SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

Fakulta elektrotechniky a informatiky

Ing. Ivan Sokol

Autoreferát dizertačnej práce

Návrh a implementácia algoritmov na redukciu množstva údajov prenášaných zariadeniami zapojenými v internete vecí

na získanie akademického titulu

„doktor“ („philosophiae doctor“, v skratke „PhD.“)

V doktorandskom študijnom programe:	Robotika a kybernetika
V študijnom odbore :	Kybernetika
Forma štúdia:	externá
Miesto a dátum:	Bratislava 30.6.2022

STU

Dizertačná práca bola vypracovaná na:

Ústave robotiky a kybernetiky
Fakulta elektrotechniky a informatiky STU v Bratislave
Ilkovičova 3, 812 19 Bratislava

Predkladateľ: Ing. Ivan Sokol
Ústav robotiky a kybernetiky
FEI STU v Bratislave

Školiteľ: prof. Ing. Peter Hubinský, PhD.
Ústav robotiky a kybernetiky
FEI STU v Bratislave

Oponenti: doc. Ing. Ján Vachálek, PhD.
Ústav automatizácie, merania a aplikovanej informatiky
SjF STU v Bratislave

doc. Ing. Peter Ševčík, PhD.
Katedra technickej kybernetiky
FRI ŽU v Žiline

Autoreferát bol rozoslaný: .....

Obhajoba dizertačnej práce sa bude konať dňa 30.8.2022, o 10:00 hod
na: Ústave robotiky a kybernetiky
Fakulta elektrotechniky a informatiky STU v Bratislave
Ilkovičova 3, 812 19 Bratislava
v miestnosti: zasadačka ÚRK

prof. Dr. Ing. Miloš Oravec

STU

Abstrakt

Nachádzame sa na počiatku novej éry, éry Internetu vecí. Na základe prognóz môžeme v blízkej budúcnosti očakávať milióny zariadení pripojených v sieti Internet, ktoré budú navzájom komunikovať. Za touto komunikáciou môžeme očakávať obrovské množstvo prenášaných informácií. To bude klásť vysoké požiadavky na existujúcu infraštruktúru. Aby infraštruktúra dokázala zvládnuť takýto obrovský nárast v komunikácii, musíme sa zamyslieť nad tým, ako tieto dáta prenášať optimálne. Jediný spôsob ako to dosiahnuť, je minimalizovať ich objem pri zachovaní konzistencie obsahu. V práci sme sa zamerali na celý proces spracovania dát od ich získania cez prvotné spracovania na strane zariadenia, ich prenos, až po ich spracovanie na strane aplikácie. Analýza priebehu spracovania dát nás priviedla k realizácii výrazných zmien v celom procese. Úsporu v objeme prenášaných dát sme dosiahli zmenou komprimačného algoritmu a komunikačného protokolu. Výsledkom je nový komprimačný algoritmus s prvkami strojového učenia a umelej inteligencie, ktorý je účinný aj v prípade kompresie krátkych správ. Elimináciou protokolu SSL/TLS sme zasa dosiahli výraznú úsporu v prenose režijných dát. Pritom je zachovaná bezpečnosť prenášaných dát. Ochranu dát realizujeme šifrovacím algoritmom na princípe ľahkej kryptografie. Implementáciou navrhnutých algoritmov sme dosiahli významnú úsporu v objeme prenášaných informácii. Zároveň môžeme očakávať energetické úspory na strane zariadenia, ako aj na strane aplikácie.

Kľúčové slová: *Internet vecí, kompresia dát, ľahká kryptografia*

Abstract

We are at the beginning of a new era, the era of the Internet of Things. Based on forecasts, we can expect millions of devices connected to the Internet soon to communicate on the network. There will be a massive amount of transmitted information behind this communication. This will place high demands on existing infrastructure. For the infrastructure to handle such a massive increase in communication, we need to think about how to transmit this data optimally. The only way to achieve this is to minimize their volume while maintaining content consistency. We focused on the data processing from their acquisition through the initial processing on the device side, transfer, and processing on the application side. The analysis of the data processing process led us to implement significant changes in the entire process. We achieved savings in the volume of transmitted data by changing the compression algorithm and communication protocol. The result is a new compression algorithm with machine learning and artificial intelligence elements, which is effective even when compressing short messages. By eliminating the SSL / TLS protocol, we have again achieved significant savings in overhead data transmission. At the same time, the security of the transmitted data is maintained. We implement data protection with an encryption algorithm based on the principle of Lightweight Cryptography. We have achieved significant savings in the volume of information transmitted by implementing the proposed algorithms. At the same time, we can expect energy savings on the device and the application side.

***Key words**: Internet of Things; data compression, lightweight cryptography*

STU

Obsah

1 Úvod

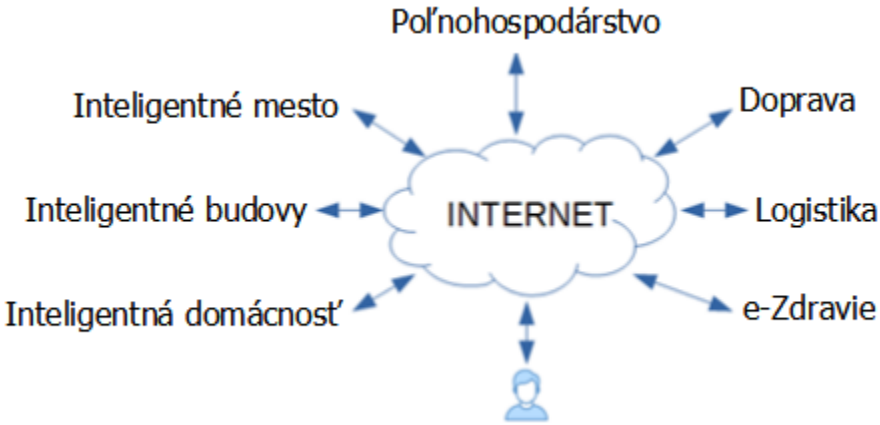
Internet vecí - Internet of Things (IoT), slovné spojenie, s ktorým sa môžeme stretnúť od 1.januára 2001. Jeho autorom je David Brock [1]. Počiatky IoT však môžeme nájsť v podstatne vzdialenejšej histórii. Z iných zdrojov sa dozvedáme, že v roku 1999 koncept IoT prezentoval Kevin Ashton z Massachusetts Institute of Technology (MIT) [2]. Aktivity inštitútu boli v tejto dobe spojené s RFID, NFC, čiarovými kódmi či QR kódmi. Ak sa ponoríme hlbšie do histórie zistíme, že už v roku 1982 bol na Carnegie Mellon University umiestnený automat na sódu, kde bola na diaľku kontrolovaná teplota nápoja [3]. Určite by sme sa dokázali ponoriť aj hlbšie do minulosti, ale pre účel tejto práce to nemá zmysel.

Napriek tomu, že sa s výrazom IoT stretávame viac ako 20 rokov, doteraz nie je definované, čo sa za týmto pomenovaním skrýva. Institute of Electrical and Electronics Engineers (IEEE) v roku 2015 [4] upozorňuje na potrebu definovania dátových, ako aj komunikačných štandardov pre oblasť IoT. Zatiaľ sa tak, i napriek mnohým prebiehajúcim aktivitám, nestalo. Ak dnes hovoríme o IoT, môžeme sa stretnúť s viacerými pomenovaniami tejto oblasti technológií. Rôzne pomenovania súvisia s rôznym uhlom pohľadu na túto stále nedefinovanú oblasť technológií.

Internet veci predstavuje komplexný heterogénny ekosystém. To nám ponúka množstvo uhlov pohľadu na tento rodiaci sa segment technológií. V závislosti od cieľa nášho záujmu môžeme pozornosť sústrediť na senzory či zariadenia, architektúru riešenia, komunikáciu alebo dáta. V tejto práci sústredíme pozornosť na dáta. Zameriame sa na redukciu ich objemu v procese komunikácie.

2 Súčasný stav

Na Obr. 1 prezentujeme niekoľko oblastí, ktoré sa najčastejšie spájajú s IoT. Podstatne hlbšie ponorenie do sveta IoT nájdeme v článku *A Review on Internet of Things for Defense and Public Safety* [5]. Nie je potrebné robiť žiadne hlboké analýzy, aby sme si uvedomili množstvo rôznych pripojených zariadení v pozadí.



Obr. 1 Najčastejšie prezentované oblasti nasadenia IoT

Internet vecí predstavuje komplexný heterogénny ekosystém zastrešujúci široké spektrum zariadení, služieb a s tým spojených aplikácií. Z toho dôvodu sa nebudeme ani snažiť vytvoriť definíciu IoT. Všetky zariadenia však majú jednu spoločnú vlastnosť, musia byť schopné v sieti komunikovať s riadiacou jednotkou alebo navzájom medzi sebou. Pri analýze priebehu spracovania dát, od ich získania na strane zariadenia až po ich spracovanie na strane servera, sústredíme pozornosť na:

- terminológiu,
- senzory – zariadenia,
- dáta,
- komunikáciu,
- architektúru,
- interoperabilitu.

2.1 Terminológia

S informáciami o Internete vecí sa môžeme denne stretnúť vo všetkých druhoch médií. Masívne rozširovanie týchto technológií prináša so sebou množstvo rôznych pomenovaní. Medzi najčastejšie pomenovania s ktorými sa môžeme stretnúť patria:

- Internet of Things (IoT) [6],
- Industrial Internet of Things (IIoT) [7] ,
- Internet of Everything (IoE) [8],
- Web of Things (WoT) [9] [10].

V tejto práci budeme pracovať so slovným spojením Internet vecí - Internet of Things (IoT).

2.2 Senzory – zariadenia

Čo všetko môžeme považovať za IoT senzor alebo zariadenie, je témou mnohých odborných diskusií ako aj diskusných fór. Pre nás senzor/zariadenia predstavuje zdroj informácií, ktoré potrebujeme v ďalšom procese spracovať. Na základe spôsobu činnosti môžeme senzory rozdeliť do dvoch kategórií:

- pasívne,
- aktívne.

2.3 Dáta

Dáta predstavujú základ Internetu vecí. Pre správne fungovanie služby je potrebné mať prístup k dátam v správny čas a v očakávanom dátovom formáte. Zároveň je od nich vyžadovaná integrita a dôveryhodnosť [11].

V práci venujeme pozornosť dátam v dátovom formáte JSON. Uvedené dátový formát predstavuje textový, na jazyku nezávislý dátový formát. Navyše ide pre človeka ľahko čitateľnú ako aj zapisovateľnú podobu dát. Zároveň patrí k najpoužívanejším dátovým formátom používanom v Internete vecí. (viď. Tab. 1)

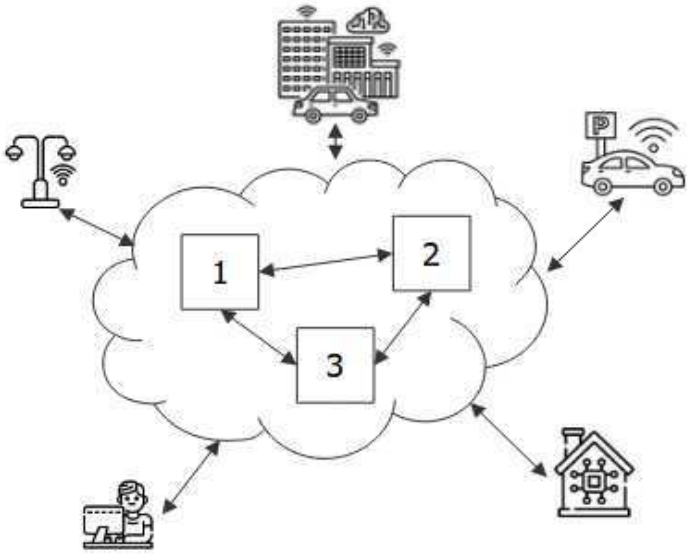
Tab. 1 Dátové formáty používané v Internete vecí

Spoločnosť	Oblasť	Dátový formát
Amazon [12]	IoT	JSON
Google [13]	IoT	JSON
Mozilla.org [14]	WoT	JSON
OneM2M.org [15]	IoT	XML
TheOpenGROUP [16]	IoT	JSON
W3.org [17]	WoT	JSON

2.4 Komunikácia

Základnou myšlienkou celého ekosystému je pripojenie zariadenia do Internetu s možnosťou komunikácie s ním z ktoréhokoľvek miesta na svete. Komunikácia zariadení v sieti môže prebiehať na rôznych úrovniach z podlahu zúčastnených strán. Z toho dôvodu ju môžeme rozdeliť do viacerých skupín:

- zariadenie – aplikácia,
- aplikácia – zariadenie,
- zariadenie – zariadenie,
- aplikácia – aplikácia / interoperabilita,
- aplikácia – používateľ.



Obr. 2 IoT ekosystém

Pre potreby vzájomnej komunikácie je využívané široké spektrum technológií ako môžeme vidieť v nasledujúcej tabuľke.

Tab. 2 Komunikačné kanály IoT zariadení

Technológia	Šírka pásma	Dosah	Spotreba	Cena
5G	1 - 2 Gbps	niekoľko km	vysoká	vysoká
2G/3G	10 Mbps	niekoľko km	vysoká	vysoká
Bluetooth/BLE	1, 2, 3 Mbps	~ 100 m	nízka	nízka
802.15.4	40, 250 kbps		nízka	nízka
LoRa	< 50 kbps	~ 5 m	nízka	stredná
LTE cat 0/1	1 – 10 Mbps	niekoľko km	stredná	vysoká
NB-IoT	0,1 – 10 Mbps	niekoľko km	stredná	vysoká
SigFox	< 1 kbps	niekoľko km	nízka	stredná
Weightless	0,1 – 24 Mbps	niekoľko km	nízka	nízka
Wi-Fi	0,1 – 54 Mbps	~ 100 m	stredná	nízka
WirelessHART	250 – kbps	~ 100 m	stredná	stredná
ZigBee	250 – kbps	100 – 150 m	nízka	stredná

Tabuľka poskytuje informácie o šírke prenosového pásme a dosahu tej ktorej technológie. Zároveň tu vidíme aké sú energetické požiadavky zariadení a v akej cenovej hladine sa pohybuje.

2.5 Šírka pásma

Šírka pásma udáva prenosovú kapacitu linky. V prípade 5G siete môže teoreticky prenosová kapacite siete dosiahnuť až 20 Gbps s oneskorením do 1 milisekundy [18]. Reálne sa rýchlosť v týchto sieťach pohybuje na úrovni 2 Gbps. Uvedená šírka pásma dovoľuje prenos veľkého objeme dát pri minimálnom oneskorení v komunikácii. Na opačnej strane spektra sa nachádza technológia SigFox so šírkou pásma do 50 kbps [19].

2.6 Architektúra

Dáta sú na svojej ceste smerované do aplikácie, kde sú následne spracované. V závislosti od poskytovanej služby môže byť aplikácia prevádzkovaná na rôznych typoch architektúry. Voľba architektúry riešenia má výrazný dopad na dátové toky. V praxi sa môžeme stretnúť s tromi základnými typmi architektúry:

- centralizovaná,
- decentralizovaná,
- distribuovaná.

3 Cieľ dizertačnej práce

Cieľom práce je návrh algoritmu redukujúceho množstvo prenášaných dát, ktorý zohľadňuje špecifiká zariadení Internetu vecí. Kľúčovú úlohu pri návrhu algoritmu zohrávajú hardvérové ako aj energetické obmedzenia zariadení. V práci vychádzame z predpokladu, že väčšina zariadení je a prípadne bude napájaná z batérie s obmedzenou kapacitou. Preto okrem primárneho cieľa redukcie objemu prenášaných dát sústredíme pozornosť na energetickú náročnosť algoritmu.

Vychádzajúc z analýzy spracovania dát na strane zariadenia, aby sme dosiahli požadovaný cieľ, zameriame pozornosť na dve oblasti súvisiace so spracovaním a prenosom dát:

- kompresia dát,
- šifrovanie dát.

3.1 Metodika práce

Dosiahnutie požadovaných cieľov realizujeme metódou simulácie procesu komunikácie zariadenia s aplikáciou. Simulácia procesu zahŕňa:

- spracovanie dát na strane zariadenia,
- prenos dát do aplikácie,
- spracovanie dát na strane aplikácie.

Simulátor je navrhnutý ako webová aplikácia s použitím platformovo nezávislej open source konfigurácie / zostavy:

- Apache,
- PHP,
- MySQL / MariaDB.

Simulácia pracuje s dvomi typmi dát:

- fiktívne IoT zariadenie – prezentuje jednoduchý spínač. Správy generované týmto zariadením použijeme v procese simulácie účinnosti štandardných kompresných algoritmov,
- dátová štruktúra IoT zariadenia SIEA [20] – predstavuje monitorovacie zariadenie zbierajúce informácie o energetickej spotrebe. Tento typ zariadenia použijeme pri návrhu nového komprimačného algoritmu s využitím UI a SU.

4 Dosiahnuté výsledky

Cieľom dizertačnej práce bol návrh algoritmov, umožňujúcich redukovať objem dát prenášaných v prostredí Internetu vecí. Aby sme dosiahli požadovaný cieľ práce, museli sme navrhnúť nové, inovatívne riešenie. Z toho dôvodu sme podrobili dôkladnej analýze proces spracovania dát na strane zariadenia ako aj aplikácie. Pozornosť sme sústredili aj na komunikáciu medzi zariadením a aplikáciou. Výsledky analýz určili naše smerovanie. Pozornosť sme sústredili na tri oblasti:

1. elimináciu SSL/TLS protokolu z procesu komunikácie,
2. šifrovanie dát,
3. kompresiu dát.

Navrhnuté riešenie je realizované metódou softvérovej simulácie. Aby sme dokázali porovnať dosiahnuté výsledky v prvom kroku sme simulovali úspešnosť používaných spôsobov kompresie dát v prípade krátkych správ typických pre Internet veci.

Prácu môžeme rozdeliť na dve časti. V prvej, prípravnej fáze, sme si pripravili referenčné dáta, zatiaľ čo v druhej hlavnej časti práce sme sa plne venovali návrhu nového algoritmu.

4.1 Kompresia dát štandardnými kompresnými algoritmami

Na kompresiu dát sme použili externé programy ako aj interné knižnice PHP. Pre účely testovania komprimačných algoritmov sme vybrali 3 najrozšírenejšie programy určené pre operačný systémom Windows za posledných 5 rokov. Voľba programov vychádzala z viacerých nezávislých hodnotení komprimačných programov

Simuláciu sme realizovali v základnom nastavení jednotlivých komprimačných programov bez optimalizácie kompresie s ohľadom na dosiahnutie maximálnej úrovne kompresie dát. Pre potreby simulácie sme definovali 10 IoT zariadení. Každé zariadenie malo predefinovaný spôsob správania sa počas dňa.

Simulácia prebiehala v 2 režimoch.

- odosielanie dát v pravidelných intervaloch,
    - kompresia každej správy samostatne,
    - agregácia správ do jeden, a jej následná kompresia,
- odosielanie dát iba v prípade zmeny.

Výsledky simulácie sme zhrnuli do tabuliek Tab. 3 – Tab. 5. Tabuľky prezentujú výsledky pri rôznych podmienkach komunikácie domácnosti so službou za časové obdobie 1 hodiny. Dĺžka správy je v celej práci uvádzaná v bajtoch.

- Tab. 3 – správa každého zariadenia sa odosiela samostatne
- Tab. 4 - odosiela sa jedna správa za všetky zariadenia
- Tab. 5 - prezentuje situáciu v prípade, ak odosielame správy iba v prípade zmeny stavu zariadenia

Tab. 3 Jedna správa za zariadenie každú minútu

Popis	Originál	Externé programy			Interné knižnice	
	JSON	WinRar	7-zip	PeaZip	gzip	bzip2
Počet správ	600	600	600	600	600	600
Celková dĺžka	75900	139453	159797	175220	63746	63783
Priemerná dĺžka	126,50	232,42	266,33	292,03	106,24	106,30
Kompresia	100%	184%	211%	231%	84%	84%

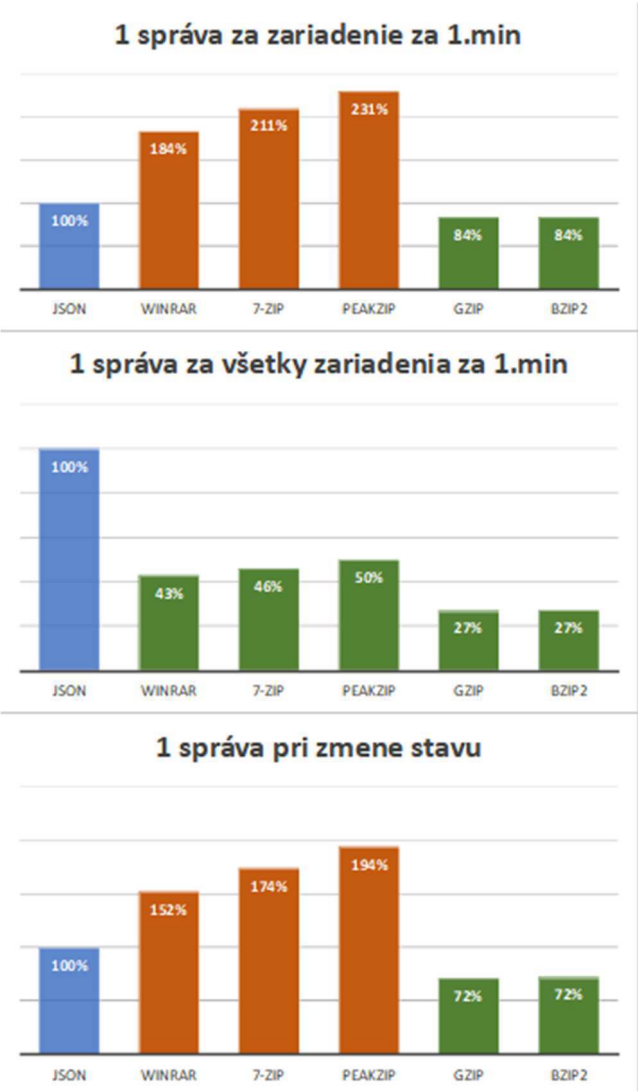
Tab. 4 Jedna správa za všetkých 10 zariadení každú minútu

Popis	Originál	Externé programy			Interné knižnice	
	JSON	WinRar	7-zip	PeaZip	gzip	bzip2
Počet správ	60	60	60	60	60	60
Celková dĺžka	54874	23434	25160	27272	14722	14786
Priemerná dĺžka	914,57	390,57	419,33	454,53	245,37	246,43
Kompresia	100%	43%	46%	50%	27%	27%

Tab. 5 Jedna spoločná správa v prípade zmeny stavu zariadenia

Popis	Originál	Externé programy			Interné knižnice	
	JSON	WinRar	7-zip	PeaZip	gzip	bzip2
Počet správ	26	26	26	26	26	26
Celková dĺžka	54874	23434	25160	27272	14722	14786
Priemerná dĺžka	4328,00	6593,00	7546,00	8406,00	3100,00	3124,00
Kompresia	100%	152%	174%	194%	72%	72%

Výsledky simulácie potvrdili očakávania, že nasadenie štandardných komprimačných algoritmov pri spracovaní krátkych správ nemá opodstatnenie. Pre lepšiu názornosť ich prezentujeme aj v grafickej podobe. Pri použití externých programov, na základe výsledkov simulácie môžeme povedať, že k reálnej úspore v objeme prenášaných dát prichádza iba v prípade agregácii viacerých správ do jednej. Priemerná dĺžka, nekomprimovanej správy je takmer 1 kilobajt. V tomto prípade je veľkosť prenášanej správy na úrovni menej ako 50 % pôvodnej veľkosti. V ostatných prípadoch simulácie veľkosť výslednej správy vzrástla.



Obr. 3 Porovnanie výsledkov simulácie

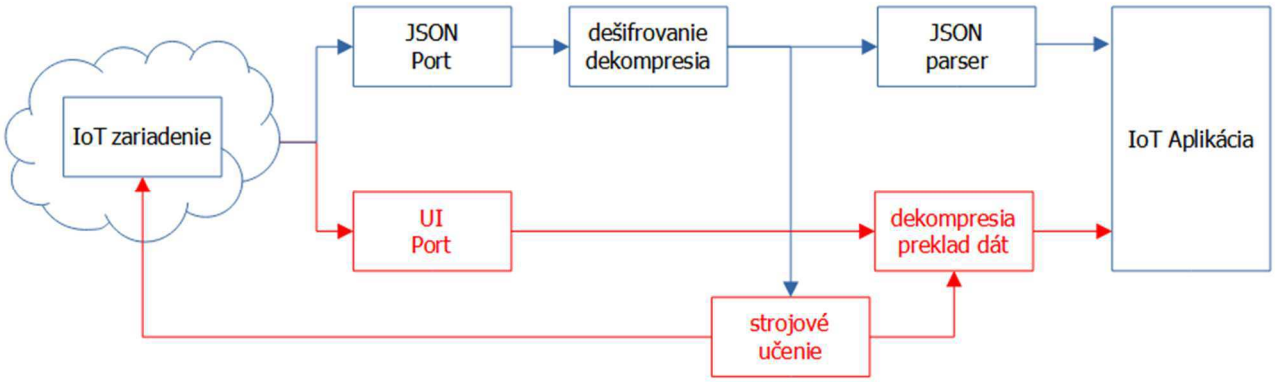
V prípade práce s internými knižnicami boli dosiahnuté výrazne lepšie výsledky. Vo všetkých prípadoch je veľkosť výslednej správy menšia ako veľkosť pôvodne správy. Podobne ako pri použití externých programov aj pri použití interných knižníc sú najlepšie výsledky v prípade, keď sú všetky správy agregované do jednej sumárnej správy a následne je táto správa komprimovaná. Veľkosť výslednej, komprimovanej správy dosahuje cca 25% pôvodnej veľkosti.

Výsledky simulácie použitia štandardných metód kompresie na IoT zariadeniach potvrdzujú, že ich nasadenie v prípade veľmi jednoduchých senzorov a zariadení stráca opodstatnenie. Dôvod neúspešnosti kompresie krátkych správ má pôvod v skutočnosti, že každá správa obsahuje slovník, ktorý tvorí jej významnú časť. Účinnosť existujúcich algoritmov rastie úmerne s veľkosťou správy. Zlúčením podobných správ do jednej je tento efekt ešte výraznejší. Podiel slovníka na celkovú veľkosť správy klesá z dôvodu opakujúcich sa textových reťazcov v komprimovanej správe. Tento trend potvrdzujú simulované spôsoby kompresie.

4.2 Kompresia dát s využitím strojového učenia

Navrhnutá koncepcia kompresie dát s využitím strojového učenia ML/SU presúva proces kompresie dát zo zariadenia na stranu servera, kde disponujeme dostatočným výpočtovým výkonom a nie je nevyhnutné obmedzovať sa ani po energetickej stránke.

Spôsob implementácie navrhovaného riešenia je zachytený na Obr. 4. Pri návrhu riešenia sme si položili požiadavku, že nové riešenie nesmie ohroziť ani obmedziť činnosť existujúceho riešenia.



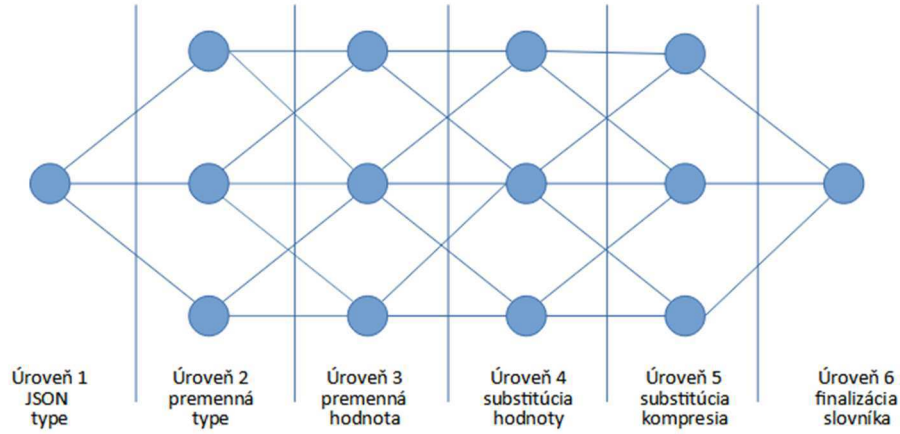
Obr. 4 Implementácia navrhovaného riešenia

V práci sme venovali pozornosť modulu strojového učenia. Aj keď sme aktivity súvisiace s kompresiou dát presunuli zo zariadenia na vzdialený server, kompresia prebieha rokmi overeným spôsobom – substitúciou pôvodných dát reťazcami znakov zo slovníka. Vytvorenie slovníka je v našom prípade nahradené algoritmom strojového učenia [21].

Proces učenia prebieha v režime:

- učenie bez učiteľa,
- učenie s učiteľom.

Proces strojového učenia prebieha v niekoľkých etapách. Jeho cieľom je vytvorenie komprimačného, substitučného slovníka, ktorý nahradí pôvodnú správu jej komprimovanou verziou.



Obr. 5 Priebeh viacúrovňového učiaceho sa procesu

Požadovaný cieľ je možné dosiahnuť viacúrovňovým procesom učenia. Učenie prebieha v niekoľkých fázach podľa nasledujúceho scenára:

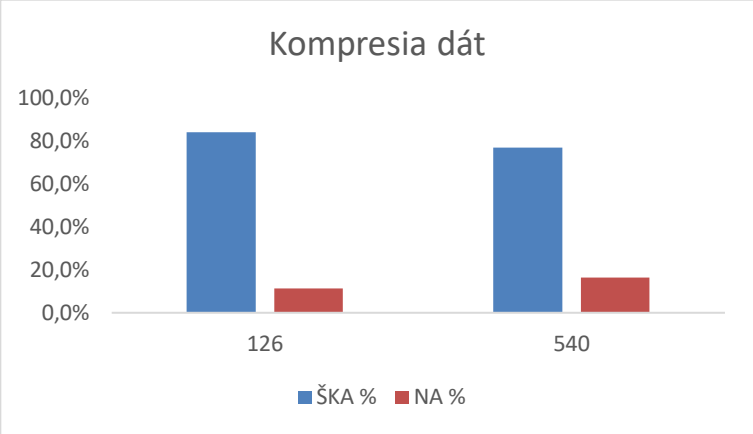
- identifikácia typu premennej na základe JSON definície (reťazec, číslo, ...),
- identifikácie typu premennej na základe obsahu (dátum, čas, celé číslo, číslo vo vedeckom formáte, ...),
- identifikácie hodnôt premennej (preddefinované hodnoty, dynamicky sa meniace hodnoty, 0 – 100 ...),
- definovanie spôsobu substitúcie (),
- definovanie finálnej verzie substitúcie,
- definovanie finálneho slovníka.

Ako sme uviedli v kapitole 4.1. štandardné kompresné algoritmy nie sú príliš účinné v prípade kompresie krátkych správ. Nami navrhnutý algoritmus tento problém eliminuje. V Tab. 6 porovnávame výsledky kompresie štandardnými algoritmami a výsledky dosiahnuté kompresiou navrhnutým algoritmom.

Tab. 6 Porovnanie účinnosti kompresie štandardného a navrhnutého algoritmu

Správa	126	540
ŠKA	106	415
NA	14	88
ŠKA %	84,1%	76,9%
NA %	11,1%	16,3%

Prvý riadok tabuľky obsahuje priemernú dĺžku nekomprimovanej správy v bajtoch. Prvý riadok v 2 a 3 stĺpci udávajú priemernú dĺžku generovanej správy v dátovom formáte JSON. Druhý stĺpec uvádza hodnotu pre správu fiktívneho zariadenia. V treťom stĺpci je priemerná veľkosť správy SIEA. ***ŠKA*** prezentuje výsledky dosiahnuté štandardnými algoritmami. ***NA*** zodpovedá výsledkom dosiahnutým novým navrhnutým algoritmom.



Obr. 6 Porovnanie účinnosti kompresie štandardného a navrhnutého algoritmu

Navrhnutým komprimačným algoritmom sme dosiahli i napriek tomu, že sme komprimovali krátke správy, pokles ich veľkosti na približne 15 - 20 % pôvodnej hodnoty. Dosiahnuté výsledky v grafickej podobe sú na Obr. 6.

Pretože sme z procesu spracovania dát na strane zariadenia z dôvodu energetických úspor vypustili šifrovanie dát a zároveň sme eliminovali z procesu komunikácie SSL/TLS protokol, bolo úlohou komprimačného algoritmu vygenerovať dáta vo formáte vhodnej pre šifrovanie nami navrhnutým algoritmom. Algoritmus kompresie a predprípravy dát sme nazvali Alias-Shaker.

4.3 Eliminácia SSL/TLS protokolu z procesu komunikácie

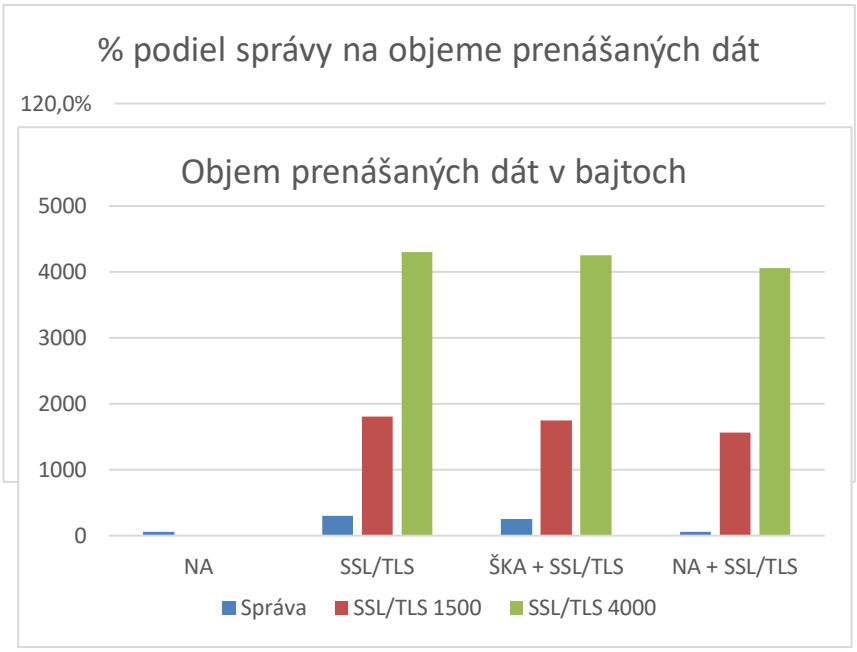
Analýzou procesu spracovania dát na strane zariadenia sme identifikovali použitie SSL/TLS ako nerentabilné. Eliminácia tohto protokolu z procesu komunikácie predstavuje majoritnú úsporu v objeme prenášaných dát. Podiel veľkosti prenášanej správy k celkovému objemu prenášaných dát je v Tab. 7.

Tab. 7 Pomer dát zariadenia k celkovému objemu prenesených dát

	SSL/TLS		**ŠA + SSL/TLS**		**NA + SSL/TLS**		**NA**
Dĺžka správy	300		250		60		60
SSL/TLS	1500	4000	1500	4000	1500	4000	
Odoslané	1800	4300	1750	4250	1560	4060	60
Podiel	16,7%	7,0%	14,3%	5,9%	3,8%	1,5%	100,0%

Výsledky v grafickej podobe sú prezentované na Obr. 8 a Obr. 9. Porovnanie rôznych scenárov komunikácie sme realizovali pre prípad, že na vybudovanie SSL/TLS spojenia bolo potrebné preniesť 1500 resp. 4000 bajtov. V oboch prípadoch porovnávame 4 scenáre komunikácie zariadenia so serverom:

1. ***NA*** – správu komprimujeme navrhnutým algoritmom, komunikácia prebieha bez použitia SSL/TLS protokolu,
2. ***SSL/TLS*** – správu nekomprimujeme, odosielame ju cez šifrované spojenie SSL/TLS,
3. ***ŠKA + SSL/TLS*** – správu komprimujeme štandardným algoritmom, odosielame ju cez šifrované spojenie SSL/TLS,
4. ***NA + SSL/TLS*** – správu komprimujeme navrhnutým algoritmom, odosielame ju cez šifrované spojenie SSL/TLS



Obr. 7 Objem prenášaných dát v bajtoch

Obr. 8 zobrazuje percentuálny podiel správy v celkovom objeme prenesených dát. Na porovnanie Obr. 9 znázorňuje objem prenesených dát v bajtoch. Ako môžeme vidieť, čím je odosielaná spáva kratšia, tým menší je jej podiel na celkovom objeme prenesených dát. Vychádzajúc z tohto poznatku prídeme k záveru, že kompresia krátkych správ pred odoslaním, pri komunikácii s použitím SSL/TLS protokolu, stráca opodstatnenie. Kompresiou dát iba zvyšujeme spotrebu energie na strane zariadenia.

5 Prínos dizertačnej práce

Z vedeckého hľadiska vnášame nový pohľad na spracovanie dát z kategórie BIG DATA. V riešení využívame možnosti moderných dnešných technológií ako aj architektúry. Počítačovou simuláciou sme overili funkčnosť nasadenia navrhnutých algoritmov. Výkonovo náročné operácie presúvame zo zariadenia tam, kde je tento výkon k dispozícii – na server. Nasadenie strojového učenia a umelej inteligencie môže v budúcnosti priniesť výrazné vylepšenia v procese kompresie ako aj zabezpečenia dát. Zároveň nechávame otvorenú možnosť pracovať s pôvodným dátovým formátom JSON. To dovoľuje rýchly vývoj a testovanie nových zariadení a zároveň „odbremení“ vývojárov od problematiky zabezpečenia prenášaných dát. Tejto úlohy sa zhostia navrhnuté algoritmy.

Na dosiahnutie cieľa sme navrhli:

- komprimačný algoritmus Alias-Shaker, využívajúci prvky strojového učenia, orientovaný na kompresiu krátkych správ
- šifrovací algoritmus na princípe Lightweight Cryptography

Z technického hľadiska prináša navrhnuté riešenie výraznú úsporu v objeme prenášaných dát na jednej strane a zároveň znižuje energetickú náročnosť riešenia. Redukcia objemu prenášaných dát umožňuje pripojenie väčšieho počtu zariadení do siete, a tým lepšie využitie prenosového pásma. Zároveň s tým úzko súvisí energetická spotreba. Menší objem prenesených dát sa rovná nižšej spotrebe energie. Výraznú úsporu energie môžeme očakávať v procese spracovania dát. Náhradou časovo a energeticky náročných algoritmov ekvivalentnými riešeniami príde z dlhodobého hľadiska k výraznej úspore v spotrebe energie. Treba si uvedomiť, že v budúcnosti očakávané milióny pripojených zariadení budú klásť vysoké požiadavky na priepustnosť siete ako aj rýchlosť odozvy aplikácie.

Z dlhodobého hľadiska môžeme považovať za benefity riešenia:

- zlepšenia využitia šírky pásma prenosových trás
- energetické úspory

6 Záver

V práci sme sústredili pozornosť na redukciu množstva dát prenášaných v ekosystéme IoT. Na dosiahnutie cieľa sme v súlade s výzvou IEEE z roku 2014 opustili zaužívané spôsoby komunikácie a spracovania dát a rozhodli sa ísť úplne novou cestou. Nepriaznivá situácia znemožnila prístup do laboratória, kde by sme mohli navrhnuté riešenie overiť na reálnych zariadeniach. Preto sme riešenie simulovali na počítači. Výsledky simulácií potvrdzujú správnosť nášho rozhodnutia a to od základov zmeniť spôsob spracovania dát a spôsob komunikácie.

Najvýraznejší dopad na redukciu objemu prenášaných dát má vyradenie SSL/TLS protokolu z komunikačného reťazca. Objem prenášaných dát sa znížil na desatinu pôvodnej veľkosti. V extrémnych prípadoch to môže byť výrazne viac (Obr. 6 a Obr. 7).

Navrhnutým komprimačným algoritmom Alias – Shaker sme dosiahli i napriek tomu, že sme komprimovali krátke správy, pokles ich veľkosti na približne 15 - 20 % pôvodnej hodnoty. (Obr. 6)

Zmenou spôsobu spracovania dát, komprimačných a šifrovacích algoritmov, môžeme povedať, že sa nám podarilo znížiť energetickú náročnosť. Reálny dopad na energetickú spotrebu nevieme potvrdiť a ani to nebol cieľ tejto práce. Ak hovoríme o energetickej úspore vychádzame z princípu činnosti algoritmov. Komplikované kompresné a šifrovacie algoritmy sme nahradili jednoduchými postupmi.

Simulácia opísaného riešenia potvrdzuje výraznú redukcia objemu prenášaných dát. Ako bolo uvedené v zadaní práce, mali sme sa prioritne sústrediť na Internet vecí. Navrhnuté riešenie reaguje na špecifiká tohto segmentu. Preto si navrhnuté algoritmy budú ťažko hľadať uplatnenie v iných oblastiach.

V práci prezentujeme nový prístup k spôsobu spracovania dát Internetu vecí ako k tomu vyzývala IEEE už v roku 2015. Doteraz Internet vecí čerpal skúsenosti zo sveta informačných technológií. Je čas, aby sa začal uberať vlastnou cestu.

7 Zoznam použitej literatúry

[1] G. Press, "A Very Short History Of The Internet Of Things," 18 Jún 2014. [Online]. Available: https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/?sh=67e8286710de#616afd7e10de/. [Accessed 28 Máj 2022]

[2] A. Pal, H. K. Rath, S. Shailendra a A. Bhattacharyya, „IoT Standardization: The Road Ahead," August 2018. [Online]. Available: http://dx.doi.org/10.5772/intechopen.75137. [Accessed 28 Máj 2022]

[3] J. Teicher, „The little-known story of the first IoT device," 7 Február 2018. [Online]. Available: https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/. [Accessed 28 Máj 2022]

[4] R. Minerva, A. Biru a D. Rotondi, „Towards a definition of the Internet of Things (IoT)," August 2014. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. [Accessed 28 Máj 2022]

[5] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo a M. González-López, „A Review on Internet of Things for Defense and Public Safety," Sensors, 2016. [Online]. Available: https://doi.org/10.3390/s16101644. [Accessed 28 Máj 2022]

[6] P. Thakudi, „RFID and the IOT," September 2017. [Online]. Available: https://www.itweb.co.za/content/2JN1gPvOkbovjL6m. [Accessed 28 Máj 2022]

[7] S. Brien, P. Linda a R. Sharon, „Industrial internet of things (IIoT)," [Online]. Available: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT. [Accessed 28 Máj 2022]

[8] cisco.com, „The Internet of Everything Global Public Sector Economic Analysis," 2013. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/business-

insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf. [Accessed 28 Máj 2022]

[9] webofthings.org, „Specifications and Standards," 2007. [Online]. Available: https://webofthings.org/standards/. [Accessed 28 Máj 2022]

[10] w3.org, „W3C Web of Things," [Online]. Available: https://www.w3.org/WoT/. [Accessed 28 Máj 2022]

[11] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi a M. Usman, „Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," November 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3417987. [Accessed 28 Máj 2022]

[12] amazon.com, „IoT services for industrial, consumer, and commercial solutions.," [Online]. Available: https://aws.amazon.com/iot/. [Accessed 28 Máj 2022]

[13] google.com, „Google's Internet of Things Solutions.," [Online]. Available: https://developers.google.com/iot/. [Accessed 28 Máj 2022]

[14] mozilla.org, „Web of Things.," [Online]. Available: https://iot.mozilla.org/about/. [Accessed 28 Máj 2022]

[15] onem2m.org, „Standards for M2M and the Internet of Things.," [Online]. Available: http://onem2m.org/. [Accessed 28 Máj 2022]

[16] opengroup.org, „Open Data Format (O-DF), an Open Group Internet of Things (IoT) Standard.," [Online]. Available: http://www.opengroup.org/iot/odf/. [Accessed 28 Máj 2022]

[17] w3.org, „Web of Things at W3C.," [Online]. Available: https://www.w3.org/WoT/. [Accessed 28 Máj 2022]

[18] P. Nikolich, C.-L. I, J. Korhonen, R. Marks, B. Tye, G. Li, J. Ni a S. Zhang, „Standards for 5G and Beyond: Their Use Cases and Applications," 2017. [Online]. Available:

https://futurenetworks.ieee.org/tech-focus/june-2017/standards-for-5g-and-beyond. [Accessed 28 Máj 2022]

[19] sigfox.com, „Sigfox technology," [Online]. Available: https://www.sigfox.com/en/what-sigfox/technology. [Accessed 28 Máj 2022]

[20] Slovenská Informačná a Energetická Agentúra, „SIEA API Monitoring system of energy efficiency," [Online]. Available: https://documenter.getpostman.com/view/2447371/SzRuWr8t?version=latest. [Accessed 28 Máj 2022]

[21] P. Mariani a M. Bieliková, „Proces učenia ako zdroj transferu poznania: strojové učenie verzus ľudské učenie," 2017, pp. 94-99.

[22] E. Guberović, F. Krišto, P. Krivić a I. Čavrak, „Assessing compression algorithms on IoT sensor nodes," 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8756995. [Accessed 28 Máj 2022]

[23] N. Rishe, O. Wolfson, B. Wongsaroj, D. Small, M. Alarcon, N. Lorenzo, R. Koller, S. Kundu, S. Graham, K. Alexander a M. Adjouadi, „Schema Based XML Compression," rev. Schema Based XML Compression, International Conference on Enterprice Information System and Web Technologies (EISWT-07), 2007.

[24] code.google.com, „Google Code Archive - Long-term storage for Google Code Project Hosting.," 2020. [Online]. Available: https://code.google.com/archive/p/htmlcompressor/. [Accessed 28 Máj 2022]

[25] atombeamtech.com, „Dramatically Reduce IoT And Machine Data in Real Time Over," [Online]. Available: https://atombeamtech.com/. [Accessed 28 Máj 2022]

[26] R. G. Kammer, DATA ENCRYPTION STANDARD (DES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 1999.

[27] iso.org, ISO/IEC 18033-3:2010 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers, 2010.

[28] G. Mustafa, R. Ashraf, M. A. Mirza a A. J. Muhammad, „A review of data security and cryptographic techniques in IoT based devices," Jún 2018. [Online]. Available: https://doi.org/10.1145/3231053.3231100. [Accessed 28 Máj 2022]

[29] A. Nilupulee, W. J. B. Gunathilake a R. Asif, „Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2020.3044526.

[30] ietf.org, „The Secure Sockets Layer (SSL) Protocol Version 3.0," August 2011. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6101/. [Accessed 28 Máj 2022]

[31] S. Mauchline, M. Teerlink a S. Manohar, „Die Zukunft von IoT," 2019. [Online]. Available: https://news.sap.com/germany/2019/10/iot-chance-moeglichkeiten/. [Accessed 30 Máj 2022]

[32] J. PRISTACH, SYSTÉM INTELIGENTNÉHO RIADENIA V PROSTREDÍ IoT., Bratislava, 2017.

8 Publikačná činnosť autora

AFD SOKOL, Ivan: 5G network is behind the door. Proceedings of ELITECH ’19 21th Conference of Doctoral Students 29 May 2019, FEI STU, Bratislava, Slovakia https://app.crepc.sk/?fn=detailBiblioForm&sid=4D4167EFBDF6647E39C2C3831D

ADN SOKOL, Ivan - HUBINSKÝ, Peter. Internet of things - nonstandard data compression. In Journal of Electrical Engineering. Vol. 71, No. 4 (2020), s. 281-285. ISSN 1335-3632 (2020: 0.647 - IF, Q4 - JCR Best Q, 0.191 - SJR, Q3 - SJR Best Q). V databáze: DOI: 10.2478/jee-2020–0038 ; WOS: 000574676300006 ; SCOPUS: 2-s2.0-85093067960.
https://app.crepc.sk/?fn=detailBiblioForm&sid=AB2F48E8C57E5DFBA47D7BA9FC

Citované v:

Liu, K., Zhong, Y., Chen, J., Zhu, Z. (2021): Data compression about Internet of Things based on HNBJSON In Nanjing Youdian Daxue Xuebao (Ziran Kexue Ban)/Journal of Nanjing University of Posts and Telecommunications (Natural Science), 41(6), pp. 29-34

Kahdim, A. N., & Manaa, M. E. (2022). Design an efficient IoT Data Compression for Healthcare Applications. Bulletin of Electrical Engineering and Informatics, 11(3).

ADC SOKOL, Ivan - HUBINSKÝ, Peter - CHOVANEC, Ľuboš. Lightweight cryptography for the encryption of data communication of IoT devices. In Electronics. Vol. 10, iss. 21 (2021), Art. no. 2567 [9] s. ISSN 2079-9292 (2020: 2.397 - IF, Q3 - JCR Best Q, 0.360 - SJR, Q2 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85117354530 ; WOS: 000719419300001 ; CC: 000719419300001 ; DOI: 10.3390/electronics10212567.
https://app.crepc.sk/?fn=detailBiblioForm&sid=CA938D5BF78F2454F94F7A71BC

Citované v:

Mohammed, A.H., Shibeeb, A.K., Ahmed, M.H. (2022): Image Cryptosystem for IoT Devices Using 2-D Zaslavsky Chaotic Map In International Journal of Intelligent Engineering and Systems, 15(2), pp. 543-553

Popularizačné články

I. Sokol, " Analýza: Internet vecí (Internet of things - IoT) a BIG DATA", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Analyza--Internet-veci--Internet-of-things---IoT--a-BIG-DATA

I. Sokol, "Mám elektromobil. Ako ďaleko sa s ním môžem vybrať?", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Mam-elektromobil--Ako-daleko-sa-s-nim-mozem-vybrat

I. Sokol, "Elektromobil a fyzika alebo koľko energie si vyžaduje pohyb", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Elektromobil-a-fyzika-alebo-kolko-energie-si-vyzaduje-pohyb

I. Sokol, "Analýza: elektromobil a energetika SR. Dokáže Slovensko utiahnuť prechod na elektromobily?", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Analyza--elektromobil-a-energetika-SR--Dokaze-Slovensko-utiahnut-prechod-na-elektromobily

I. Sokol, "Keď fyzika nepustí: Ultrarýchle nabíjanie elektromobilov – mýty a realita", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Ked-fyzika-nepusti--ultrarychle-nabijanie-elektromobilov-myty-a-realita

I. Sokol, "Úvaha: Dopravná zápcha – nočná mora elektromobilov", *IT News*, 2018. [Online]. Dostupné na internete: https://www.nextech.sk/a/Uvaha--Dopravna-zapcha--E2-80-93-nocna-mora-elektromobilov