ROZŠÍRENÉ ZADANIE DIPLOMOVEJ PRÁCE

Názov práce: Využitie FPGA na bezpečnú komunikáciu medzi IoT zariadeniami

Autor: Bc. Milan Chrastina

Vedúci práce: doc. RNDr. Jozef Jirásek, PhD.

Školiace pracovisko: ÚINF - Ústav informatiky

Ciele:

1. Analyzovať požiadavky na bezpečnú komunikáciu medzi IoT zariadeniami a možnosti ich realizácie pomocou FPGA polí.
2. Navrhnúť bezpečné protokoly pre priamu komunikáciu medzi IoT zariadeniami aj bez pripájania do siete Internet.
3. Implementovať rýchle bezpečné protokoly pre riadenie IoT zariadení v reálnom čase pomocou FPGA polí.
4. Otestovať rýchlosť komunikácie na navrhnutých čipoch.

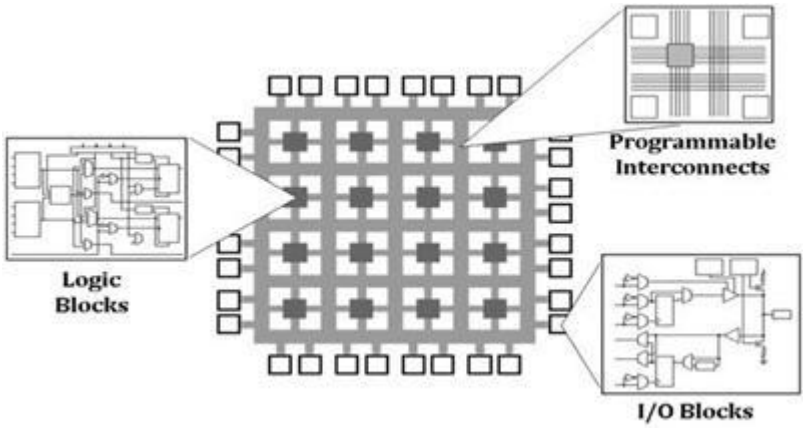
Popis:

Zariadenia IoT (Internet of things – Internet vecí) zažívajú v dnešnej dobe prudký vývoj. Sú to malé zariadenia určené na jeden konkrétny účel, ktoré sa ovládajú cez rozhranie, ktoré je pripojené na internet. Jedná sa o málo-účelové, malé zariadenia, ktoré nedisponujú veľkým výpočtovým výkonom a sú vybavené malou pamäťou. Každé z týchto zariadení je pripojené a ovládané cez Internet samostatne.

Cieľom našej diplomovej práce bude navrhnúť možnosť centralizovaného uzlu, ktorý bude schopný bezpečne komunikovať s viacerými IoT zariadeniami a následne pripojený na Internet.

V prvej časti sa budeme venovať analýze bezpečnostných protokolov na komunikáciu medzi IoT zariadeniami, ktoré ako som spomínal sú obmedzené pamäťovou a výpočtovou kapacitou. Navrhneme protokol, ktorý bude výkonný a implementovateľný na FPGA (Field Programmable Gate Array – Pole programovateľných logických členov) obvodoch. FPGA je typ integrovaného logického obvodu konfigurovateľný resp. konštruovaný používateľom jazykom HDL (hardware description language). Schému FPGA procesora môžete vidieť na obrázku1.

V druhej časti budeme implementovať navrhnutý protokol do FPGA obvodov na FPGA karte Virtex 6 a následné naviazanie komunikácie s druhou kartou.



Obr. 1 Schéma FPGA

Po úspešnom návrhu a implementácii komunikačného protokolu na FPGA karte dáme vyrobiť viacero rovnakých čipov. Na tých budeme následne testovať rýchlosť navrhnutého komunikačného protokolu v simulovanej reálnej prevádzke použitia viacerých IoT zariadení.

V práci sa taktiež budeme venovať analýze odľahčených protokolov na bezpečnú komunikáciu s obmedzeným použitím výpočtového výkonu a obmedzenou pamäťou, ktorá ako som spomínal je charakteristická pre IoT zariadenia. V tabuľke 1 môžeme vidieť niektoré z dopadov na sieť a protokoly ku ktorým dochádza pri IoT zariadeniach.

IoT End Network Requirements	Networking Style Impact
Self-Healing / Scalable	Mesh capable
Secure	Scalable to no, low, medium and high security without over burdening clients
End-node Addressability	Device specific addressing scalable to thousands of nodes
Device Requirements	**Messaging Protocol Impact**
Low Power / Battery-Operated	Lightweight connection, preamble, packet
Limited Memory	Small client footprint, persistent state in case of overflow
Low cost	Ties to memory footprint

Tab. 1 Dopady pri používaní obmedzených zdrojov

Zdroje:

- Ch. V. Raghavendran, G. Naga Satish, P. Suresh Varma: Internet of Things – A Big Challenge in getting the Right Protocol, IARJSET International Advanced Research Journal in Science, Engineering and Technology, Vol. 4, Issue 7, July 2017, ISSN (Online) 2393-8021 ISSN (Print) 2394-1588
- P. Johnson, R. S. Chakraborty, D. Mukhopadhyay, A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications,
  IEEE Transactions on Multi-scale Computing Systems, Vol.1. No 2, 2015, ISSN: 2332-7766