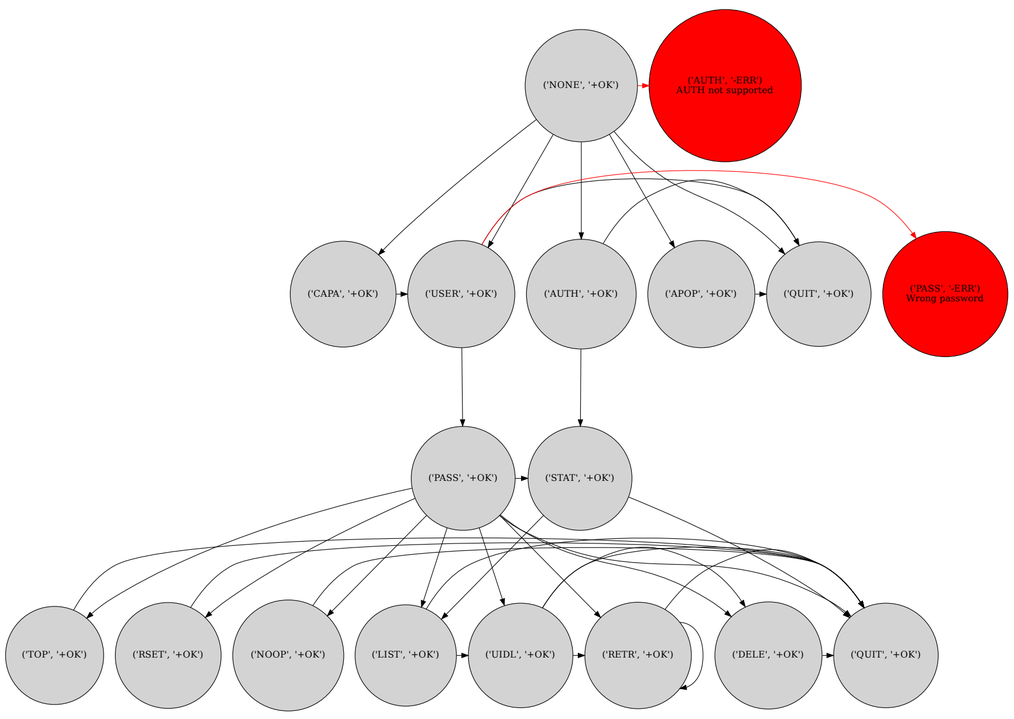
Excel@FIT 2018

Pro správce sítě a administrátory je v podstatě nemožné znát podrobně všechny protokoly, které se používají v jimi spravovaných sítích. Pokud se v síti vyskytne nějaký problém, tak správcům nezbyde nic jiného, než nastudovat normu daných protokolů a pokusit se problém odhalit manuálně. Proto byl vytvořen nástroj, který se dokáže naučit popis protokolu ze vzorků korektní komunikace a následně do něj přidat chyby naučené z nekorektní komunikace. Tento popis lze potom použít ke kontrole komunikace neznámé, kde nástroj buď tuto komunikaci označí za korektní anebo v ní nalezne chybu.



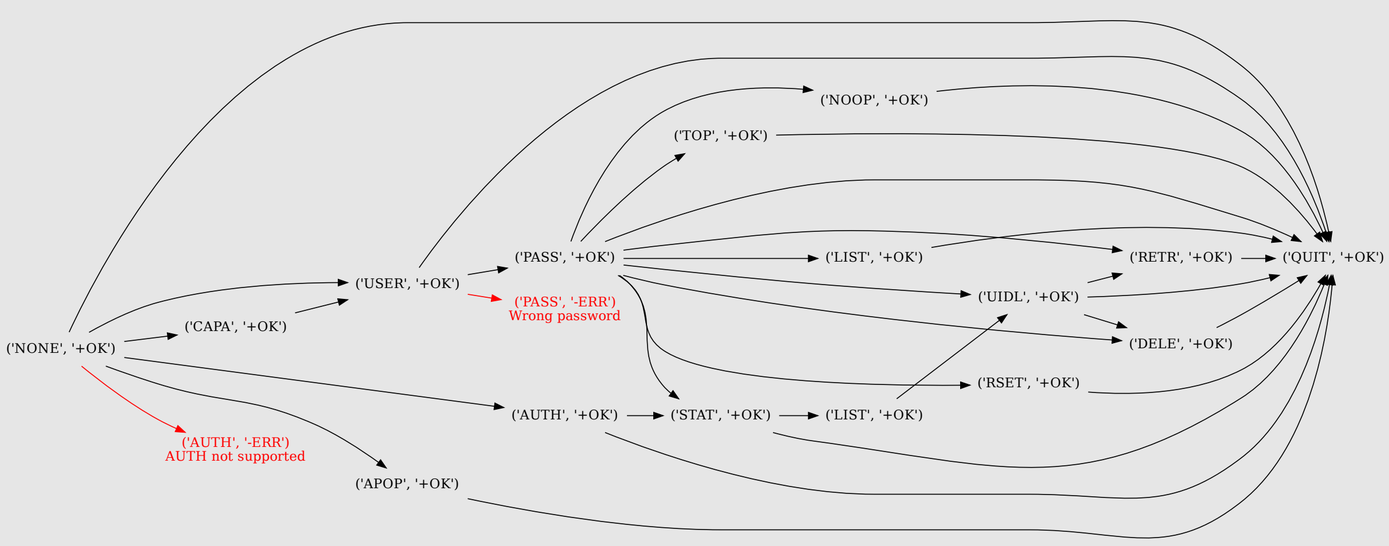
Vstupem pro trénování popisu protokolu jsou pcap soubory, obsahující zprávy komunikace v tomto protokolu. Důležitou částí trénování je předzpracování těchto zpráv. Problémem jsou zprávy, které jsou určitým způsobem náhodně generované anebo šifrované. Tyto zprávy není vhodné do popisu protokolu zanášet, protože jsou unikátní pro každou komunikaci. Při kontrole neznámé komunikace se také může stát, že se v této komunikaci nachází nějaký nový, pro nás neznámý příkaz. To může snadno nastat vzhledem k tomu, že značná část protokolů má nějaká rozšíření, která přinášejí nové typy zpráv.

```
S: 220 localhost.localdomain ESMTP Postfix (Ubuntu)
C: EHLO
S: 250 Syntax: HELO hostname
C: mail from: <dan>
S: 250 Ok
C: rcpt to: <bounce@goofy.uhcc.hawaii.edu>
S: 554 <bounce@goofy.uhcc.hawaii.edu>: Relay access denied
data  , cat /etc/passwd
S: 554 Error: no valid recipients
C: quit
S: 221 Bye
```



Důležitou součástí aplikace jsou metody na převod posloupnosti zpráv v komunikaci protokolu na popis reprezentující tento protokol. Byly navrženy tři metody z nichž každá přistupuje k tvorbě popisu jiným způsobem. Popisy mají dvě důležité vlastnosti, které jsou do značné míry protichůdné. Popis by měl být co nejvíce obecný, což znamená, že by měl umět akceptovat, co možná nejvíce korektních posloupností zpráv, na které nebyl trénován. Na druhou stranu by měl být co nejvíce přesný, neboli neměl by označovat nekorektní posloupnosti zpráv za korektní.

Nástroj bý testován na protokolu POP3 a částečně na protokolu SMTP. Dokázal správně zařadit neznámou správnou komunikaci asi v 80 % případů. Testovány byly také chybové komunikace a ukázalo se, že pokud byl nástroj na danou chybu trénován, tak ji vždy dokázal odhalit. Pokud na ni trénován nebyl, tak ji přeskočil s tím, že se jednalo o neznámý příkaz.



ONDŘEJ SVOBODA #20

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY