**Technická dokumentace**

**Smart Metering Honeypot**

(software)

2022

Identifikační číslo výsledku: FW02020084-V1

Název projektu: Výzkum systémových prvků pro zvýšení bezpečnosti a spolehlivosti infrastruktury chytrého měření

# ÚVOD

Tento dokument popisuje softwarovou aplikaci Smart Metering Honeypot, která byla složí k emulaci chytrých elektroměrů. Emulovaný virtuální elektroměr je reálnou kopii chytrých elektroměrů, to je docíleno extrakcí konfigurace z reálných elektroměrů. Honeypot využívá protokol DLMS/COSEM, který se primárně využívá pro chytré elektroměry.

Základní informace:

* Software
* Řešitelský tým: David Kohout, Mlýnek Petr, Fujdiak Radek, Sláčik Jan
* Software je k dispozici na ukázky na: Vysoké učení technické v Brně, Technická 12 Brno 61600, Česká republika, laboratoř SD 5.64.
* Kontakt: Petr Mlýnek, [mlynek@vut.cz](mailto:mlynek@vut.cz)

# Technická dokumentace

Smart Metering Honeypot je softwarová aplikaci, která dokáže emulovat velké množství chytrých elektroměrů na jediném zařízení s využitím standardu DLMS. Díky použitému programovacímu jazyku Java je výsledná aplikace snadno přenositelná a lze tak spustit na Windows i Linuxu.

Emulátor funguje tím způsobem, že si předem extrahujeme konfiguraci z reálných elektroměrů, a výsledný xml soubor lze pak využít pro následné emulování elektroměrů.

Obrázek 1 zobrazuje konzolový výstup po spuštění jednoho honeypotu (DLMS server) a Obrázek 2 zobrazuje ukázka funkčnosti na OS Linux (Ubuntu).

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek : Konzolový výstup po spuštění jednoho serveru

Obsah obrázku text, monitor, snímek obrazovky, černá

Popis byl vytvořen automaticky

Obrázek : Ukázka funkčnosti na OS Linux (Ubuntu)

**Novost:**

* Emulace reálných elektroměrů.
* Naplnění požadavků na kybernetickou bezpečnost – splněny všechny požadavky přílohy č. 4 k vyhlášce č. 359/2020 Sb. Soulad použitých algoritmů s kryptografickými požadavky doporučenými NÚKIB.

**Přínosy**:

* Přenositelnost aplikace.
* Emulace jakéhokoliv reálného elektroměrů.
* Napojení na klientskou aplikaci.
* Ověření a testy bezpečnosti elektroměrů před nasazením.
* Analýza komunikace DLMS a možných útoků.

# Ekonomické parametry

Výsledek bude implementován v laboratoři Chytrých sítí na VUT v Brně, kde bude probíhat kontinuální sběr dat a následné vyhodnocení. To umožní sběr praktických výsledků pro další prezentace výsledků pro konference a marketingové účely, zároveň bude výsledek dostupný pro ukázky v rámci návštěv firem. To umožní diskuze s komerčními partnery a v případě zájmu využití pro další smluvní výzkum či poskytnutí SW či dat komerčním způsobem.

Ekonomické parametry výsledky lze shrnout do těchto bodů:

* Zvýšení obratu smluvního výzkumu VUT (0,3-0,5 mil. Kč/ročně po dobu 3 let).
* Zvýšení prestiže VUT. Zapojení reálných zařízení do výuky.
* Získané know-how bude sloužit k dalšímu výzkumu a vývoji.

Software poskytován na základě licenčních podmínek následovně:

* Zapůjčení SW nasazeném na HW (raspberry pi) na testy.
* Testování produktů na základě smluvního výzkumu – testy v laboratoři s využitím SW.
* Kontakt na licence a testování: mlynek@vut.cz, +420 54114 6960

# Instalační manuál

Aplikace serveru lze jednoduše spustit na kterémkoliv zařízení, pokud je na daném zařízení nainstalována minimálně Java 11 a výše.

## Instalace na OS Windows:

Stažení souboru Java JDK11 z oficiálních stránek Oracle, případně OpenSource distribuce OpenJDK.

Následně nainstalovat a po instalaci ověřit nainstalovanou verzi pomocí příkazového řádku:

java -version

Po zadání příkazu by konzole měla vypsat aktuální nainstalovanou verzi. Viz Obrázek 3. V opačném případě je nutné upravit systémové proměnné a doplnit cestu k nainstalované verzi Javy.

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek : Ověření verze Javy

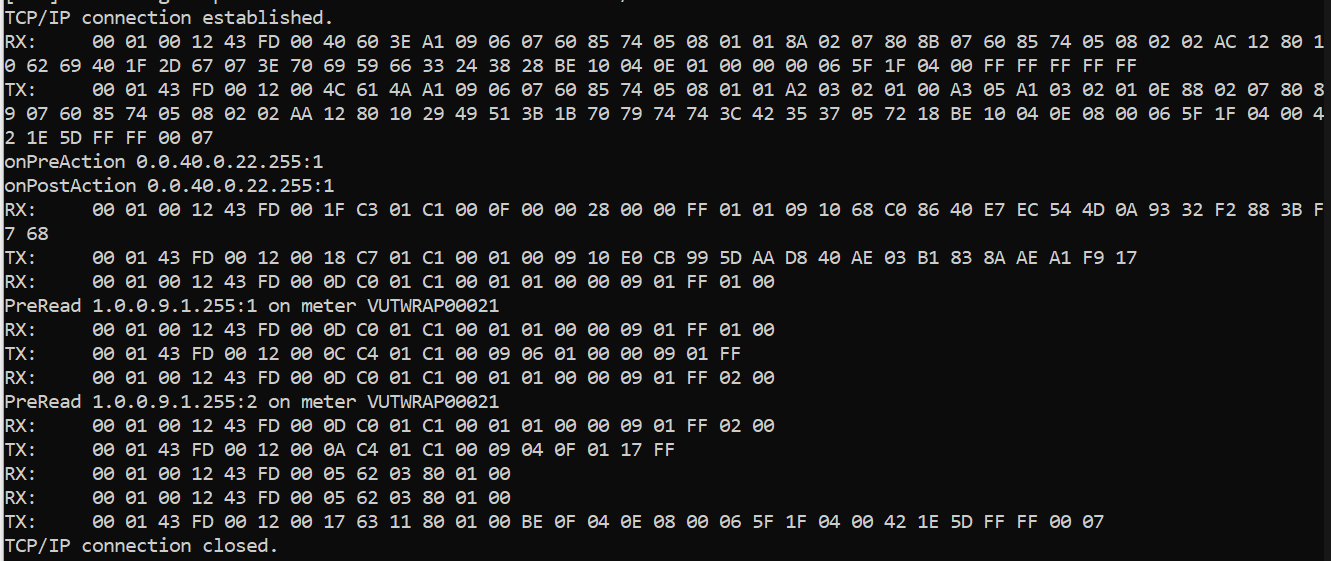
## Instalace na OS Ubuntu (Linux) i Raspbian:

Na OS Linux je instalace jednodušší, kde stačí využít pouze jeden příkaz:

sudo apt install openjdk-11-jdk

## Spuštění aplikace serveru

Po úspěšném nainstalování Javy je již možné aplikaci spustit. Spuštění aplikace je blíže popsáno v části Uživatelský manuál. Po správné volbě parametrů a vstupních souborů je možné se k aplikaci připojit. Obrázek 8 znázorňuje funkčnost odečtu emulovaného elektroměru z klientské aplikace. Odečet je možné realizovat z kteréhokoliv DLMS klienta. Odečet na obrázku obsahuje navázání spojení (autentizace úrovně high), odečtení objektu typu DATA (LN: 1.0.0.9.1.255) a ukončení spojení.



Obrázek : Odečet emulovaného elektroměru

# Uživatelský manuál

## Argumenty pro spuštění serveru

Pro vhodné nakonfigurování celého spuštění obsahuje aplikace několik argumentů, pomocí kterých lze snadno a rychle měnit základní parametry spuštění celé aplikace. Nejzákladnější příkaz pro spuštění nějakého serveru je následující:

java -jar DATEL-1.4.0-Server.jar O -w 1 -f objects.xml

První část příkazu spouští aplikaci pomocí javy (java -jar DATEL-1.4.0-Server.jar). Následuje „O“, které definuje, jakým způsobem se bude server načítat (v tomto případě pomocí souboru s OBIS kódy). Zbytek příkazů slouží k následujícím akcím:

|  |  |  |  |
| --- | --- | --- | --- |
| **Příkaz** | **Vstupní data** | **Popis** | **Výchozí hodnota** |
| -f | Soubor | Soubor s objekty pro meter | - |
| -c | Soubor | Konfigurační soubor s dalšími parametry | - |
| -w | Číslo | Počet serverů typu Wrapper | 0 |
| -h | Číslo | Počet serverů typu HDLC | 0 |
| -p | Číslo | Počáteční port pro tvorbu serverů | 4059 |
| -samePort | - | Servery poběží na stejném portu | - |
| -SN | - | Server použije SN odkazování (pokud to umožňují zadané OBIS) | - |
| -remote | - | Vypne vzdálenou správu | - |
| -rp | Číslo | Port pro vzdálenou správu | 4444 |
| -t | - | Detailnější výpis do konzole | - |
| -v | - | Výpis všeho do konzole | - |
| -l | - | Zapnutí logování zpráv do logů | - |

V případě nespecifikování žádných argumentů dojde k automatickému zobrazení nápovědy k příkazům, viz Obrázek 3.

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek : Nápověda při nespecifikování žádných parametrů

## Tvorba seznamu objektů

Vytvoření seznamu objektů je velice důležité pro správné a očekávané fungování samotného emulovaného elektroměru. Pomocí některých OBIS kódů dochází k přímému ovlivňování funkčnosti celého řešení. Nejdůležitější objekty jsou následující:

* AssociationLogicalName – umožňuje specifikovat dostupné objekty pro jednotlivé úrovně přístupu, včetně volby požadované autentizace, hesel a adres k přístupu.
* HDLCSetup – nastavení chování spojení s využitím HDLC zpráv.
* TcpUdpSetup – nastavení chování spojení při využití Wrapper zpráv.

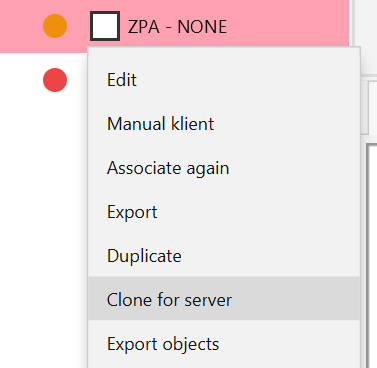
Ostatní objekty jsou převážně pouze datové a mohou být čteny/měněny při odečtech v závislosti na nastavení přístupových oprávnění k daným objektům pro přístupové role. Hodnoty všech objektů se v čase nijak nemění, dochází k odečtení toho, co bylo nastavené v seznamu objektů, případně co bylo za běhu přepsáno stranou klienta. Jedinou výjimkou jsou objekty, které obsahují hodiny. Hodiny získávají aktuální čas ze systému.

Seznam objektů je ve formátu XML a využívá se zde elementů, které používá DLMS knihovna Gurux. Jak vypadá seznam objektů je znázorněno na obrázku 4.

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek : XML se seznamem objektů



Obrázek 7: Export seznamu z klientské aplikace

Export seznamu objektů z reálného elektroměru je možný v klientské aplikaci po kliknutí na vybraný elektroměr a zvolením tlačítka „Clone for server,“ případně tlačítkem „Export objects.“ První možnost začne vyčítat kompletní obsah objektů, které jsou dostupné pro danou přístupovou úroveň.

## Tvorba konfiguračního souboru

Následující Obrázek 6 obsahuje základní konfigurační soubor, kterým je možné přepsat ostatní výchozí nastavení, které není možné definovat pomocí argumentů v příkazové řádce. Nejdůležitější nastavení je zvýrazněno v rámečku. V tomto nastavení lze definovat použití šifrování zpráv, nastavení klíčů a případně změnit nastavení, zda se mají kontrolovat některé prvky komunikace. Mezi tyto prvky patří vypnutí kontroly autentizace, zadané adresy a případně nastavení přístupu k objektům.

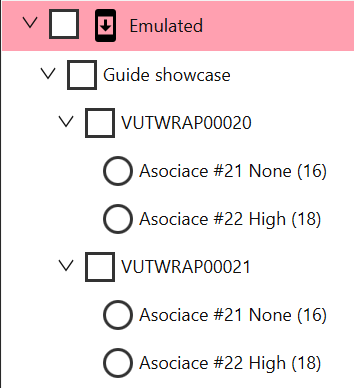


Obrázek : Konfigurační soubor

## Ovládání z klientské aplikace

Aplikace serveru je částečně propojená s klientskou aplikací. Toto vzájemné propojení umožňuje automaticky zjistit, jaké elektroměry jsou aktuálně emulované a jaké přístupové úrovně jednotlivé servery využívají.

Při inicializaci z klientské strany tak stačí znát IP adresu zařízení, port pro vzdálenou správu. Veškeré přenášené ovládací zprávy a přenášené konfigurace mohou být šifrované. K šifrování se využívá AES-CBC-256 a pro dohodnutí klíčů slouží algoritmus ECDH-256.



Obrázek : Automaticky načtené emulované elektroměry

# Programátorský manuál

Software a zdrojové kódy jsou dostupné na vyžádání na základě licenčních podmínek viz kapitola 2.

## Použité nástroje

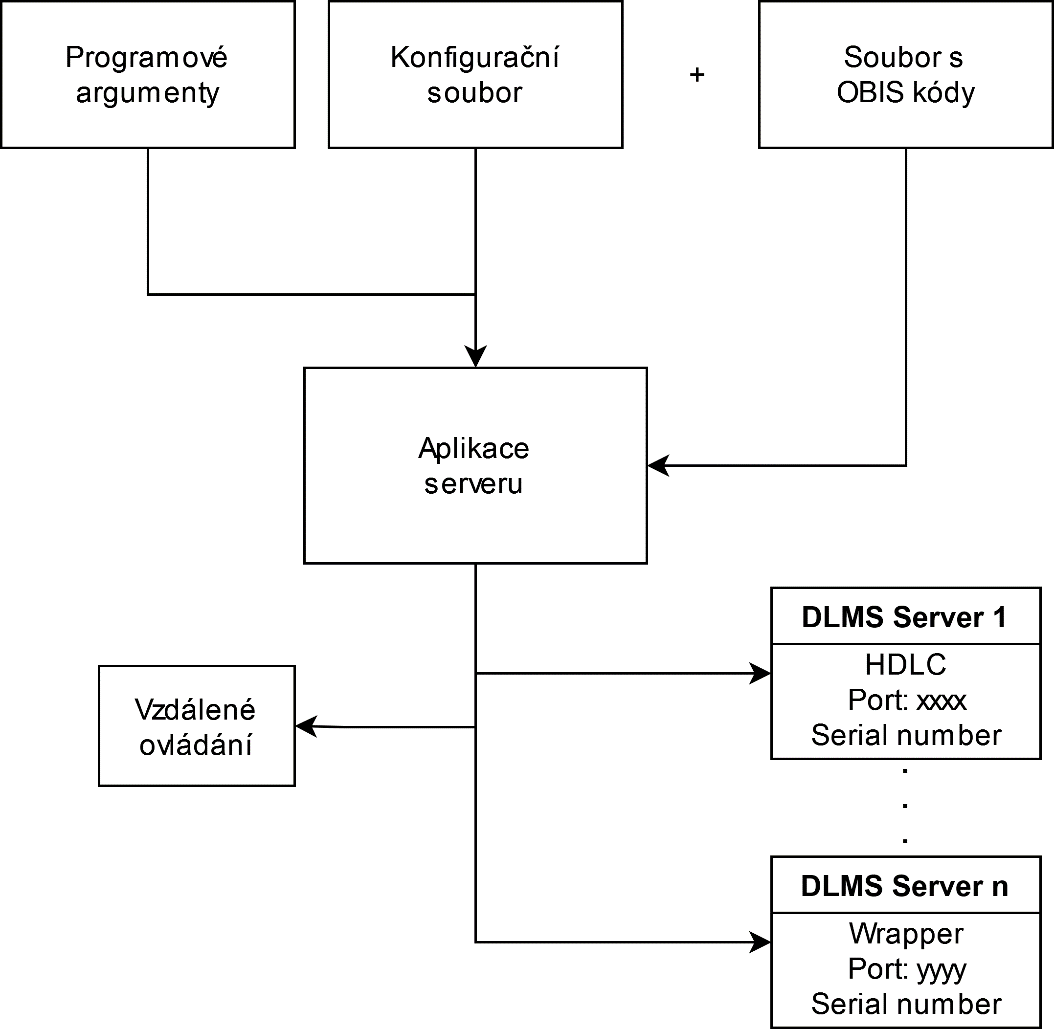
Pro implementaci DLMS serveru byla využita knihovna Gurux Ltd. Jedná se o open source licenci GNU GPL v2. Celé řešení pak využívá programovací jazyk Java verze 11.

Celkové řešení je primárně určené k využití na RaspberryPi, ale díky použitému jazyku je aplikace přenositelná a spolehlivě funkční na OS Linux i OS Windows.

## Základní schéma spuštění aplikace

Aplikace obsahuje v aktuálním stavu 3 vstupní části (příkazové argumenty, konfigurační soubor a v neposlední řadě soubor, který obsahuje všechny objekty, které chceme na elektroměru emulovat). Po zadání všech náležitostí dojde k otevření specifikovaného množství portů, na kterých dojde ke spuštění definovaného množství elektroměrů. Jeden port také může být použit pro přístup k několika emulovaným elektroměrům. V takovém případě dochází k odpovídání pouze toho elektroměru, který obsahuje volané sériové číslo. V reálném nasazení by se takto choval koncentrátor, který by tímto způsobem zprostředkovával připojení k dalším elektroměrům.

Kromě otevření portů pro elektroměry, může aplikace otevřít ještě jeden port, který tak slouží pro vzdálené ovládání celé aplikace.



Obrázek : Základní schéma aplikace emulátoru