TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Cílená distribuce informací

Disertační práce

Studijní program: P6209 – Systémové inženýrství a informatika
Studijní obor: 6209V003 – Ekonomická informatika

Autor práce: **Mgr. Tomáš Žižka**
Vedoucí práce: doc. Ing. Jan Skrbek, Dr.

Liberec 2018

Prohlášení

Byl jsem seznámen s tím, že na mou disertační práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé disertační práce pro vnitřní potřebu TUL.

Užiji-li disertační práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Disertační práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé disertační práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Anotace a klíčová slova

Předkládaná disertační práce se zaměřuje na problematiku cílené distribuce informací v průběhu mimořádných a krizových situací, při nichž mohou být ohroženy lidské životy, infrastruktura, ekonomika apod. Právě v těchto případech je důležité zprostředkovat správné informace ve správný čas a na správné místo. Konceptuální řešení popisované v této práci je založeno na faktu, že důležitá informace by měla být cílena pouze tam, kde je jí v danou chvíli třeba. K tomu lze využít principu pozičního šifrování, pomocí kterého lze zajistit, aby zprávu odeslanou prostřednictvím systému včasného varování bylo možné správně dešifrovat pouze v určité předem vymezené oblasti.

S ohledem na uvedené vymezení problematiky je hlavním cílem práce návrh konceptuálního řešení pro realizaci systému, který bude schopen distribuovat varovné informace do určité oblasti s atributem exkluzivity. Pro dosažení hlavního cíle práce byly stanoveny následující dílčí cíle:

1. Popsat současný stav v oblasti systémů včasného varování obyvatel v České republice i ve světě.
2. Stanovit požadavky na efektivní systém včasného varování, včetně požadavků na dílčí subsystémy, mezi které patří i komponenta zajišťující šifrování informací.
3. Navrhnout modelové situace vycházející z aktuálních hrozeb.
4. Stanovit vhodné distribuční kanály (rozhlasové vysílání, sítě GSM, Internet apod.)
5. Navrhnout konceptuální řešení pro včasnou distribuci pozičně šifrovaných varovných informací:
   - Porovnat šifrovací algoritmy vhodné pro dosažení atributu exkluzivity informace v předem vymezené geografické lokalitě.
   - Navrhnout algoritmus vymezení oblasti pro příjem varovné zprávy s atributem exkluzivity.

Klíčová slova: krizová komunikace, mimořádná událost, kryptografie, šifrování informací, symetrická kryptografie, AES.

Annotation and keywords

Targeted Distribution of Information

This dissertation theses focuses on the issue of targeted information distribution during the emergency and crisis situations where human lives, infrastructure, economy, etc. can be at risk. It is in these cases where it is important to convey the right information at the right time and in the right place. The conceptual solution described in this paper is based on the fact that important information should be targeted only in locations where it is needed at that exact moment. This can be achieved by implementing the principle of positional encryption, which ensures that a message sent through an early warning system can be properly decrypted only in a predefined area.

In view of the above-mentioned definition of the problematic, the main goal of the thesis is the proposition of a conceptual solution of a system that would be able to distribute the warning information in a certain area with an exclusivity attribute. In order to achieve the main goal of the paper, the following partial objectives were set:

1. Describe the current situation of early warning systems of the population in the Czech Republic and in the world.
2. Set requirements for an effective early warning system, including requirements for sub-systems, including a component encryption.
3. Design model scenarios based on current threats.
4. Establish appropriate distribution channels (radio broadcasting, GSM networks, Internet, etc.)
5. Design a conceptual solution for the timely distribution of positionally encrypted warning information:
   - Compare cryptographic algorithms suitable for achieving an exclusivity information attribute in a predefined geographic location.
   - Suggest an area delimitation algorithm to receive a warning message with an exclusivity attribute.

Keywords: crisis communication, non-standard situations, cryptography, information encryption, symmetric cryptography, AES

Annotation und Schlüsselwörter

Gezielte Verteilung von Informationen

Die vorliegende Dissertationsarbeit konzentriert sich auf die Frage der gezielten Verbreitung von Informationen in Notfällen und Katastrophensituationen, in denen Menschenleben, Infrastruktur, Wirtschaft, etc. gefährdet werden kann. In diesen Fällen ist es wichtig, die richtigen Informationen zur richtigen Zeit und am richtigen Ort zu vermitteln. Die konzeptionelle Lösung, die in dieser Arbeit beschrieben wird, basiert auf der Tatsache, dass wichtige Informationen nur dort ausgerichtet werden sollten, wo sie zu einem bestimmten Zeitpunkt benötigt werden. Dies kann mit dem Prinzip der Positionsverschlüsselung geschehen, mit dem sichergestellt werden kann, dass eine durch das Frühwarnsystem gesendete Nachricht nur in einem bestimmten vordefinierten Bereich ordnungsgemäß entschlüsselt werden kann.

Im Hinblick auf diese Definition der Frage, das Hauptziel der These ist es, eine konzeptionelle Lösung für die Umsetzung eines Systems, das in der Lage, die Warnung Informationen an einen bestimmten Bereich mit einem Attribut der Exklusivität zu verteilen. Um das Hauptziel der Arbeit zu erreichen, wurden folgende Teilziele festgelegt:

1. Beschreibung der gegenwärtigen Situation im Bereich der Frühwarnsysteme der Bevölkerung in der Tschechischen Republik und der Welt.
2. Anforderungen für ein wirksames Frühwarnsystem ermitteln, einschließlich der Anforderungen für Subsysteme, die einige Komponente, die Informationsverschlüsselung bietet, enthalten.
3. Entwicklung Modellsituationen, die auf aktuellen Bedrohungen basieren.
4. Auswahl geeigneter Vertriebskanäle (Hörfunk, GSM-Netze, Internet usw.)
5. Vorschlag einer konzeptionellen Lösung für die rechtzeitige Verteilung von positionsverschlüsselten Warninformationen:
   - Kryptografische Algorithmen vergleichen, die für die Erzielung von Attribut-exklusiv Informationen in einem vordefinierten geographischen Standort geeignet sind.
   - Einen Algorithmus vorschlagen, um den Bereich für den Empfang einer Warnmeldung mit einem exklusiv Attribut zu begrenzen.

Schlüsselwörter: Krisenkommunikation, außergewöhnliches Ereignis, Kryptographie, Informationsverschlüsselung, symmetrische Kryptographie, AES.

Poděkování

Chtěl bych poděkovat svému vedoucímu disertační práce doc. Ing. Janu Skrbkovi, Dr. za odborné vedení, rady a pomoc při zpracování této práce.

Obsah

Seznam zkratek ____ *9*

Seznam obrázků ____ *10*

Seznam tabulek ____ *12*

Úvod ____ *13*

1 Cíle práce a výzkumné otázky ____ *15*

1.1 Východiska a formulace výzkumných otázek ____ **15**

1.1.1 Východiska disertační práce ____ 15

1.1.2 Výzkumné otázky ____ 16

1.2 Cíle práce ____ **16**

1.3 Použité metody ____ **17**

1.4 Struktura práce ____ **17**

1.5 Přínos práce ____ **18**

2 Vymezení základních pojmů a deskripce současného stavu ____ *19*

2.1 Vymezení základních pojmů ____ **19**

2.1.1 Rozdělení mimořádných událostí ____ 21

2.1.2 Krizové řízení ____ 22

2.1.3 Krizová komunikace ____ 24

2.2 Stávající systémy pro včasné varování obyvatel ____ **26**

2.2.1 Jednotný systém varování a vyrozumění (JSVV) ____ 26

2.2.2 Varovné informace distribuované prostřednictvím SMS zpráv ____ 28

2.2.3 Bezdrátový rozhlas ____ 29

2.2.4 Systém eCall ____ 30

2.2.5 KATWARN ____ 33

2.2.6 The Global Disaster Alert and Coordination System (GDACS) ____ 34

2.2.7 Indian Ocean Tsunami Warning and Mitigation System (IOTWS) ____ 36

2.2.8 Shrnutí ____ 37

3 Požadavky na efektivní systém včasného varování ____ *38*

3.1 Kritické zhodnocení stávajících systémů ____ **38**

3.2 Analýza požadavků ____ **40**

3.3 Radio-Help ____ **41**

3.3.1 Využití systému Radio-Help ____ 44

4 Modelové situace ____ *46*

4.1 Motivační aspekty pro návrh modelových situací ____ **46**

4.1.1 Hrozby současného terorismu ____ 48

4.2 Varování obyvatel před vstupem do nebezpečné oblasti ____ **49**

4.3 Cílená dezinformace směřovaná do epicentra nebezpečí ____ **51**

4.4 Řízená evakuace z ohrožené oblasti 52
4.4.1 Modelová situace – ohrožení vzniklé poškozením vodního díla 52
4.4.2 Modelová situace pro přímořské lokality 55

5 Poziční šifrování 58

5.1 Úvod do kryptografie 58
5.1.1 Základní kryptologické pojmy 58
5.1.2 Symetrické kryptografické systémy 59
5.1.3 Asymetrické kryptografické algoritmy 63
5.1.4 Bezpečnost kryptografických systémů 64
5.1.5 Matematické operace využívané v kryptografii 66

5.2 Princip pozičního šifrování 67

5.3 Aplikace pozičního šifrování 69

5.4 Aspekty systému pro pozičně šifrované vysílání informací 71
5.4.1 Operační centrum varovného systému 72
5.4.2 Uživatelský terminál 72
5.4.3 Přenosový kanál 73
5.4.4 Šifrovací algoritmus 76

6 Využití algoritmu AES pro šifrování varovné zprávy 79

6.1 Souřadnicový systém WGS84 79

6.2 Příklad šifrování varovné zprávy algoritmem AES 80
6.2.1 Přípravná fáze 81
6.2.2 Expanze klíče K_E 82
6.2.3 Šifrování zprávy Z 85

7 Návrh konceptuálního řešení 88

7.1 Vymezení oblasti pro příjem dešifrované varovné zprávy 88
7.1.1 Vymezení oblasti na základě předem definované přesnosti určení bodu 89

7.2 Konceptuální modely 99

8 Ekonomicko-implementační hledisko 102

8.1 Zavedení systému jako inovace v rámci používaného systému včasného varování 102

8.2 Postupně řízená evakuace a její ekonomické zhodnocení 103

Závěr 104

Seznam použité literatury 106

Přehled publikační činnosti autora 112

Příloha A: Substituční tabulka S-Box pro operaci SubBytes 115

Seznam zkratek

AES	*Advanced Encryption Standard*
ČRo	Český rozhlas
DAB	*Digital Audio Broadcasting*
GDACS	*Global Disaster Alert and Coordination System*
GIS	Geografický informační systém
GPS	*Global Positioning System*
GSM	Globální systém pro mobilní komunikaci
HZS ČR	Hasičský záchranný sbor České republiky
HZS LK	Hasičský záchranný sbor Libereckého kraje
IOTWS	*Indian Ocean Tsunami Warning and Mitigation System*
IZS	Integrovaný záchranný systém
JSVV	Jednotný systém varování a vyrozumění obyvatelstva
LBS	Lokálně kontextové služby (*Location based service)*
MU	Mimořádná událost
MVČR	Ministerstvo vnitra České republiky
NIST	*National Institute of Standards and Technology* (Americký Národní institut standardu a technologií)
ORP	Obec s rozšířenou působností
RH	Radio-Help
SVV	Systém včasného varování

Seznam obrázků

Obrázek 1: Průběh procesů krizového řízení 23

Obrázek 2: Průběh signálu všeobecné výstrahy, zkušebního tónu a požárního poplachu .. 26

Obrázek 3: Trend počtu sirén v ČR v letech 2012-2017 27

Obrázek 4: Počet dopravních nehod a úmrtí v ČR v letech 2009–2010 30

Obrázek 5: KATWARN – mapa pokrytí v Německu a sociální sítě Twitter 33

Obrázek 6: Princip systému GDACS 35

Obrázek 7: Blokové schéma osobního informačního terminálu systému Radio-Help 42

Obrázek 8: Blokové schéma začlenění systému Radio-Help do struktury HZS ČR 43

Obrázek 9: Model rychlého doručení varovných informací k řidičům 44

Obrázek 10: První modelová situace 50

Obrázek 11: Druhá modelová situace 51

Obrázek 12: Třetí modelová situace 54

Obrázek 13: Čtvrtá modelová situace 56

Obrázek 14: Základní klasifikace symetrických kryptografických systémů 60

Obrázek 15: Princip kaskádové šifry 61

Obrázek 16: Princip blokové iterované šifry při šifrování a dešifrování 62

Obrázek 17: Základní koncepce pozičního šifrování 68

Obrázek 18: Blokové schéma algoritmu pozičního šifrování 69

Obrázek 19: Blokové schéma obecného utajovacího kryptografického systému 71

Obrázek 20: Základní části systému pro pozičně šifrované vysílání informací 72

Obrázek 21: Uvažované přenosové kanály 73

Obrázek 22: Mapa pokrytí ČR systémem DAB+ (leden 2018) 75

Obrázek 23: Vymezení konkrétního zeměpisného bodu 79

Obrázek 24: Vymezení obdélníkové a kruhové oblasti pro příjem dešifrované zprávy 89

Obrázek 25: Vzdálenost mezi body odpovídající změně o jednu minutu 93

Obrázek 26: Vymezení oblasti pro příjem dešifrované zprávy 95

Obrázek 27: Vymezení prostoru střední velikosti 97

Obrázek 28: Vymezení dvou sousedních oblastí..... 98

Obrázek 29: Use case diagram 100

Obrázek 30: UML diagram aktivit – procesní logika systému..... 101

Seznam tabulek

Tabulka 1: Počet nehod v ČR a jejich následků v letech 2009–2017 30

Tabulka 2: Nehody a jejich následky, řešené Policií ČR pro jednotlivé měsíce roku 2017 31

Tabulka 3: Počet ztrát na životech způsobených jevem tsunami 37

Tabulka 4:Počet významných vodních děl v ČR 53

Tabulka 5: Základní logické operace používané v kryptografii 66

Tabulka 6: Přednosti a nedostatky komunikačního kanálu DAB+ 76

Tabulka 7: Přednosti a nedostatky kryptografického algoritmu AES 78

Tabulka 8: Rozdělení zprávy do bloků 81

Tabulka 9: Převod šifrovacího klíče a textu zprávy do hexadecimálního formátu 82

Tabulka 10: operace g(w[3]) – RotWord, SubBytes, Rcon 83

Tabulka 11: Příklad výpočtu prvního iteračního klíče 84

Tabulka 12: Iniciační šifra 85

Tabulka 13: operace SubBytes a ShiftRows 86

Tabulka 14: operace MixColumns obecný zápis 86

Tabulka 15: operace MixColumns pro referenční příklad 86

Tabulka 16: operace AddRoundKey 86

Tabulka 17: Komparace trigonometrických metod pro výpočet vzdálenosti dvou bodů ... 92

Tabulka 18: Výpočet vzdálenosti mezi „sousedními“ body pro různé úrovně přesnosti.... 94

Tabulka 19: Velikost vymezené oblasti pro různé úrovně přesnosti 95

Tabulka 20: Souřadnice bodů definující oblast pro příjem dešifrované zprávy..... 96

Tabulka 21: Vzdálenost mezi body, které tvoří oblast vymezenou pro příjem zprávy..... 98

Úvod

Zabezpečení rychlého přenosu relevantních informací v mimořádných situacích na potřebná místa bylo vždy důležité. Nicméně až v dnešním „moderním světě“ plném informačních technologií máme k dispozici pokročilé technické prostředky, které nám mohou pomoci k tomu, aby se klíčové informace dostaly včas na požadovaná místa. Avšak jak se ukázalo v nedávné minulosti, předávání potřebných, někdy i životně důležitých informací v krizových situacích (povodně v Libereckém kraji v roce 2010, únik nebezpečných kalů z hliníkárny na západě Maďarska v říjnu 2010, teroristické akce v Paříži v roce 2015, orkán Herwart v říjnu 2017 apod.) nebylo vždy efektivní nebo selhalo úplně.

Různé druhy katastrof, mimořádných událostí a nehod představují – bohužel – nedílnou součást každodenního života. Tyto situace ovlivňují život obyvatel na celém světě, a to buď nepřímo, nebo přímo v případech, kdy se stávají jejich – mnohdy na životě ohroženými – účastníky. Často v těchto případech dochází k tomu, že „potřebné“ informace jsou dostupné pouze pro obyvatele, kteří nejsou postiženi mimořádnou událostí přímo. Tato skupina se většinou o událostech dozvídá především prostřednictvím médií, což má mnohdy za následek výrazné zkreslení informací – tedy informační šum. Na druhé straně, skupina obyvatel, která je určitou hrozbou ovlivněna přímo, často neobdrží životně důležité informace vůbec nebo s velkým zpožděním, a to může znamenat zásadní problém.

Tato situace vyvolává otázku, zda by za pomoci informačních a komunikačních technologií 21. století – integrovaných do specifických funkčních celků – nemohlo být dosaženo větší efektivity současných procesů distribuce informací a zda by mohly být obohaceny o nové procesní přístupy napomáhající tomu, aby informace mohly být distribuovány skutečně včas a ve formě, která může lidem ohroženým mimořádnou událostí reálně pomoci. Tyto informace nemusejí mít význam pro občany mimo vymezený prostor – v některých případech může být dokonce nevhodné, aby pozičně cílené informace obdrželi příjemci, kteří se v cílové lokalitě nenacházejí.

Disertační práce spojuje oblast krizového managementu s aplikovanou informatikou – konkrétně se jedná o použití kryptografických metod pro účely návrhu systému včasného varování s funkcí pozičního šifrování varovných informací. Takový systém by měl být schopen cíleně distribuovat informace do předem vymezené lokality s atributem exkluzivity.

Tímto způsobem lze zajistit, aby původní (originální) informace byla přijata skutečně jen v těch lokalitách, ve kterých to její odesílatel zamýšlel. Pro ostatní oblasti by měla původní informace zůstat utajena. Základem šifrovacího klíče, bez ohledu na použitý kryptografický algoritmus, by v tomto případě byly zeměpisné souřadnice bodu, v jehož rozšířeném okolí by byla vymezena cílová oblast. Systém včasného varování, do kterého by byla implementována funkce pozičního šifrování, by mohl pomoci k efektivnějšímu varování obyvatelstva v různých fázích mimořádných a krizových situací.

1 Cíle práce a výzkumné otázky

1.1 Východiska a formulace výzkumných otázek

Východiska disertační práce vychází z projektu, který je dlouhodobě řešen na katedře informatiky EF TUL. Cílem projektu je navrhnout efektivní možnosti cílené distribuce potřebných informací při mimořádných situacích, které mohou ohrozit infrastrukturu a životy lidí nacházejících se v určité geografické lokalitě. Jeho dlouhodobým záměrem je pokusit se začlenit dosažené výsledky do procesů krizového řízení Jednotného systému varování a vyrozumění, za který má zákonnou odpovědnost Generální ředitelství HZS ČR.

1.1.1 Východiska disertační práce

Důvodem pro výzkum v oblasti inovací systémů včasného varování je skutečnost, že současná civilizace je každodenně konfrontována mimořádnými a krizovými událostmi, které jsou následkem přírodních anomálií nebo jsou způsobené lidským faktorem. V těchto situacích je více než kdykoli jindy důležitá **včasná a relevantní informovanost potenciálně ohrožených obyvatel** s cílem předejít důsledkům neočekávaných situací či je minimalizovat. Významným aspektem předávaných informací by měla být snaha co nejvíce potlačit možnost vyvolání paniky, což v těchto situacích obvykle hrozí. Bohužel stávající procesy a systémy včasného varování v ČR i ve světě v těchto případech mnohdy selhávají. Problémem jsou také zprávy získané z médií. Často se k občanům dostanou zkreslené informace, což může v důsledku způsobit paniku na místech, kde k tomu není objektivní důvod. Podobně problematické může být i prostředí Internetu a sociálních sítí, neboť ty jsou v mnoha případech zdrojem dezinformací a šíření panických zpráv.

O tom, že se jedná o důležitou oblast výzkumu, svědčí i nedávné mezinárodní sympozium s názvem „Ochrana obyvatelstva – Zdravotní záchranářství 2018“, která se uskutečnila na konci ledna 2018 v Ostravě. Je důležité, že si příslušné instituce a složky integrovaného záchranného systému uvědomují, že *„spíše než vyrozumění orgánů krizového řízení a složek integrovaného záchranného systému, které řeší jiné technologie, je nutné informovat obyvatelstvo o průběhu mimořádné události“* (Hartmann, 2018).

1.1.2 Výzkumné otázky

V souvislosti s uvedenými východisky byly formulovány následující výzkumné otázky:

1. Je možné nalézt řešení, které by eliminovalo nebo alespoň snižovalo míru nedostatků stávajících procesních přístupů a systémů v oblasti včasného varování?
2. Lze zajistit, aby co nejvyšší počet potenciálně ohrožených občanů získal relevantní informace odpovídající skutečné míře aktuálního nebezpečí a aby naopak ti, co ohroženi nejsou, byli uklidněni informací, že se jich nebezpečí netýká?
3. Lze navrhnou takový konceptuální model systému, který bude zohledňovat, co nejnižší náklady na implementaci takového řešení a zároveň klást důraz na optimální funkčnost tohoto systému?
4. Lze zajistit atribut exkluzivity informace vztažený k určité předem vymezené lokalitě?
5. Lze zajistit postupnou a zároveň centrálně řízenou evakuaci rozsáhlé oblasti v případě mimořádné události?

1.2 Cíle práce

Hlavním cílem disertační práce je návrh konceptuálního řešení systému, který bude schopen distribuovat varovné informace do určité oblasti s atributem exkluzivity. To znamená, že tento systém musí zajistit, aby zpráva byla pro anonymního adresáta srozumitelná (čitelná) pouze v určité předem vymezené lokalitě. Pro ostatní lokality by zpráva měla být nesrozumitelná (nečitelná), resp. nedostupná.

Jednou z možností, jak lze zmíněného atributu exkluzivity dosáhnout, je šifrování informací, u kterého bude šifrovací klíč odvozen od geografických souřadnic cílové oblasti. Tato funkce by mohla být aplikována jako dílčí součást systému včasného varování, jehož základní koncepce je publikována pod názvem Radio-Help a který si klade za cíl odstranit negativa stávajících varovných systémů.

Výše uvedeného hlavního cíle práce bude dosaženo pomocí následujících dílčích cílů práce:

- analýza současného stavu v oblasti systémů včasného varování obyvatel v České republice i ve světě;
- stanovení požadavků na efektivní systém včasného varování, včetně požadavků na dílčí subsystémy, mezi které patří i komponenta zajišťující šifrování informací;

- návrh modelových situací vycházejících z aktuálních hrozeb (zejména terorismus a přírodní katastrofy);
- analýza možných distribučních kanálů (rozhlasové vysílání, sítě GSM, Internet apod.)
- konceptuální návrh řešení pro včasnou distribuci pozičně šifrovaných varovných informací:
    - analýza a porovnání vhodných šifrovacích algoritmů pro dosažení atributu exkluzivity informace v předem vymezené geografické lokalitě;
    - návrh vhodného algoritmu vymezení oblasti pro příjem varovné zprávy.

1.3 Použité metody

V první části práce je realizována rešerše sekundárních pramenů v oblasti systémů včasného varování. Na základě metod deskripce a klasifikace stávajících poznatků obsahuje třetí kapitola kritické zhodnocení stávajícího stavu zkoumané oblasti. Ve čtvrté kapitole je pro vytvoření tzv. modelových situací použita metoda abstraktního modelování. Ve druhé části práce je provedena analýza dílčích komponent uvažovaného systému a následně syntéza v podobě konceptuálního návrhu systému pro poziční šifrované vysílání varovných informací.

1.4 Struktura práce

Disertační práce je členěna do osmi kapitol. V první části se práce věnuje nejprve vymezení základních pojmů souvisejících se zkoumanou problematikou. Dále je zde provedena deskripce současného stavu používaných systémů včasného varování v České republice i v zahraničí. Ta je podkladem pro třetí kapitolu, v níž jsou souhrnně kriticky zhodnoceny stávající systémy včasného varování. Následně jsou formulovány požadavky na systém, který by některé nedostatky stávajících systémů zmírnil nebo úplně eliminoval.

Ve čtvrté kapitole jsou na základě motivačních aspektů reflektujících aktuální hrozby současného světa navrženy čtyři modelové situace, které se zaměřují na možné způsoby využití systému pro cílenou distribuci informací s atributem exkluzivity vztahujícím se k určité předem vymezené geografické oblasti. Tohoto atributu exkluzivity může být dosaženo pomocí tzv. pozičního šifrování. Pátá kapitola pojednává v první části o základních principech kryptografie a v její druhé části jsou stanoveny charakteristické rysy

systému určeného pro pozičně šifrované vysílání informací. Závěr této kapitoly obsahuje zdůvodnění výběru šifrovacího algoritmu AES.

V šesté kapitole je na bázi konkrétního příkladu šifrování varovné zprávy proveden rozbor kryptografického algoritmu AES. První část sedmé kapitoly se věnuje stěžejnímu cíli této práce, což je vymezení oblasti pro příjem dešifrované varovné zprávy. Na základě stanovení cílové lokality se následně vygeneruje šifrovací klíč, který se použije pro vytvoření kryptogramu. Ve druhé části sedmé kapitoly je pomocí UML diagramů nastíněna základní koncepce systému včasného varování s funkcí pozičního šifrování, která by měla zajistit exkluzivitu informace v rámci určité oblasti. Osmá kapitola se věnuje ekonomicko-implementačnímu hledisku.

1.5 Přínos práce

Disertační práce se snaží přinést odpověď na otázky, zda by navržené postupy byly v praxi realizovatelné, zda mohou přinést výhody (vyšší efektivita, ekonomický přínos apod.) oproti systémům stávajícím a zda lze vyřešit některé problémy distribuce varovných informací spojené se stávajícím stavem systémů včasného varování.

2 Vymezení základních pojmů a deskripce současného stavu

V první části kapitoly jsou vymezeny základní pojmy, které souvisí s problematikou cílené distribuce informací. Je zde uvedeno rozdělení mimořádných událostí a související aspekty krizového managementu a krizové komunikace. Druhá část kapitoly přináší deskripci vybraných systémů včasného varování používaných v ČR i v zahraničí. Na jejím základě je ve třetí části kapitoly zhodnocen stávající stav v oblasti SVV.

2.1 Vymezení základních pojmů

Informace

Pojem informace je možné pro účely DDP vymezit pomocí následující definice: *„Informace vyvolává změnu stavu nebo chování příjemce“* (Žid, Svoboda et al., 1998). Pak lze informaci charakterizovat jako sdělení, které **má pro příjemce smysl** a usnadňuje mu volbu mezi různými možnostmi. Z informací si příjemce vytváří znalosti, které mu umožní porozumět nějaké skutečnosti (mimořádná událost) s cílem předvídat její chování a vývoj. Znalosti jsou předpokladem pro vědomé jednání.

Cílená distribuce informací

Záměrem cílené distribuce informací v kontextu této práce je zprostředkovat prostřednictvím systému včasného varování informaci pouze těm subjektům, pro které je určena. Pro takovou informaci, která je v danou chvíli relevantní a může mít „praktický význam“ pro určitou konečnou množinu příjemců, lze zavést označení **velmi praktický obsah** – *very practical content* (Skrbek, 2015).

Systém včasného varování

Systém včasného varování (*early warning system*) *„poskytuje včasné a relevantní informace prostřednictvím stanovených institucí, které jednotlivcům vystaveným riziku umožní přijmout opatření k vyloučení nebo snížení rizika a přípravě na účinnou reakci“* (UNEP, 2012; Ismail-Zadeh, 2014).

Mezi charakteristické vlastnosti systému včasného varování patří:

- znalost aktuálních i potenciálních rizik, která poskytuje vstupní informace, na jejichž základě lze varování založit;
- provázanost s monitorovacími a predikčními systémy;
- schopnost rychlého přenosu informací mezi záchrannými složkami;
- schopnost bezprostředně předat adekvátní informace z autorizovaného zdroje aktuálně či potenciálně ohroženým lidem;
- zabezpečení účinné reakce na vyslané varování, která závisí na průběžném testování systému, efektivní koordinaci, vhodných krizových plánech a důvěře ohrožených obyvatel v samotný systém včasného varování.

Aby byl SVV efektivní, musí být kladen důraz na zvyšování povědomí veřejnosti, vzdělávání a komunikaci. Pokud nejsou obyvatelé na potenciálně ohrožených místech včas varováni a/nebo složky záchranného systému informacím nerozumějí a nevědí, jak na vzniklou situaci reagovat, systém není účinný.

Mimořádná situace, mimořádná událost a krizová situace

Pod pojem **mimořádné situace** zahrnujeme mimořádné události, krizové situace a další situace, které mohou ovlivnit normální běh života větší skupiny obyvatel.

Pojem **mimořádná situace** je vymezen MVČR jako situace vzniklá v určitém prostředí v důsledku hrozby vzniku nebo důsledku působení mimořádné události, která je řešena obvyklým způsobem složkami integrovaného záchranného systému, bezpečnostního systému, systému ochrany ekonomiky, obrany apod. a příslušnými orgány za použití jejich běžných oprávnění, postupů a na úrovni běžné spolupráce bez vyhlášení krizových stavů.

Mimořádná událost je pak podle MVČR definována jako událost nebo situace vzniklá v určitém prostředí v důsledku živelní pohromy, havárie, nezákonnou činností, ohrožením kritické infrastruktury, nákazami, ohrožením vnitřní bezpečnosti a ekonomiky, která je řešena obvyklým způsobem orgány a složkami bezpečnostního systému podle zvláštních právních předpisů. Pod tímto termínem je v současných právních předpisech ČR uváděna řada pojmů, jako jsou např. mimořádná situace, nouzová situace, pohroma, katastrofa, havárie.

Zákon č. 239/2000 Sb. (o integrovaném záchranném systému a o změně některých zákonů) definuje mimořádnou událost jako „*škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací*“.

§ 2 písm. b) zákona č. 240/2000 Sb. (krizový zákon) vymezuje pojem krizová situace jako „*mimořádnou událost podle zákona o integrovaném záchranném systému (zákon č. 239/2000 Sb.), narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (dále jen „krizový stav“)*“.

Krizovou situaci definuje MVČR jako mimořádnou událost, v jejímž důsledku se vyhlašuje stav nebezpečí, nouzový stav, stav ohrožení státu nebo válečný stav. Jsou při ní ohroženy důležité hodnoty, zájmy či statky státu a jeho občanů. Hrozící nebezpečí nelze odvrátit a způsobené škody odstranit běžnou činností orgánů veřejné moci, ozbrojených sil a ozbrojených bezpečnostních sborů, záchranných sborů, havarijních a jiných služeb a právnických a fyzických osob.

Pro účely této práce bude dále používán zejména pojem mimořádná událost.

2.1.1 Rozdělení mimořádných událostí

Mimořádné události dělíme podle Veverky (2003) na dvě základní skupiny: naturogenní (přírodní) a antropogenní (způsobené činností člověka).

Naturogenní mimořádné události (vyvolané přírodními vlivy) dále dělíme na:

- abiotické mimořádné události – jsou způsobené neživou přírodou
    - např. požáry způsobené přírodními vlivy, povodně a záplavy, tsunami, zemětřesení, vichřice, tornáda, sněhové kalamity, dlouhodobá sucha apod.;
- biotické mimořádné události – jsou způsobené živou přírodou
    - např. epidemie – rozsáhlá nákaza lidí, epizootie – rozsáhlá nákaza zvířat, přemnožení přírodních škůdců apod.

Antropogenní mimořádné události dále dělíme na:

- technogenní mimořádné události – provozní havárie a havárie spojené s infrastrukturou
    - např. radiační havárie, rozsáhlé dopravní havárie (silniční, železniční, letecké), znečištění životního prostředí rozsáhlými haváriemi apod.;
- sociogenní mimořádné události interní – vnitrostátní společenské, sociální a ekonomické krize
    - např. hrozba teroristických akcí, aktivity vnitřního a mezinárodního zločinu a terorismu, narušení dodávek pitné vody apod.;
- sociogenní mimořádné události externí – vojenské krizové situace
    - např. vnější vojenské napadení státu nebo jeho spojenců, rozsáhlé ekologické havárie přesahující hranice států apod.;
- agrogenní mimořádné události – spojené se zemědělstvím a půdou
    - např. vysychání a znehodnocování vodních zdrojů apod.

V dalších částech práce budou informace zde uváděné souviset zejména s naturogenními abiotickými a antropogenními sociogenními interními mimořádnými událostmi.

2.1.2 Krizové řízení

Krizové řízení (krizový management) lze podle Coombse (2012) definovat jako *„soubor faktorů určených pro boj s krizemi a pro zmírnění škod krizemi způsobených“*. Krizové řízení se rovněž snaží zabránit negativním důsledkům krize nebo je alespoň snížit, a tím ochránit zúčastněné strany před škodami. Krizové řízení je proces, který má několik částí, mezi něž patří preventivní opatření, plány pro řešení krizí a způsoby vyhodnocení proběhlých procesů po krizi. Zmíněné *„soubory faktorů“* lze rozdělit na tři hlavní procesní kategorie:

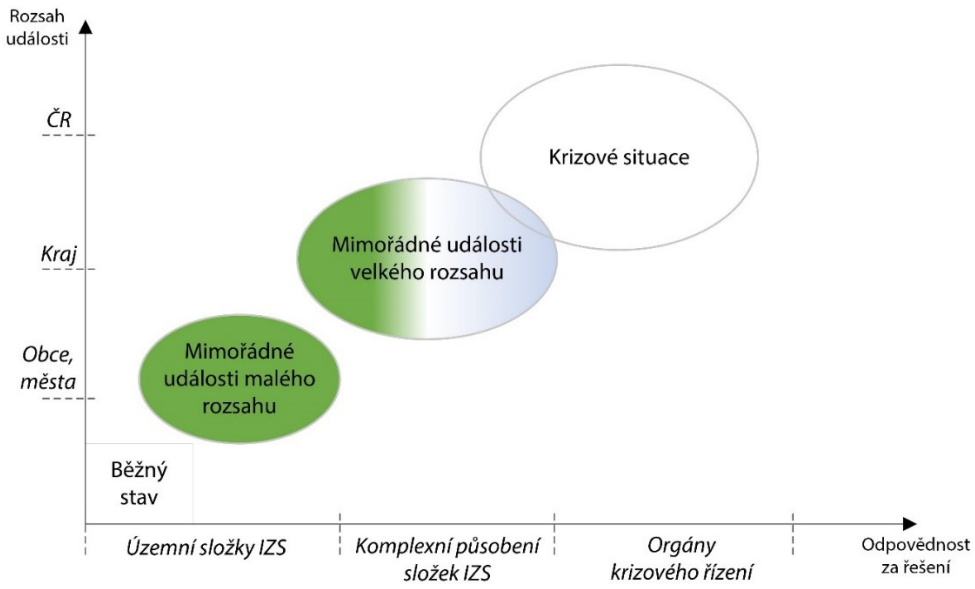
1) procesy zabývající se situací před krizí – snahy předcházet krizím a příprava na krizové řízení;
2) řízení během krize – reakce na aktuální událost;
3) procesy aplikované po krizi – poučení z krizové události.

Uvedené tři kategorie odrážejí fáze řízení krizí a jsou užitečné, jelikož poskytují mechanismus pro posouzení šíře krizové komunikace.

Antušák (2016) zavádí pět hlavních funkcí krizového řízení. Jedná se o propojené činnosti, které tvoří celý proces řízení krizí. Jsou jimi:

- prevence,
- korekce,
- protikrizové intervence,
- redukce,
- obnova.

Obrázek 1 graficky znázorňuje vzájemné vztahy mezi mimořádnými událostmi a krizovými situacemi.



Obrázek 1: Průběh procesů krizového řízení
Zdroj: Upraveno podle Viláška (2012)

V období běžného stavu, kdy nedochází k narušování života společnosti, mohou občas nastat malé živelní pohromy, požáry, záplavy, hromadné zranění menšího počtu občanů. V těchto případech se jedná o mimořádné události malého rozsahu a řešení je v kompetenci jednotlivých územních složek IZS. Mimořádné události mohou ale nabýt i rozsahu většího, pokud se havárie, pohroma či epidemie rozšíří mimo obec do dalších lokalit a zasáhne další obce, případně se rozšíří v kraji. Takto rozsáhlá mimořádná událost se řeší komplexním

působením složek IZS spolu s běžnou činností správních úřadů a subjektů kritické infrastruktury v rámci zákona IZS a využívá dokumentace havarijního plánování.

Pokud se nepodaří mimořádnou událost, která ohrožuje území přesahující kraj či části ČR, odvrátit, zmírnit nebo zastavit pomocí všech dostupných složek IZS a běžnou činností správních orgánů a subjektů kritické infrastruktury, nastává krizová situace. Tu řeší orgány krizového řízení v rámci platné legislativy, především krizového zákona, a vyhlásí některý z krizových stavů s využitím dokumentace krizového plánování. Tím, že nelze přesně vymezit hranice mezi jednotlivými událostmi (viz průniky na obrázku 1), se vyjadřuje určitá eskalace průběhu mimořádné události k hraniční mezi.

Krizová situace vznikne tak, že mimořádná událost eskaluje z události malé na velkou a následně docílí maxima. Toto maximum označuje stav, který se vyznačuje nemožností řešit MU (tzn. nelze ji odvrátit, zastavit ani zmírnit), a tím vzniká krizová situace. V této fázi musí nastoupit institut vyhlášení některého z krizových stavů. Na rozdíl od krizové situace se krizový stav vyhlašuje, neboť se jedná o právní akt (Antušák, 2016).

Zaměření systému popisovaného v této práci klade důraz zejména na využití ve fázích běžného stavu, mimořádné události malého rozsahu až po mimořádné události velkého rozsahu na úrovni krajů, kde odpovědnost za řešení mají stále ještě složky IZS. Na obrázku 1 je toto znázorněno zelenou barvou.

2.1.3 Krizová komunikace

S řešením mimořádných událostí a distribucí informací během nich úzce souvisí pojem krizová komunikace. Krizová komunikace je definována jako shromažďování, zpracování a šíření informací, které jsou nezbytné k zabránění vzniku či k optimálnímu vyřešení nastalé mimořádné události (Coombs, 2012).

Podle Coombse lze krizovou komunikaci rozdělit do tří fází na komunikaci:

- předcházející mimořádné události,
- v průběhu mimořádné události,
- po skončení mimořádné události.

V situaci před mimořádnou událostí tato komunikace zahrnuje shromažďování informací o potenciálních rizicích, vytváření krizových plánů a školení způsobilého personálu, jenž bude součástí řízení krize. Do této skupiny lidí patří například zásahové týmy, krizoví mluvčí či dobrovolníci. Komunikace v průběhu mimořádné události se skládá ze sběru a zpracování informací nezbytných pro rozhodování krizového týmu, vytváření krizových zpráv a jejich šíření mezi jedince, kteří nejsou součástí tohoto týmu (tradiční definice krizové komunikace). Post-krizová fáze spočívá v řízení a řešení následků krize, přičemž jsou sdíleny informace o změnách, které byly přijaty jako opatření pro zamezení podobným situacím či pro vyřešení stávající situace s cílem navrácení do normálního stavu (Coombs, 2012).

S přihlédnutím k dalšímu obsahu této práce můžeme krizovou komunikaci charakterizovat podle definice, kterou uvádí Antušák (2009): „*přesun informací mezi státními orgány, územními samosprávnými orgány a mezi složkami integrovaného záchranného systému za využití příslušných prostředků hlasového i datového přenosu informací veřejné telekomunikační sítě i vybrané části neveřejných telekomunikačních sítí*“.

Cílem krizové komunikace podle Antušáka (2009) *„je uvolnit správné (včasné, hodnotné, důvěryhodné a přesvědčivé) informace* ***ve správný čas a na správném místě“***, a tím dosáhnout včasné a odborně plnohodnotné připravenosti orgánů a elementů krizového řízení k následným činnostem. S tím souvisí další atributy krizové komunikace: snižování nejistoty, možnost přispět k zajištění efektivního chování v dané situaci (veřejnosti, podřízených, členů rodiny, zaměstnanců firmy) a zabránit vzniku paniky, posilování víry v budoucnost. Jedním z cílů této práce je navrhnout koncepci systému, který by efektivněji varoval potenciálně ohrožené občany. Z tohoto pohledu chybí ve výše uvedeném cíli krizové komunikace důležitý aspekt, a to **doručení aktuálně potřebné informace k zamýšlenému příjemci.** To, že se informace uvolní, nemusí vždy znamenat, že bude opravdu doručena ve správný čas a na správné místo.

2.2 Stávající systémy pro včasné varování obyvatel

V současném světě, ve kterém média téměř denně vysílají zprávy o mimořádných událostech a katastrofách, je nutné zajistit informovanost obyvatelstva, a to způsobem, jenž je efektivní a dostupný pro co nejširší okruh obyvatel. Celosvětově existuje celá řada varovných systémů, které jsou zaměřeny na různé oblasti případných hrozeb. V následujících podkapitolách budou některé z nich popsány včetně upozornění na jejich nedostatky.

2.2.1 Jednotný systém varování a vyrozumění (JSVV)

Základní a důležitou součástí „Integrovaného záchranného systému ČR (IZS ČR)“ je „Jednotný systém varování a vyrozumění“. Tento varovný systém je v České republice budován od roku 1991 a je spravován Generálním ředitelstvím Hasičského záchranného sboru České republiky (HZS ČR). Podle zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů zabezpečují varování obyvatelstva hasičské záchranné sbory krajů a obecní úřady.

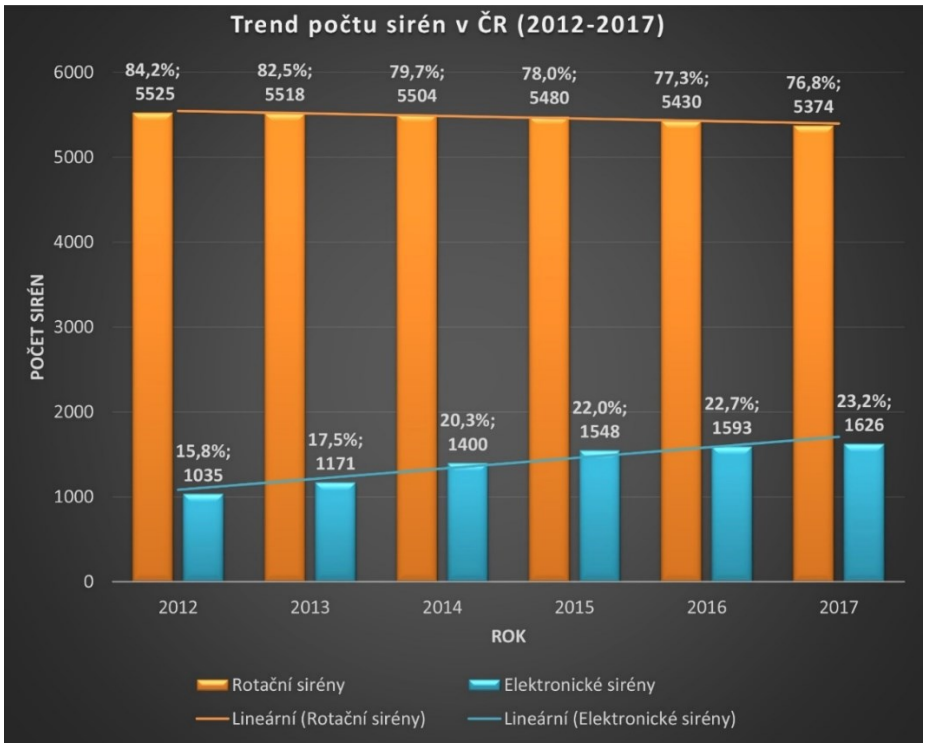
Bezprostřední varování obyvatelstva zabezpečují koncové prvky, kterými jsou zejména poplachové sirény a obecní rozhlasy dálkově ovládané připojením k JSVV. Dále je tento systém tvořen soustavou vyrozumívacích center (krajská operační střediska HZS), jejichž součástí je počítačové pracoviště se zadávacím terminálem a telekomunikační sítí, která sestává z rádiových vysílačů rovnoměrně rozmístěných po kraji. Vysílače zajišťují přenos a šíření rádiového signálu, jímž se ovládají koncové prvky, přičemž je umožněno spouštět sirény v kraji jednotlivě, ovládat skupiny sirén, případně spouštět všechny najednou.

Obrázek 2: Průběh signálu všeobecné výstrahy, zkušebního tónu a požárního poplachu
Zdroj: www.hzscr.cz/clanek/sireny.aspx

Podle informací Hasičského záchranného sboru ČR slouží pro varování obyvatelstva pouze jeden varovný signál nazvaný **„Všeobecná výstraha“**. U signálu všeobecné výstrahy siréna po dobu 2 minut a 20 sekund vysílá kolísavý tón, který může zaznít 3× za sebou v přibližně tříminutových intervalech (HZS ČR, 2014). Starší rotační typy sirén mají dosah cca 1000 m a jsou postupně nahrazovány modernějšími elektronickými sirénami (tzv. mluvicí sirény).

Ty doplňují varovný tón o hlasové informace, které přesněji specifikují druh ohrožení (povodňová vlna, orkán apod.), a navíc je jejich prostřednictvím obyvatelstvo verbálně vyzváno ke sledování vysílání Českého rozhlasu a České televize. Dosah elektronických sirén je cca 500 až 700 metrů. Je nicméně ovlivněn výkonem koncových prvků varování, profilem terénu a hustotou zástavby (HZS LK, 2016). Druhým signálem je „Zkušební tón“, který slouží k pravidelné akustické zkoušce sirén. Třetím signálem, jenž může zaznít prostřednictvím sirén JSVV, je „Požární poplach“. Ten slouží ke svolání jednotek požární ochrany.

Pokud zazní signál všeobecné výstrahy, doporučuje HZS ČR po jeho odeznění následující kroky: 1) okamžitě se ukrýt; 2) zavřít okna a dveře; 3) zapnout rádio nebo televizi. Problémem tohoto řešení je zejména skutečnost, že informace, které obyvatelé obdrží, jsou příliš obecné. Navíc, média mohou být zdrojem neadresných, obecných, v horším případě i zkreslených zpráv, což může vyvolat nežádoucí reakce obyvatel. Řešením může být pozičně vymezená, cílená distribuce informací, která by využívala rozhlasové vysílání, případně GSM sítě. Tímto způsobem by bylo možné zajistit, aby obyvatelé obdrželi varovné informace, jež se vztahují k jejich lokalitě a skutečné míře nebezpečí.



Obrázek 3: Trend počtu sirén v ČR v letech 2012-2017
Zdroj: Vlastní zpracování podle interních dokumentů HZS ČR

V České republice bylo v roce 2017 podle dostupných údajů (interní dokumenty HZS ČR) provozováno 7 000 sirén, přičemž převažují stále starší rotační typy sirén – 5374 rotačních sirén (76,8 %) oproti 1626 elektronickým sirénám (23,2 %). V roce 2012 bylo k dispozici celkem 6560 sirén, z toho 5525 sirén rotačních (84,2 %) a 1035 elektronických (15,8 %). Z těchto údajů je patrné, že sirény, které byly od roku 2012 vybudovány nově, jsou elektronického typu. Bohužel trend nahrazování stávajících rotačních sirén sirénami elektronickými je příliš pozvolný. Počet sirén v letech 2012–2017 podrobněji dokládá obrázek 3.

Další možnost činnosti IZS vymezuje již zmíněný zákon č. 239/2000 Sb. – každý, kdo provozuje hromadné informační prostředky, včetně televizního a rozhlasového vysílání, je povinen bez náhrady nákladů na základě žádosti operačního a informačního střediska integrovaného systému neprodleně a bez úprav obsahu a smyslu uveřejnit tísňové informace pro záchranné a likvidační práce.

2.2.2 Varovné informace distribuované prostřednictvím SMS zpráv

Dalším varovným systémem dostupným v České republice je způsob informování v krizových situacích prostřednictvím posílání SMS zpráv na mobilní telefony obyvatel. O funkčnost tohoto systému se starají obecní a městské úřady obcí a měst, které jsou do tohoto projektu zapojeny. V současnosti se jedná například o Jihomoravský kraj a Plzeňský kraj. Kromě zpráv o mimořádných událostech je možné tento systém využívat i pro distribuci informací z běžného života obce či města. Potřebné informace jsou zasílány nejen přímo obyvatelům, ale i příslušným krizovým štábům. V případě Jihomoravského kraje jsou do projektu navíc zapojena všechna zdravotnická zařízení v Jihomoravském kraji včetně fakultních nemocnic.

Občané, kteří mají zájem o odebírání zpráv prostřednictvím tohoto komunikačního kanálu, se musí nejprve prostřednictvím speciálně definované SMS do systému zaregistrovat (např. PLZ mezera PLZEN mezera 7 mezera INFORMACE mezera ANO mezera PRIJMENI mezera JMENO hvězdička ULICE hvězdička CISLO ORIENTACNI). Seznam obcí a měst, které jsou do projektu zapojeny, je k dispozici na adrese http://www.krizoveinfo.cz/.

Výhodou použité technologie je bezesporu to, že mobilní telefon je zařízení, které má většina lidí téměř neustále u sebe. Je zde tedy určitá pravděpodobnost, že si konkrétní občan danou

informaci přečte. Ovšem pouze za předpokladu, že jsou v provozu mobilní sítě. Bohužel právě v případě živelných katastrof, jako jsou povodně, vichřice, tornáda, zemětřesení, dochází poměrně rychle nejen k výpadkům elektrické rozvodné sítě, ale i k omezené funkčnosti či úplné nefunkčnosti mobilních sítí v důsledku přetížení. To má za následek, že se potřebná informace odeslaná prostřednictvím SMS služby dostane k občanům buď pozdě, anebo vůbec. **A přitom právě v případě živelních katastrof je rychlost získávání informací klíčovým faktorem pro záchranu životů a eliminaci hmotných škod**. Další nevýhodou je nutnost registrace do tohoto systému, takže případné varovné informace o mimořádné události jsou dostupné pouze pro registrované občany určité obce. Navíc v případě, že se občan bude pohybovat v jiné lokalitě mimo oblast obce, ve které je registrován (např. v jiné části ČR) a ve které dojde např. k úniku nebezpečných látek, nebude o této situaci informován.

2.2.3 Bezdrátový rozhlas

Kromě běžných hlášení o životě v konkrétní obci nebo městě je bezdrátový rozhlas koncipován jako jedna z dalších možností, jak varovat občany před nejrůznějším nebezpečím, jako jsou záplavové vlny, požáry apod.

Například v Kopřivnici vyšlo vybudování tohoto systému v roce 2014 na 11 miliónů Kč. Některé místní části města Kopřivnice se nacházejí na břehu řeky Lubiny, která několikrát ročně hrozí při prvním či druhém povodňovém stupni vylitím z břehů. V takto ohrožených lokalitách bývá součástí systému bezdrátového rozhlasu instalace hladinových čidel několik km před ohroženými lokalitami, tedy proti proudu řeky. Tato čidla by v případě Kopřivnice měla varovat kopřivnickou povodňovou komisi před případnou povodňovou vlnou.

Většina obcí v okrese Nový Jičín, které byly v roce 2009 zatopeny povodní, již tento systém využívá. Mezi tyto obce patří např. Nový Jičín, Životice u Nového Jičína a další. Podle informací z roku 2014 je těchto systémů v Moravskoslezském kraji 90 a systémy bezdrátového rozhlasu jsou navíc napojené na integrované bezpečnostní centrum HZS.

Systém obecního bezdrátového rozhlasu s předem nahranými hlášeními odstraňuje některé nevýhody staršího řešení obecních rozhlasů. Jednotlivá bezdrátově propojená tlampačová hnízda jsou na sobě nezávislá, takže porucha jednoho místa (např. pád sloupu) neohrozí

výpadek celého systému. Dále odpadá kabelové vedení mezi jednotlivými sloupy, čímž se snižují také nároky na údržbu a eliminuje se riziko přerušení kabelového vedení.

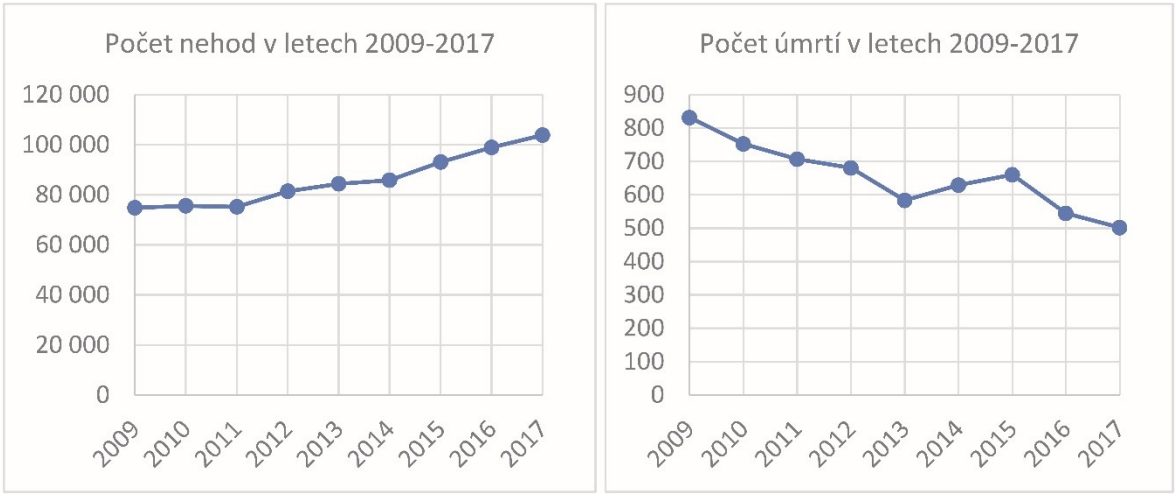
2.2.4 Systém eCall

Systému eCall (*emergency call*) je v této části práce věnován prostor zejména z důvodu, že se jedná o „nově“ zavedený systém, který má kromě ambice urychlení prioritní aktivace integrovaných záchranných složek i potenciál významně zrychlit některé procesy distribuce informací při prevenci hromadných dopravních nehod. Jedním z hlavních cílů implementace tohoto systému napříč EU je snížení počtu úmrtí způsobených dopravními nehodami, díky rychlejšímu zásahu IZS.

Tabulka 1: Počet nehod v ČR a jejich následků v letech 2009–2017

Počet nehod	Počet úmrtí	Počet těžkých zranění	Počet lehkých zranění
74 815	832	3 536	23 777
75 522	753	2 823	21 610
75 137	707	3 092	22 519
81 404	681	2 986	22 590
84 398	583	2 782	22 577
85 859	629	2 762	23 655
93 067	660	2 540	24 426
98 864	545	2 580	24 501
103 821	502	2 339	24 740

Zdroj: Statistiky nehodovosti Policie ČR, 2017



Obrázek 4: Počet dopravních nehod a úmrtí v ČR v letech 2009–2010
Zdroj: Zpracováno na základě statistik nehodovosti (Policie ČR, 2017)

Z tabulky 1 a grafů na obrázku 4 je patrné, že i přes vzrůstající počet dopravních nehod klesá počet úmrtí jejich následkem. V porovnání s rokem 2009 stoupl počet nehod evidovaných Policií ČR o 38,77 %, ale klesl počet úmrtí o 39,66 %. Je optimistické, že počet úmrtí způsobených dopravními nehodami byl v roce 2017 dokonce historicky nejnižší od roku 1961, od kterého dopravní policie zpracovává statistiky o dopravních nehodách (Policie ČR, 2017). Podobně je tomu i u dalšího sledovaného údaje, jenž eviduje počet těžkých zranění. Jejich počet se od roku 2009 snížil o 33,85 % a i zde se jedná o počet, který je nejnižší od roku 1961. Tento zdánlivě paradoxní fakt je nejspíše ovlivněn rostoucí pasivní bezpečností vozidel.

Podrobné údaje o dopravní nehodovosti a následcích nehod jsou pro jednotlivé měsíce roku 2017 zpracovány na základě dat Policie ČR v následující tabulce 2.

Tabulka 2: Nehody a jejich následky, řešené Policií ČR pro jednotlivé měsíce roku 2017

Měsíc	Počet nehod celkem	Počet úmrtí	Počet těžkých zranění	Počet lehkých zranění	Hmotná škoda (odhad na místě nehody)
leden	8 626	30	94	1 524	496 123 700 Kč
únor	6 969	26	114	1 255	395 223 500 Kč
březen	7 714	30	166	1 560	449 178 700 Kč
duben	7 934	35	181	1 886	494 650 600 Kč
květen	9 228	40	236	2 339	537 449 100 Kč
červen	9 426	62	325	2 728	567 458 300 Kč
červenec	8 280	45	229	2 403	484 123 100 Kč
srpen	9 028	56	275	2 631	532 305 800 Kč
září	8 930	43	190	2 150	564 106 200 Kč
říjen	9 941	48	195	2 332	645 266 200 Kč
listopad	8 983	42	187	1 925	571 175 200 Kč
prosinec	8 762	45	147	2 007	579 196 300 Kč
Celkem	**103 821**	**502**	**2 339**	**24 740**	**6 316 256 700 Kč**

Zdroj: Statistiky nehodovosti Policie ČR, 2017

Lze očekávat, že s postupnou obměnou vozového parku by díky systému eCall mohly údaje o počtu úmrtí v průběhu další let klesat ještě více. Je otázkou, zda se optimistický odhad Evropské komise o snížení počtu úmrtí o 2500 za rok díky systému eCall v průběhu následující dekády naplní.

Systém eCall řeší zejména zmírnění následků nehod, ale zatím **neřeší prevenci**, tedy způsob, jak nehodám předcházet, aby k nim pokud možno vůbec nedošlo. Jedno z možných řešení

využití systému eCall pro varování účastníků dopravního provozu je podrobněji nastíněno v kapitole 3.3.1.

Zkušenosti se zaváděním systému eCall v ČŘ z pohledu HZS ČR

Podle rozhodnutí Evropského parlamentu a Rady č. 585/2014/EU ze dne 15. 5. 2014 byla uložena všem členským státům EU povinnost zavést všechny služby související se systémem eCall do 30. 9. 2017. Ke spuštění systému eCall v České republice došlo na konci září roku 2017. Podle generálního ředitele HZS ČR genmjr. Drahoslava Ryby došlo v průběhu září k intenzivnímu testování tohoto systému zejména v Ostravě s konstatováním, že se veškeré funkce chovají podle očekávání a všechna operační střediska HZS ČR jsou od 30. září 2017 připravena na přijímání tísňových hovorů prostřednictvím eCallu. V prvním měsíci ostrého provozu byly prostřednictvím systému eCall přijaty tísňové hovory v řádu jednotek. Česká republika, konkrétněji HZS ČR byl od začátku jedním z hlavních inovátorů při zavádění a implementaci eCallu, přičemž některá řešení HZS se dokonce promítla do specifikací Evropské komise, podle nichž se nyní musí implementovat systém eCall v celé EU.

Zavádění v rámci EU naráželo v počátcích na některé problémy. Jednak se mnohé státy k myšlence zavedení nestavěly v prvotní fázi příliš vstřícně a jednak v realizačním týmu napříč EU nebyl k dispozici dostatečný počet členů záchranných složek.

HZS ČR patřil mezi několik málo zkušených zástupců záchranných složek, kteří měli praktičtější pohled a dobře se orientovali v dané problematice. Dle slov mluvčího krajského operačního a informačního střediska HZS hlavního města Prahy se *„bohužel některé záležitosti s obtížemi vysvětlovaly a argumentovaly těm kolegům, kteří se do projektu zapojovali např. z ministerstva dopravy a neměli dostatečný záchranářský rozměr. Vzhledem k této situaci bylo velmi náročné některé inovace a návrhy obhajovat před ostatními týmy, které byly do projektu zainteresovány.“* (Zaoralová, 2017)

Realizace mnoha projektů v oblasti systému eCall a bohaté zkušenosti udělaly z ČR inovátorskou zemi. *„Posunuli jsme se hodně dopředu, měli jsme jasné cíle, věděli jsme, čeho chceme dosáhnout, i když před námi vyvstávaly nové technické komplikace, které se musely řešit a překonávat, zatímco zástupci z ostatních zemí o nich v počátcích projektu neměli ještě dostatečné povědomí a při realizaci svých projektů naše argumenty podceňovali.“* (Zaoralová, 2017)

2.2.5 KATWARN

KATWARN je německý varovný a informační systém, který se začal v praxi testovat v roce 2011. Mezi nesporné výhody tohoto systému patří zejména to, že pro komunikaci využívá nejrozšířenější zařízení – a to mobilní a chytré telefony. Obyvatelé Německa mohou tento systém využívat bezplatně a dobrovolně.

Původně byl systém KATWARN koncipován tak, že měl na případné mimořádné události upozorňovat zejména prostřednictvím SMS zpráv. S rostoucím užíváním chytrých mobilních telefonů je od roku 2012 dostupná také aplikace pro tato „smart" zařízení, přičemž jsou podporované tři nejrozšířenější mobilní platformy (iOS, Android, Windows). Právě s rozšířením této aplikace souvisí rostoucí obliba a využitelnost systému KATWARN. Dalším komunikačním kanálem systému KATWARN jsou sociální sítě. Mezi nevýhody systému KATWARN patří zejména závislost na funkčnosti mobilních sítí, případně Internetu. Nicméně je deklarováno, že v případě hrozby přetížení mobilních sítí budou zprávy od orgánů záchranného systému doručovány přednostně.

Obrázek 5: KATWARN – mapa pokrytí v Německu a sociální sítě Twitter
Zdroj: SV, GI5 Herr Vetter, www.katwarn.de/aktuell.php

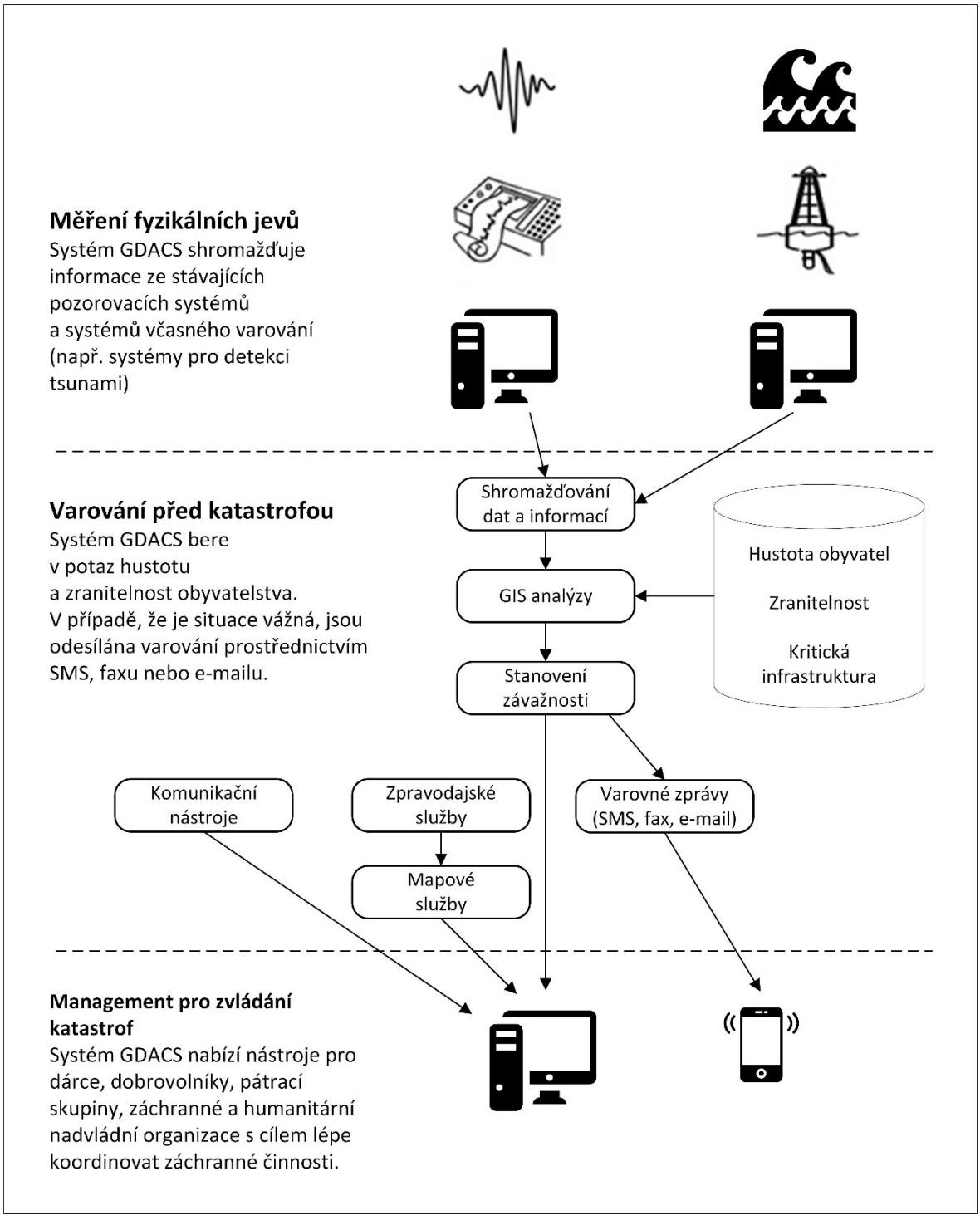
Nedostatek varovné aplikace v podobě závislosti na mobilní síti a Internetu se v plné míře projevil při mimořádné události v Mnichově 22. července 2016. Útočník v nákupním centru Olympia usmrtil 9 osob, zraněno jich bylo 27. Mnichovské orgány varovaly prostřednictvím

systému KATWARN obyvatelstvo krátce po tragické události, aby neopouštěli své domovy a vyhýbali se veřejným prostorám. Varování bylo spuštěno celkem 3×. V důsledku časově paralelní mimořádné události, při které došlo v jiné části Německa k silné vichřici a bouři, bylo k systému připojeno současně 250 000 lidí. Bohužel tím došlo k celkovému přetížení systému a lidé následně přestali dostávat varovné informace. (Greiner, 2016)

2.2.6 The Global Disaster Alert and Coordination System (GDACS)

The Global Disaster Alert and Coordination System – GDACS (Globální systém varování před katastrofami a koordinační systém) je internetový informační systém, který byl spuštěn v roce 2004 a využívá již existující informační systémy zaměřené na katastrofy. Součástí GDACS je soubor pracovních procedur a pravidel o spolupráci mezi Organizací spojených národů, Evropskou komisí a krizovými manažery po celém světě. Slouží ke zlepšení včasného varování a výměny informací a ke koordinaci jednotlivých složek v první fázi katastrof velkého rozsahu (GDACS, 2017). Hlavním účelem tohoto systému je usnadnit koordinaci reakcí mezinárodních týmů v době předcházející katastrofě (tj. od okamžiku její předpovědi), v jejím průběhu i po skončení katastrofy (tzv. pomocná fáze). Doba trvání pomocné fáze je závislá na závažnosti katastrofy, nicméně předpokládá se v rozmezí tří až čtyř týdnů po katastrofě.

Systém je cílen zejména na naturogenní a technogenní katastrofické události většího rozsahu, při kterých postižený stát není schopen samostatně zajistit přechod do běžného stavu a vyžaduje mezinárodní pomoc. Mezi hlavní výhody GDACS patří schopnost poskytovat velmi rychle varovné informace o katastrofách z celého světa, následně také vhodné koordinační nástroje s cílem vytvořit virtuální koordinační centrum operací (OSOCC – *On-Site Operations Coordination Centre*). Základní princip fungování systému GDACS je patrný z obrázku 6.



Obrázek 6: Princip systému GDACS
Zdroj: upraveno podle GDACS (2009)

Ačkoli systém GDACS má díky napojení na další systémy poměrně rozsáhlé možnosti predikce katastrofy, neslouží primárně jako systém včasného varování pro potenciálně postižené regiony, ale jak již bylo řečeno, primárním účelem je aktivovat, optimalizovat

a lépe koordinovat záchranné činnosti. Napojení na GDACS a využití informací z tohoto systému pro účely včasného varování je v kompetenci jednotlivých států.

Výše zmíněné virtuální centrum operací (OSOCC) je on-line virtuální platforma spolupráce používaná Organizací spojených národů a dalšími subjekty humanitární pomoci při katastrofách. Smyslem virtuálního centra je tyto složky koordinovat. Ačkoli GDACS není zaměřen výhradně na GIS a mapování, představují tyto dvě komponenty důležitou součást služeb GDACS. Systém navíc poskytuje data, mapy a satelitní snímky pro různé události, které umožňuje sledovat právě prostřednictvím virtuálního centra, a jsou tak dostupné pro mezinárodní charty a další složky mezinárodní humanitární pomoci (Tomaszewski, 2015).

2.2.7 Indian Ocean Tsunami Warning and Mitigation System (IOTWS)

Do roku 2004 neexistoval v Indickém oceánu žádný systém, který by alarmoval obyvatelstvo před blížícím se nebezpečím, i přesto, že mnozí odborníci na bezpečnost vytvoření takového systému doporučovali. Systém IOTWS je v provozu od roku 2006 a je primárně zaměřen na varování před tsunami v oblastech Indického oceánu. IOTWS je schopen během pěti minut předat informace do operačních center NTWC (National Tsunami Warning Centres). Monitorovací stanice tohoto systému se skládají z podvodního seismografu, který je určen k měření síly zemětřesení pod hladinou, a bóje na hladině oceánu, která zajistí přenos informací do operačních center jednotlivých států (IOTIC, 2017).

Neexistuje však efektivní kanál umožňující varovat obyvatele a řídit případnou evakuaci. Preferovanými koncovými prvky tohoto systému jsou zatím nepříliš četné tlampačové reproduktorové soustavy, v některých státech plní roli messengerů dokonce lidé – běžci (UN Development Programme, 2014).

Výhodou systému IOTWS je možnost rychlého zjištění blížící se tsunami. Nicméně, vezmeme-li v úvahu fakt, že se o přicházejícím nebezpečí dozví celá oblast v jednu chvíli, hrozí zejména v přelidněných oblastech problémy způsobené panikou a následné problémy při hromadné evakuaci. Pro názornost jsou v tabulce 3 uvedeny nejničivější tsunami od roku 1992 z pohledu ztrát na lidských životech. Japonsko investovalo, zejména na základě zkušeností po ničivé tsunami v Indonésii (2004), nemalé prostředky do varovných systémů spojených s tímto jevem. Nicméně ani tato skutečnost nezmírnila následky katastrofy

v březnu 2011, kdy Japonsko bylo zasaženo sérií tsunami, vyvolaných zemětřesením o síle 9,0 Richterovy stupnice. (International Tsunami Information Center - IOC/Unesco, 2017)

Tabulka 3: Počet ztrát na životech způsobených jevem tsunami

Den	Lokalita	Odhadovaný počet úmrtí (včetně nezvěstných obyvatel)
12. 12. 1992	Flores Sea, Indonésie	1 169
17. 07. 1998	Papua-Nová Guinea	2 205
26. 12. 2004	Banda Aceh, Indonésie	227 899
17. 07. 2006	Java, Indonésie	802
25. 10. 2010	Mentawai, Indonésie	431
11. 03. 2011	Tohoku, Japonsko	18 453

Zdroj: Zpracováno podle International Tsunami Information Center - IOC/Unesco (2017)

2.2.8 Shrnutí

Pokud shrneme výše uvedené příklady varovných systémů (v jejich současné podobě), dojdeme k tomu, že v případě výpadku energetických sítí, mobilních sítí a internetu tyto komunikační kanály selhávají, a potřebné informace tedy nebudou doručeny ve správný čas na správné místo. Proto je nutné co nejvíce eliminovat závislost na energetické síti, mobilních sítích a internetu a nalézt takové informační kanály a systémy, které nám umožní šířit mnohdy „životně“ důležité informace vhodnou formou a na místa, kde je jich aktuálně nejvíce třeba. Podrobnějšímu kritickému zhodnocení výše zmiňovaných aspektů se věnuje kapitola 3.1.

3 Požadavky na efektivní systém včasného varování

„Občané, podniky, organizace a instituce jsou v rostoucí míře konfrontování se situacemi, vyžadujícími získat v reálném čase adekvátní informace, které by jim umožnily na neobvyklou či mimořádnou situaci odpovídajícím způsobem reagovat. Takovéto informace jsou velmi často potřebné pouze v úzce ohraničených lokalitách. V sousedících či vzdálenějších místech již tato informace nemá význam, naopak občané často potřebují získávat odlišné – adekvátní – aktuální informace.“ (Skrbek, 2010)

3.1 Kritické zhodnocení stávajících systémů

Každý ze systémů popisovaných v kapitole 2.2 má minimálně jednu koncepční nevýhodu, jejímž následkem se informace (přestože je k dispozici) nemusí dostat k reálně či potenciálně ohroženým občanům včas nebo vůbec.

Občané ČR jsou v případě mimořádných událostí odkázáni zejména na Jednotný systém varování a vyrozumění. Koncovými prvky jsou především sirény. HZS ČR udává, že varovným signálem je pokryto přibližně 85 % území ČR (HZS ČR, 2018). Jako přednosti těchto koncových prvků lze zmínit nezávislost na mobilních sítích a Internetu, případně garantovanou funkčnost i v případě přerušení dodávek elektrické energie (72 hodin, za předpokladu 10 minut aktivního provozu). (HZS ČR, 2018)

Problémem těchto koncových prvků je plošný způsob šíření varovného signálu a zároveň jejich omezený dosah. Navíc většina sirén je rotačních, což znamená, že neposkytují konkrétní verbální informaci. V případě mimořádné události a následného vyhlášení signálu všeobecné výstrahy občané nedostanou žádnou konkrétní informaci. Lidem, kteří uslyší zmiňovaný signál, je jasné, že se něco děje, ale těžko se jim odhaduje, o jakou situaci jde a zda se jich přímo týká, nebo jsou mimo nebezpečí. Starší rotační typy sirén jsou velmi pozvolně (viz kapitola 2.2.1) nahrazovány elektronickými sirénami, ale ty situaci příliš nezlepšují. Po odeznění signálu všeobecné výstrahy se sice ozve doprovodná hlasová informace, ale jedná se pouze o několik předem nahraných hlášení, která jsou přehrávána ze záznamu. Autorizované osoby (na úrovni hejtmana, primátora a starosty) mají sice teoretickou možnost přímého vstupu do hlášení sirén, nicméně tato varianta není ani průběžně testována. Hlášení elektronické sirény v případě reálného využití má po odeznění

signálu všeobecné výstrahy následující podobu: *„Všeobecná výstraha, všeobecná výstraha, všeobecná výstraha. Sledujte vysílání Českého rozhlasu, televize a regionálních rozhlasů. Všeobecná výstraha, všeobecná výstraha, všeobecná výstraha.“* V tomto případě tedy obyvatelstvo nedostane bližší informace o typu mimořádné situace. Hlášení nerozlišuje, zda se jedná o chemické, radiační, či jiné nebezpečí. Problémem sirén je i to, že občanům nemusí být signál všeobecné výstrahy povědomý, jelikož při testování sirén každou první středu v měsíci ve 12:00 se používá zkušební tón, který je odlišný.

„Modernějším“ prvkem možnosti varování obyvatelstva v je možnost dostávat informační a varovné SMS. Většina občanů v ČR se může na příslušném obecním nebo městském úřadě zaregistrovat a následně má možnost dostávat varovné a informační SMS zprávy. Nevýhodou je zde: 1) zmíněná potřeba registrace do systému a 2) skutečnost, že provoz těchto systémů je závislý na mobilních sítích. V prvním případě je problémem obecná nechuť se někam registrovat související s obavami ze zneužití osobních informací, z obtěžování irelevantními informacemi apod. Závislost na mobilních sítích může mít za následek to, že se informace k občanům nemusí dostat kvůli výpadku mobilních sítí. Dochází k němu velmi často při živelních katastrofách, jako jsou povodně, vichřice aj. Navíc může být mobilní síť v nutných případech (např. v případě možného zneužití) vyřazena z provozu Policií ČR na základě § 39 *„Rušení provozu elektronických komunikací“* zákona č. 273/2008 Sb. (Zákon o Policii České republiky).

U systémů, které zajišťují sběr, analýzu a vyhodnocení dat (IOTWS, GDACS), je nevýhodou následný krok, který spočívá ve využití získaných informací. Tyto systémy sice dokáží informaci včas distribuovat do operačních center příslušných států, ale konkrétní oblasti, které jsou potenciálně ohroženy, disponují většinou pouze neefektivními varovnými technologiemi, jako jsou například tlampačové systémy rozmístěné na pobřeží.

Závislost používaných technologií na energetických sítích, ať už na straně distributora nebo na straně příjemce informace, je další nevýhodou, kterou bohužel nelze zcela eliminovat. Lze ji pouze snížit s využitím jinak koncipovaných technologických řešení.

Mezi nevýhody současných varovných informačních systémů, které by bylo možné s využitím vhodných implementačních postupů a dostupných technologií eliminovat, patří:

- stávající varovné systémy nepracují s pozicí příjemce,
- v řadě zemí včetně ČR nepracují varovné systémy na principu nuceného příjmu,
- není zajištěna exkluzivita informace vztažená k určité geografické lokalitě.

3.2 Analýza požadavků

Pro stanovení požadavků na efektivní varovný systém, který by do jisté míry mohl odstranit nebo alespoň zmírnit některá negativa systémů stávajících, je nutné vzít v potaz komunikační kanály v dnešní době pro přenos informací využitelné. Jsou jimi:

- rozhlasová síť (analogová, digitální),
- televize,
- internet,
- telefonní síť (pevná, GSM),
- Jednotný systém varování a vyrozumění.

Dále je nutné formulovat některé problémy, které mohou nastat v případě potřeby distribuovat důležité informace do určité lokality:

- závislost informačních a komunikačních technologií na energetických sítích;
- možnost vypnout mobilní sítě ze strany Policie ČR v případě teroristického ohrožení;
- informace není do požadované lokality doručena včas;
- informace není do požadované lokality distribuována vhodnou formou;
- panika způsobená neadekvátností informace v určité lokalitě;
- panika způsobená nevhodně formulovanou informací;
- není zajištěna důvěrnost zprávy;
- problém s evakuací větší skupiny obyvatel v případě omezeného počtu únikových cest.

Z výše uvedeného vyplývají požadavky (bez ohledu na použité technické řešení) na podobu varovného systému určeného pro distribuci informací v případě mimořádných událostí tak, jak je definoval Skrbek (2011). Těmito základními požadavky jsou:

- dostupnost **aktuálně potřebných** informací pro všechny občany;
- nezávislost na funkčnosti mobilních sítí a internetu;

- geografická adresovatelnost pro šíření informací;
- poskytovatelem informace musí být důvěryhodný (autorizovaný) zdroj;
- bezpečnost systému a odolnost proti zneužití;
- finanční a časová realizovatelnost;
- možnost dalšího průběžného testování a prověřování funkčnosti;
- další využitelnost.

Kromě výše uvedených požadavků lze zvažovat i další atributy:

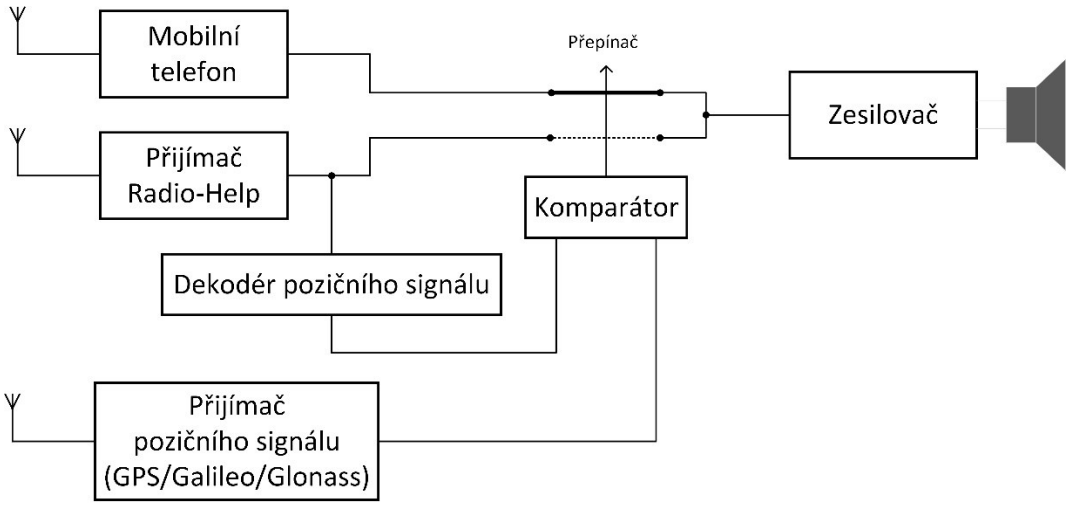
- zajištění důvěrnosti informací;
- anonymita systému, která vyplývá z požadavku na geografickou adresovatelnost informací;
- snadná použitelnost systému ze strany uživatelů.

Anonymitou systému je myšleno to, že potenciální příjemci informací se nemusí do systému registrovat, nemusí být známa MAC adresa zařízení apod. Aby uživatel mohl při pozičně cíleném vysílání pomocí svého zařízení (mobilní telefon s GPS přijímačem) zprávu přijmout, je nutné, aby se nacházel v oblasti, do které je zpráva adresována. Požadavek na důvěrnost informací lze charakterizovat tak, že v určitých specifických situacích, které budou popsány v dalších částech práce ve formě modelových situací, může být z důvodu bezpečnosti nutné zajistit, aby zpráva adresovaná do určité lokality byla šířena jako zpráva šifrovaná. Jinými slovy, v případě, že se osoba bude nacházet mimo oblast určení zprávy, nemůže dojít k tomu, že tato osoba získá dešifrovanou zprávu. Naopak osoba nacházející se uvnitř oblasti určení zprávy musí být schopna ve svém komunikačním zařízení (přijímači) zprávu dešifrovat.

3.3 Radio-Help

Radio-Help (Skrbek, 2010) je systém, který je navržen primárně pro varování obyvatel nejen v případě mimořádných událostí, jako jsou povodně či hromadné nehody, ale i pro varování v případě, že dojde ke kriminální aktivitě či situaci ohrožující bezpečnost obyvatelstva v určité oblasti. Hlavní myšlenkou systému Radia-Help je distribuce velmi potřebných informací s atributem exkluzivity prostřednictvím rozhlasového vysílání. Technicky lze využít princip analogově či frekvenčně modulovaného signálu, do kterého je superponován digitální signál. Tento princip využívá například systém HD Radio, který je používán

zejména v USA. Myšlenka dlouhovlnného vysílání se nabízí zejména proto, že k pokrytí velkého území o velikosti ČR by postačoval jediný vysílač (např. stávající vysílač Topolná), jehož ochrana může být v případě nutnosti zajištěna armádními složkami. Samozřejmostí je ale i možnost využití ostatních vlnových pásem (SV, VKV, UKV), která se využívají pro rozhlasové vysílání. Pro pokrytí ČR signálem programu Český Impuls (AM 981 kHz) postačují dva středovlnné vysílače, které se nacházejí u obcí Líbeznice ve středních Čechách a Domamil na jižní Moravě. Výkon těchto vysílačů je 10 kW a 5 kW, přesto vysílání pokryje prakticky celé území ČR. Navíc lze principiálně systém Radio-Help využít i v digitální komunikační síti. Blokové schéma systému osobního informačního terminálu Radia-Help je znázorněno na obrázku 7.



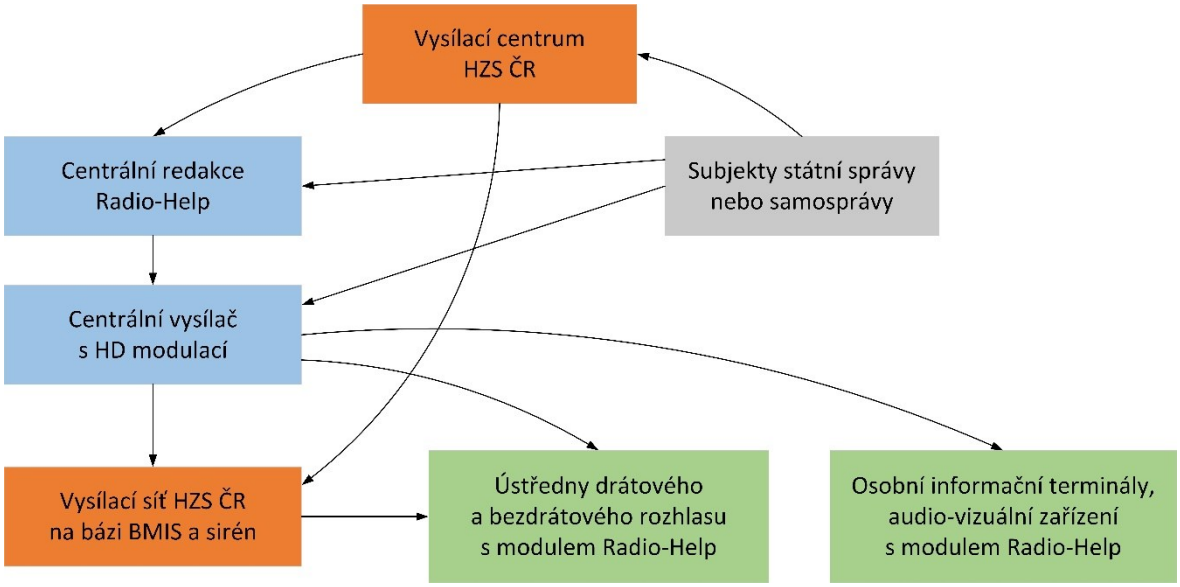
Obrázek 7: Blokové schéma osobního informačního terminálu systému Radio-Help
Zdroj: Skrbek (2010)

Osobní informační terminál je zařízení, jehož základním elementem je mobilní telefon. Tím v dnešní době disponuje většina obyvatel. Do těla mobilního telefonu je zakomponován rozhlasový přijímač signálu Radia-Help a jednotka pro generování pozičního kódu (dnes standardní součást většiny mobilních telefonů). Signál z rozhlasového přijímače je přiveden na vstup dekodéru pozičního kódu. Komparátor porovná kód polohy terminálu s aktuálně vysílaným pozičním kódem signálu Radio-Help. V případě souladu obou kódů aktivuje osobní informační terminál nucený poslech rozhlasové relace, případně zajistí zobrazení varovné zprávy na displeji zařízení.

I přesto, že je informace cílena do vymezené oblasti, existuje z důvodu celoplošné povahy rádiového signálu možnost přijmout informace v podstatě na libovolném místě, pokud bude

mít uživatel ve svém informačním terminálu povolený příjem všech varovných zpráv, tzn. i takových, které jsou mířeny mimo aktuální pozici uživatele. Z tohoto důvodu je žádoucí v určitých případech (viz modelové situace) zajistit pomocí šifrování již zmíněnou exkluzivitu informací pro vymezenou oblast.

Původní koncept systému Radio-Help spočívá v možnosti přidání určitých hardwarových komponent do libovolných zařízení vybavených audio či vizuálními výstupy, tj. i těch, která jsou široce dostupná pro většinu obyvatel – těmi jsou v dnešní době nejen mobilní telefony a rozhlasové přijímače, ale i televizory, přehrávače, počítače, rozhlasové ústředny aj. Lze si ovšem docela dobře představit (stejně jako v případě systému KATWARN) softwarovou implementaci systému Radio-Help, která by fungovala jako aplikace pro nejrozšířenější mobilní operační systémy.



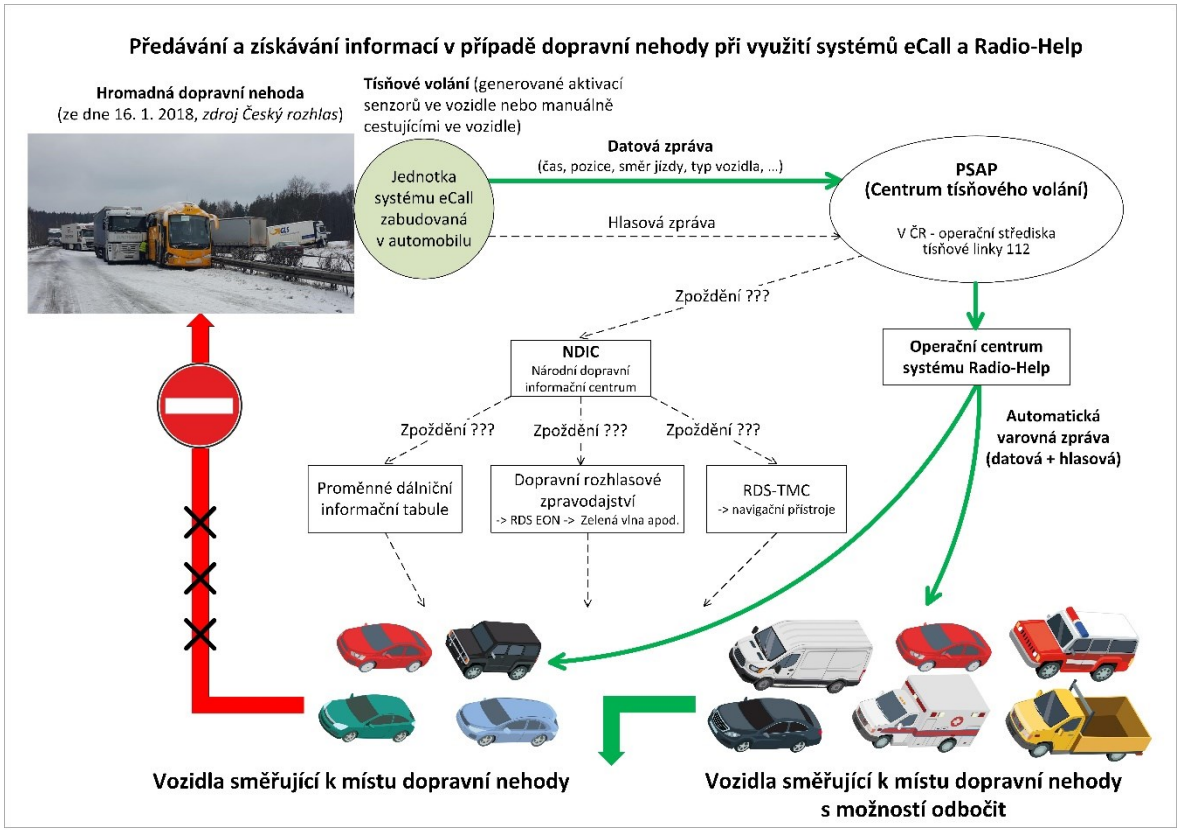
Obrázek 8: Blokové schéma začlenění systému Radio-Help do struktury HZS ČR
Zdroj: Skrbek (2013)

Obrázek 8 naznačuje, jakým způsobem by mohl být systém Radio-Help (RH) začleněn do již existující sítě HZS ČR. Hierarchicky nadřazeným systémem je Vysílací centrum HZS ČR, které zajišťuje tvorbu varovného informačního obsahu. Ten je následně paralelně distribuován do Centrální redakce Radio-Help a do vysílací sítě HZS. V případě krizových situací a závažných mimořádných událostí přebírá Centrální redakce RH obsah z nadřazeného systému. V ostatních případech je varovné vysílání iniciováno Centrální redakcí RH, která zajistí pomocí vysílače s HD modulací distribuci informací směrem

k dalším komponentám systému s cílem co nejrychleji varovat potenciálně ohrožené občany (Skrbek, 2013).

3.3.1 Využití systému Radio-Help

Jedna z navržených koncepcí systému Radio-Help by mohla vylepšit situaci při varování účastníků silničního provozu v případě různých typů dopravních nehod. Situace na obrázku 9 znázorňuje situaci, kdy na dálnici dojde k hromadné nehodě. Jedná se o poměrně běžný typ technogenní mimořádné události, která v mnoha případech nastává v důsledku nějaké abiotické mimořádné události (v ČR se jedná zejména o sněhové kalamity, vichřice apod.). Jedna z nedávných hromadných nehod se stala 16. 1. 2018 na 99. kilometru dálnice D1 u Větrného Jeníkova na Vysočině ve směru na Prahu (iRozhlas, 2018). „Při této hromadné nehodě havarovalo 30 automobilů včetně 10 kamiónů, přičemž některá vozidla byla zaklíněna a musela se vyprostit za pomoci těžké techniky. Naštěstí se tato událost obešla bez obětí na životech, nicméně došlo ke zranění 10 lidí. Provoz ve směru na Prahu byl obnoven v jednom pruhu až následující den kolem osmé hodiny ranní.“



Obrázek 9: Model rychlého doručení varovných informací k řidičům
Zdroj: Vlastní zpracování

Obdobné situace s vysokou naléhavostí evokují otázku, jak snížit čas potřebný k doručení zprávy řidičům, případně pasažérům ve vozidlech, která směřují k místu nehody, s cílem odklonit co nejrychleji co nejvíce vozidel na výjezdech předcházejících místu hromadné nehody. Tím, že by zprávu obdrželo pokud možno co nejvíce řidičů včas, a tím pádem by stihli sjet z dálnice, by se celkově zlepšil průjezd pro vozidla IZS ČR. Včasně obdrženou zprávou by byli varováni i řidiči, kteří již bohužel nemají možnost sjezdu z dálnice, tedy ti, kteří minuli poslední možný výjezd. Nicméně by měli daleko více času reagovat na hromadnou nehodu a eliminovat tak riziko, že se stanou jejími účastníky.

Díky systému eCall se zrychlí distribuce informace o nehodě zejména ve směru k integrovaným záchranným složkám, které díky tomu mohou velmi rychle organizovat záchranné operace a včas zasáhnout. Stále ale není příliš vylepšena informovanost účastníků silničního provozu, kteří se k místu nehody blíží.

Model na obrázku 9 vychází ze situace, kdy se na dálnici stane hromadná nehoda. V současné době neexistuje v České republice nástroj, který by informaci o této nehodě dokázal předat řidičům, kteří se k ní blíží, během několika sekund. Navrhovaný model ukazuje, že při spolupráci systému Radio-Help s technologií eCall lze zajistit, že řidiči obdrží důležitou informaci včas. Zpráva se zobrazí uživateli na mobilním telefonu (nebo na jiném typu mobilního zařízení) a navíc se předpokládá, že řidič bude upozorněn na blížící se nebezpečí také nucenou hlasovou zprávou. Řidiči by mohli včas adekvátně zareagovat, a pokud se nacházejí před nějakým dálničním sjezdem, měli by možnost sjet z plánované trasy a objet místo, kde se stala nehoda. Informační toky v případě použití technologií Radio-Help + eCall jsou na obrázku 9 znázorněny plnou čarou zelené barvy. Jde o informace, které řidič obdrží s minimálním zpožděním. Čárkované čáry znázorňují informační toky, které odpovídají dnes používaným technologiím, mezi něž patří RDS, RDS-TMC nebo informační tabule. Šíření těchto informací zajišťuje a koordinuje Národní dopravní informační centrum (NDIC). Bohužel čas potřebný pro doručení zprávy k příjemcům se pohybuje v řádech minut, nikoli sekund. Výsledkem toho je, že řidiči nemohou zareagovat (nehodu objet) a uvíznou v dopravní zácpě, v horším případě se mohou stát součástí hromadné nehody.

4 Modelové situace

V této kapitole jsou popsány dvě modelové situace, které vycházejí z reálných hrozeb aktuálních zejména v dnešní době – tedy nebezpečí terorismu a kriminálních aktivit. Třetí situace má technogenní charakter. Čtvrtá modelová situace spadá do kategorie mimořádných událostí způsobených přírodními katastrofami. Společným jmenovatelem všech čtyř situací je zamýšlené využití poziční distribuce informací (koncepce systému Radio-Help), jež je založena na principu lokálně kontextových služeb (LBS – Location Based Services). Příjemci informace jsou tedy uživatelé zařízení, která se nacházejí v určité oblasti, a nikoliv uživatelé s konkrétními telefonními čísly, IP adresami nebo MAC adresami svých zařízení. Jinými slovy, není dopředu známo, jaká konkrétní zařízení se vyskytnou v oblasti, do níž je nutné varovnou informaci odeslat.

4.1 Motivační aspekty pro návrh modelových situací

Od začátku roku 2015 je bezpečnostní situace v Evropě spojena s teroristickými útoky, které svojí brutalitou i stylem provedení představují nový fenomén, jímž je evropská společnost do značné míry zaskočena. V prvních lednových dnech 2015 se na první stránky novin a zpravodajských relací dostal útok na redakci časopisu Charlie Hebdo. Na konci února francouzskou tragédii vytěsnila z „headline news“ tragédie v uherskobrodské restauraci. Mimořádná brutalita zdánlivě zcela rozdílných událostí má však společného jmenovatele – v současnosti neexistuje v okamžicích napadení, útoků, teroristických akcí či stíhání pachatelů účinný komunikační prostředek umožňující chránit nebo varovat potenciálně ohrožené obyvatele nebo ovlivňovat jejich chování. Zákony o kybernetické bezpečnosti umožňují vypnout veškerá komunikační média. V řadě případů však takováto opatření mohou být kontraproduktivní a nebyla ve výše zmíněných případech použita. (Žižka, 2015b)

Cílem této kapitoly je naznačení cesty k hledání možného komunikačního prostředku efektivní pomoci ohroženým občanům i zasahujícím jednotkám. Pro připomenutí je níže uvedena stručná rekapitulace obou událostí.

8. ledna bratři Chérif a Said Kouachiové, vrahové z redakce týdeníku Charlie Hebdo, přepadli na svém útěku benzinovou stanici severně od Paříže. Oba muži se dle mediálních informací pohybovali v okolí města Villers-Cotteret. Dalším údajným úkrytem teroristů byla obec Longpont se třemi stovkami obyvatel, kterou policisté před dvaadvacátou hodinou

prohledávali dům po domu. Poté se obdobným způsobem zaměřili i na nedalekou vesnici Corcy. Obyvatelé měli zakázáno vycházet z domovů. Druhý den se pátrání po obou mužích soustředilo na oblast asi 80 kilometrů severovýchodně od Paříže. Policie oblast zcela uzavřela (u zátarasů však čekaly na další vývoj štáby televizí a dalších médií). Místní obyvatelé v této době prožili desítky hodin ve stresu a velkém strachu, že na ně uprchlíci v obydlích či venku zaútočí.

V závěrečné fázi dopadení pachatelů útoku na Charlie Hebdo bylo do akce zapojeno 88 000 policistů a vojáků. Přepadová komanda zasáhla současně jak proti dvojici mužů zabarikádovaných po celý den v areálu tiskárny ve městě Dammartin-en-Goële, tak proti útočníkovi, který držel rukojmí v židovském obchodě v Paříži. Je evidentní, že cena opatření pro zajištění bezpečnosti je enormní. Odhlédneme-li od ceny, kterou daňoví poplatníci zaplatili v přímé souvislosti se zneškodněním teroristů z redakce časopisu Charlie Hebdo, následné náklady spojené s vysláním 10 000 vojáků na řadu týdnů ke střežení veřejných míst původní částku mnohonásobí. Kromě toho se francouzská vláda rozhodla rozšířit zpravodajské služby o tisíce nových pracovníků.

Příběh z Uherského Brodu byl z hlediska pohnutek útočníka odlišný, dopady hrůzného činu však byly obdobné. V úterý 24. února 2015 ve 12.30 třiašedesátiletý Zdeněk Kovář zastřelil osm osob v restauraci Družba a o necelé dvě hodiny později při akci policejní zásahové jednotky spáchal sebevraždu. Mezitím telefonicky hovořil s redaktorem zpravodajství televizní stanice Prima.

Celou policejní akci provázala řada kontroverzních informací a rozhodnutí. Jediný přímý svědek přišel se zajímavou a zároveň hrozivou informací. V rozhovoru pro časopis Respekt řekl, že ze svého úkrytu slyšel, jak televize v restauraci přináší zprávy z místa masakru. Zdeněk K. tak mohl v přímém přenosu sledovat, co se proti němu chystá.

Pozičně cílené informace by ve výše uvedených případech mohly přispět k efektivnější informovanosti obyvatel například těmito způsoby:

- upozornit obyvatele obcí Longpont a Corcy na potenciální nebezpečí s žádostí o sdělení podstatných informací na konkrétní telefonní číslo;
- pokud možno doplnit zákaz vycházení o „uklidňující informace“;

- zprostředkovat instrukce, jak se v dané situaci chovat, s cílem snižování stresu a případné paniky;
- předat varování a instrukce občanům v okolí restaurace s cílem zajistit, aby se tyto informace nedostaly k útočníkovi.

Není prokazatelné, zda by pozičně cílená informace dokázala eliminovat tragické ztráty na životech. Lze si však snadno představit modelové situace, kdy lokálně cílená potřebná informace může ochránit zdraví, životy a majetek obyvatel i institucí. K pozičnímu varování a vyrozumění byl navržen systém Radio-Help. Digitální rozhlas, ať už šířený po internetu nebo terestriálním vysíláním, nabízí možnosti cíleného směřování vysílání navíc tak, aby mimo vymezené oblasti nebylo možné rozhlasové vysílání přijímat. Technologie šifrování na základě pozice cílové oblasti by umožnila efektivně varovat osoby před vstupem do ohrožených oblastí, aniž by tyto informace mohli útočníci v jiných oblastech zjistit.

4.1.1 Hrozby současného terorismu

Dalším motivačním aspektem pro hledání nových způsobů distribuce informací v případě teroristického nebezpečí je článek z časopisu Economist (2015), který byl vydán krátce po zmíněných útocích na redakci časopisu Charlie Hebdo a který poukazuje na to, proč je v současné době boj proti terorismu stále složitější.

a) V lednu 2015 oznámil ředitel evropské policejní agentury Europol, že ve válečných konfliktech na Blízkém východě, ale i v Africe bojuje až 5 000 občanů Evropské unie, kteří se připojili do řad islámských extrémistů, a hrozí, že se někteří z těchto radikálů mohou vrátit a pokusit se o atentáty na území EU.

Velmi alarmující je pro země EU nejen samotné navýšení počtu potenciálních útočníků, ale i další faktory: radikálové pocházejí z EU, takže dokáží efektivně využívat internet a moderní technologie; jsou organizováni decentralizovaně, nemají jednotné velení, mnohdy se jedná i o jednotlivce. Útoky jsou sofistikovanější, z čehož vyplývá, že pro protiteroristické organizace je velmi náročné eliminovat všechny potenciální hrozby a zastavit jednotlivé útoky. Proto se riziko terorismu v současné době dotýká každého z nás.

Paradoxně se po tom, co byla v prosinci 2017 vyhlášena porážka Islámského státu, zvýšilo nebezpečí terorismu pro Evropu. Bojovníci, kteří z Evropy odešli bojovat za IS, se nyní

budou do svých domovských zemí vracet, a tím pádem hrozí nebezpečí, že se stanou organizátory potencionálních útoků v EU. Z evropského pohledu tedy nebezpečí terorismu nepominulo, ale naopak se zvýšilo.

b) Druhým důvodem je, že útoky ve stylu napadení komandem je snadné naplánovat, ale obrana proti nim je komplikovaná. Nemusí se zabít tolik obyvatel jako v případě útoku na letadlo, důležitá je propaganda těchto činů, která šíří myšlenku, že je možné naprosto ochromit obyčejný život v důležitém městě s bonusem nepřetržitého vysílání ve zpravodajských relacích.

c) Dalším problémem v boji proti terorismu je to, že západní bezpečnostní organizace ztrácejí technologický náskok, který by jim umožnil monitorovat komunikaci potenciálních teroristů. Jedním z důvodů je i to, že technologické společnosti se předhánějí v úsilí poskytovat svým zákazníkům „neprolomitelnou“ ochranu soukromí prostřednictvím sofistikovaného šifrování, které je někdy nabízeno i v základní výbavě dodaných komunikačních zařízení.

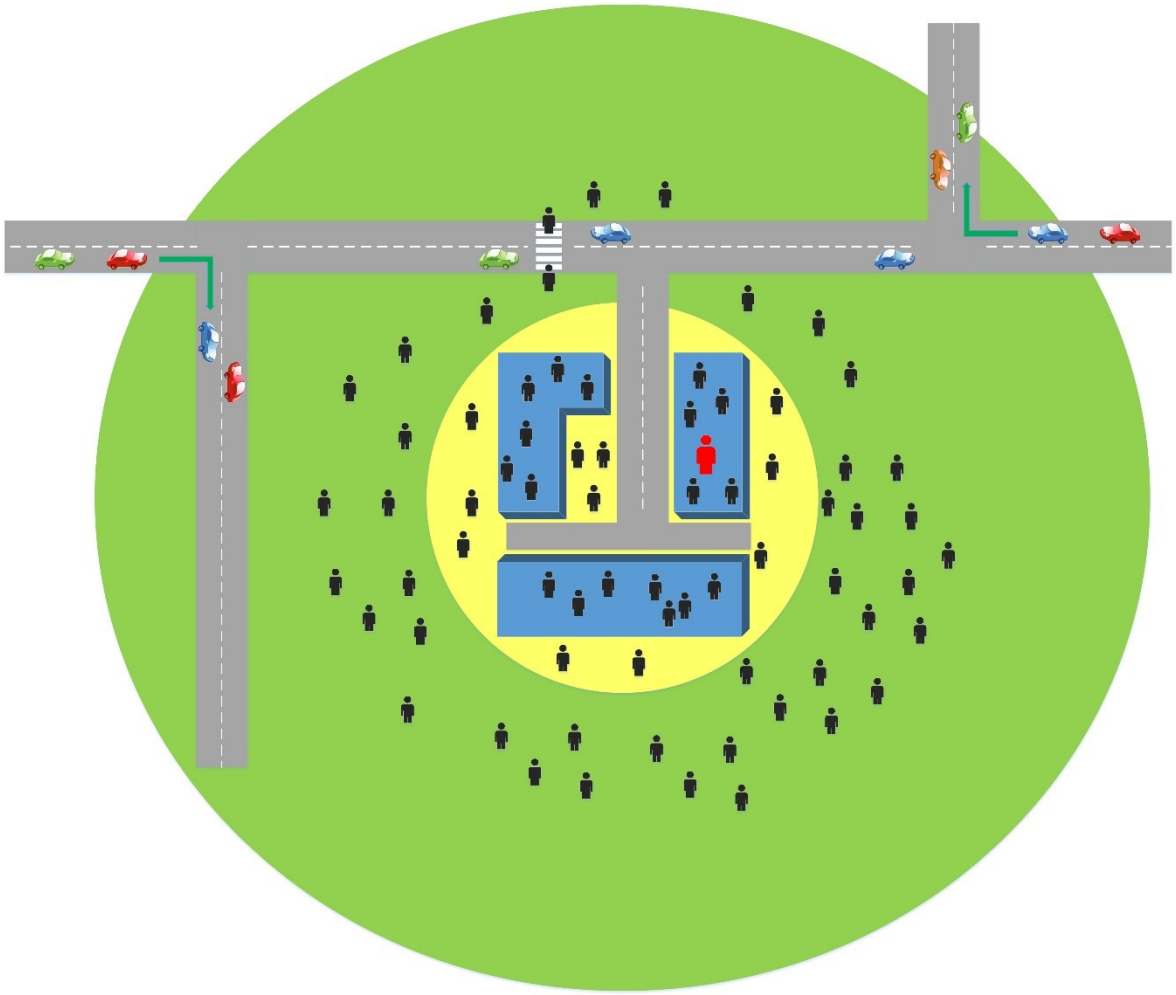
4.2 Varování obyvatel před vstupem do nebezpečné oblasti

Popis modelové situace

Uvnitř blíže nespecifikovaného nákupního centra větší rozlohy (epicentrum nebezpečí) je spatřen celostátně hledaný a potenciálně ozbrojený zločinec. Že jde o zločince, bylo zjištěno prostřednictvím kamerového systému, případně s pomocí lidského faktoru. Následně je o výskytu nebezpečné osoby informována policie a ostraha objektu. Policie je schopna v poměrně krátké době zajistit koordinační akce související se zajištěním bezpečnosti uvnitř objektu, případně v jeho těsné blízkosti. Z důvodu dalšího policejního zásahu v jiné části města nemá policie dostatečný počet policistů, kteří by fyzicky uzavřeli cesty a silnice směřující k nákupnímu centru.

Dále je totiž nutné varovat občany, kteří směřují k potenciálně nebezpečné oblasti nebo se pohybují v její blízkosti, pro případ, že v dané oblasti dojde k zásahu nebo by zásah proti zločinci skončil neúspěchem. Cílem je tedy minimalizovat nebezpečí, tzn. informovat pokud možno co největší množství lidí o tom, že se blíží k nebezpečné oblasti, a zároveň tyto informace uchovat v utajení před zločincem. Vzhledem k tomu, že příjezd policie (i přes

rychlou reakci) do oblasti zásahu zabere určitý čas, je žádoucí, aby obyvatelé směřující do blízkosti epicentra byli varováni co nejdříve – tedy již během doby, kdy se policie přesouvá na místo zásahu. Vhodným systémem pro varování obyvatelstva by v těchto případech mohla být právě koncepce podobná systému Radio-Help, jelikož bezprostředně po zjištění přítomnosti zločince by bylo možné odeslat varovnou zprávu do cílové oblasti s tím, že by se zde navíc (z níže uvedených důvodů) využil princip šifrování informací závislého na poloze příjemce.



Obrázek 10: První modelová situace
Zdroj: vlastní zpracování

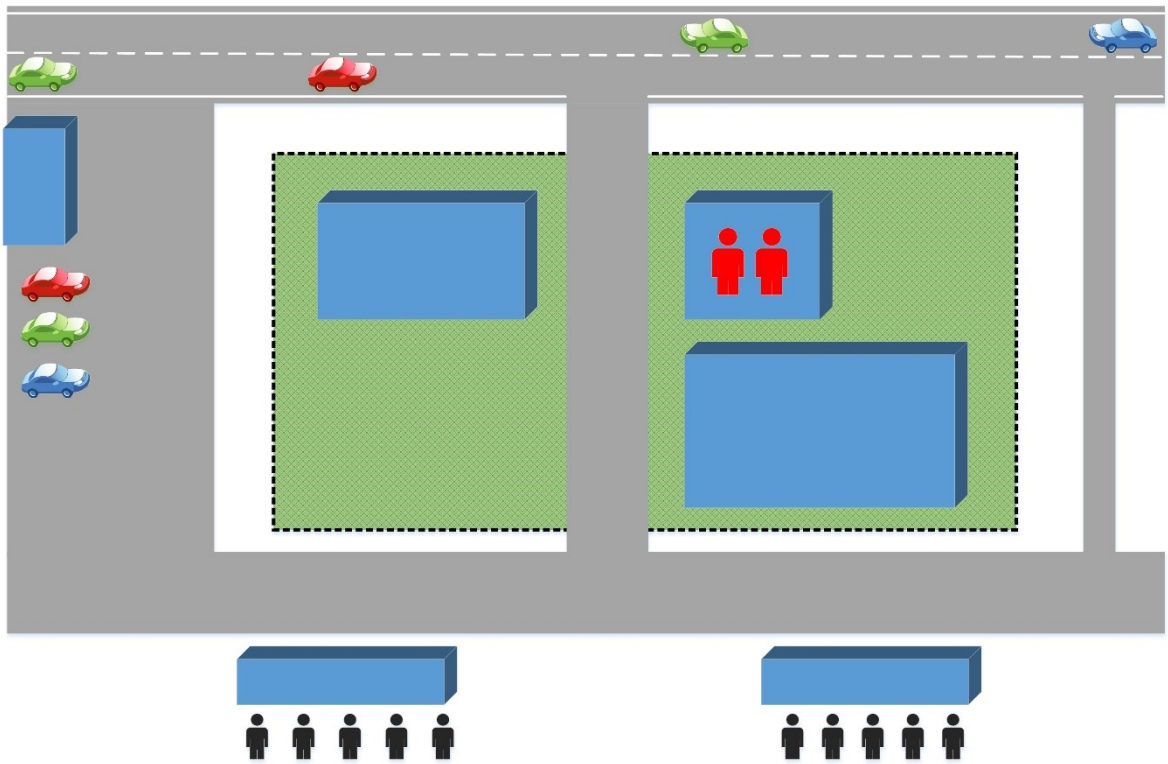
Jelikož distribuci informací uvnitř epicentra nebezpečí a v jeho těsné blízkosti řeší policie přímo, bylo by nežádoucí, aby byli lidé uvnitř oblasti „ohroženi“ další zprávou určenou pro jinou skupinu. Mohlo by to mezi nimi vyvolat paniku a současně způsobit nepředvídatelnou reakci zločince. Proto je důležité, aby byly zprávy distribuované prostřednictvím uvedeného informačního kanálu utajeny před zločincem i před bezprostředně ohroženými lidmi. Jinými

slovy, v oblasti vymezené jako epicentrum nebezpečí musí být v tomto případě zpráva distribuovaná prostřednictvím tohoto varovného kanálu nesrozumitelná.

Grafickou prezentaci modelové situace zachycuje obrázek 10. Oblast, kde by měla být přijata dešifrovaná zpráva, je vyznačena zelenou barvou. Oblast nákupního centra a žlutou barvou vybarvený kruh jsou oblasti, pro které by měla být zpráva šifrovaná (nesrozumitelná). Poloha ozbrojeného zločince je na obrázku 10 označena červenou postavou.

4.3 Cílená dezinformace směřovaná do epicentra nebezpečí

Tento model se vyznačuje odlišnou filozofií (viz obrázek 11) a vychází ze skutečné situace popsané v úvodní části tohoto článku, kdy se skupina uprchlých teroristů zabarikádovala v areálu tiskárny. Zde se nabízí možnost dezinformovat uprchlíky o činnosti bezpečnostních složek a jejich plánech, což by mohlo vést k tomu, že se uprchlíci rozhodnou k určité akci – k útěku.



Obrázek 11: Druhá modelová situace
Zdroj: vlastní zpracování

Takovou dezinformací může být např. příprava na vniknutí policistů do areálu severním vchodem nebo soustředění pozornosti policie na základě telefonátu na jinou oblast, kam přesouvá své složky. Vezměme v úvahu fakt, že teroristi disponují komunikačním zařízením (mobilní telefon) a že mají vně areálu komplice, který by je mohl informovat a sdělit jim, že největší skupina policistů je ve skutečnosti připravena u jižního vchodu. Opět je zde klíčové, aby informace (dezinformace), která bude distribuována pomocí pozičního vysílání do vymezené oblasti (areál tiskárny), byla pro ostatní místa zašifrovaná, a tudíž na dalších pozicích nečitelná. V porovnání s předchozí modelovou situací jde tedy o situaci inverzní – nešifrovaná informace je zde směřována do epicentra nebezpečí. Cílová oblast pro příjem nešifrované zprávy je v obrázku vyznačena zeleným obdélníkem. Zároveň je možné do jiných oblastí zasílat šifrované zprávy jiného typu (např. uklidňující).

4.4 Řízená evakuace z ohrožené oblasti

Tato podkapitola se v první části zaměřuje na modelovou situaci spojenou s typem ohrožení, které je velmi reálné i v našich zeměpisných podmínkách, a to ohrožení související s narušením hrází vodohospodářských děl. Druhá část podkapitoly se věnuje nebezpečí obrovských vln tsunami, jež je charakteristické pro přímořské lokality, zejména místa na pobřeží Indického a Tichého oceánu.

4.4.1 Modelová situace – ohrožení vzniklé poškozením vodního díla

Přehradní nádrže (přehrady) spadají pod označení vodní dílo. Vodní dílo je pojem, který souhrnně označuje všechny stavby, které slouží k zadržování, jímání, vedení nebo k jinému nakládání s povrchovou a podzemní vodou (Mareš, 2013). § 55 odst. 1 vodního zákona č. 254/2001 Sb. charakterizuje vodní díla jako stavby, které slouží *„ke vzdouvání a zadržování vod, umělému usměrňování odtokového režimu povrchových vod, k ochraně a užívání vod, k nakládání s vodami, ochraně před škodlivými účinky vod, k úpravě vodních poměrů nebo k jiným účelům sledovaným tímto zákonem“*. Podle Říhy (2011) význam přehrad spočívá zejména v zachycení vody pro obyvatelstvo a průmysl, případně k zadržení vody v případě menších povodňových vln.

Počet významných vodních děl v ČR je uveden v tabulce 4. Zdrojem dat jsou webové portály jednotlivých státních podniků Povodí, které jsou sdruženy pod **Elektronickým digitálním**

povodňovým portálem na adrese https://www.edpp.cz/. Primárním účelem tohoto portálu je shromažďovat relevantní informace, které souvisejí s povodňovým nebezpečím. Součástí portálu jsou **povodňové plány** jednotlivých obcí rozdělené hierarchicky na kraje, ORP a obce. Dále je zde k dispozici online povodňová mapa ČR, kde lze získat aktuální informace ze srážkoměrů a hladinoměrů.

Tabulka 4:Počet významných vodních děl v ČR

Celkový počet významných vodních děl spravovaných státními podniky Povodí	**134**
Povodí Moravy – počet významných vodních děl (spravuje Povodí Moravy, s.p., web: www.pmo.cz)	47
Povodí Vltavy – počet významných vodních děl (spravuje Povodí Vltavy, s.p.; web: www.pvl.cz)	35
Povodí Labe – počet významných vodních děl (spravuje Povodí Labe, s.p.; web: www.pla.cz;)	20
Povodí Odry – počet významných vodních děl (spravuje Povodí Odry, s.p.; web: www.pod.cz)	8
Povodí Ohře – počet významných vodních děl (spravuje Povodí Ohře, s.p.; web: www.poh.cz)	24

Zdroj: http://voda.gov.cz/portal/cz/

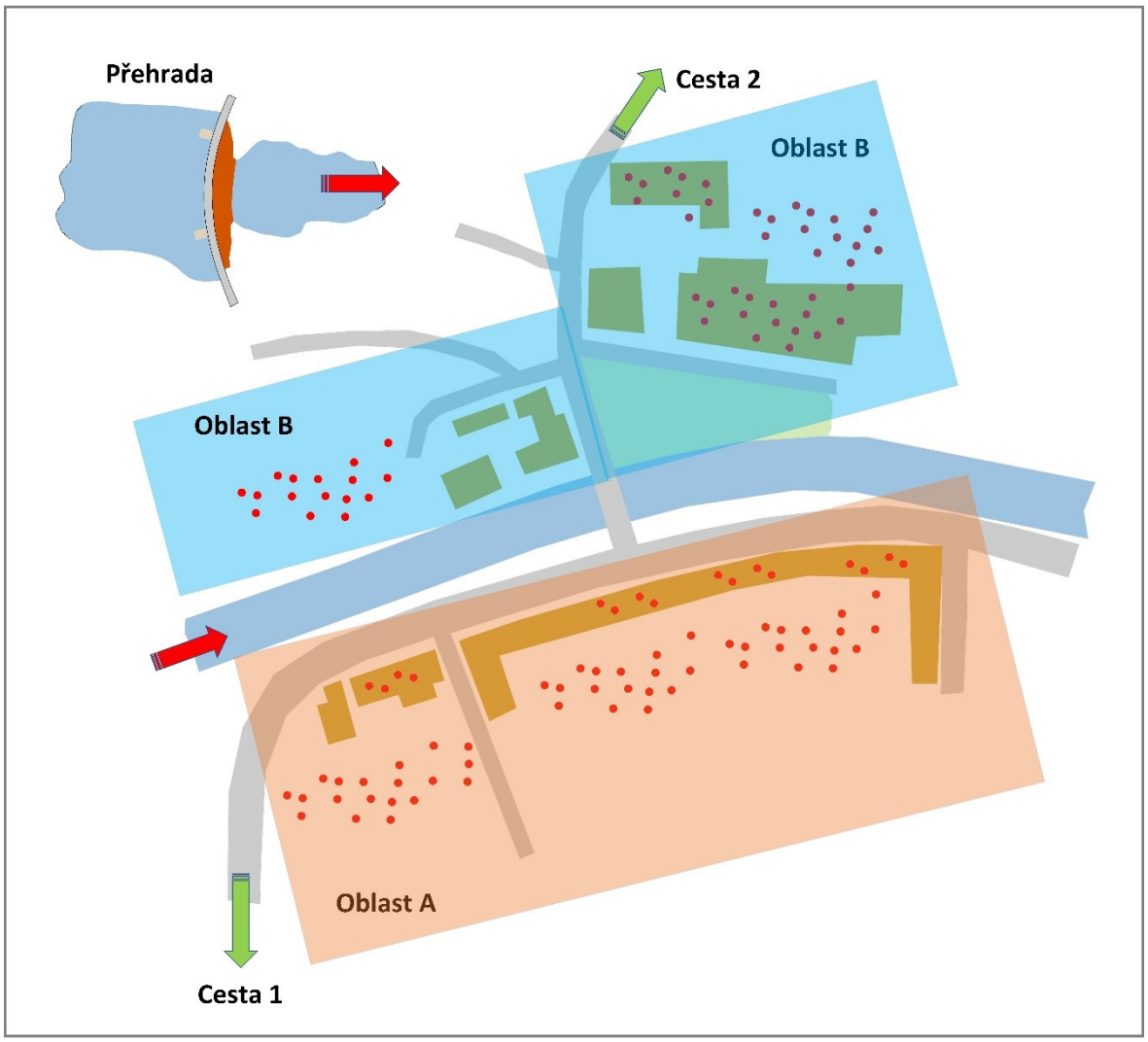
Motivačním aspektem pro vytvoření následující modelové situace je jednak velký počet přehradních nádrží na území České republiky a dále skutečnost, že přehradní nádrže mohou z pohledu bezpečnosti občanů představovat riziko pro blízké i vzdálenější lokality. To se může projevit v průběhu živelních pohrom, případně po napadení nepřátelskými silami. Míra rizika je závislá zejména na velikosti stavby, na vodním objemu, který stavba zadržuje, a také na technickém stavu vodního díla. Některé přehradní nádrže v ČR byly postaveny a zprovozněny před druhou světovou válkou (např. v roce 1920 Les Království poblíž Dvora Králové nad Labem, v roce 1930 Luhačovice, v roce 1934 Vranov nad Dyjí). I přesto, že na bezpečnost, spolehlivost, kontrolu a údržbu těchto staveb se klade velký důraz, může být vyšší stáří takové stavby jedním z faktorů zvýšeného rizika. Technické požadavky na průběh vodních staveb stanovuje v ČR vyhláška č. 590/2002 Sb. o technických požadavcích pro vodní díla, ve znění pozdějších předpisů. Poslední novela této vyhlášky se datuje k 1. 1. 2005. Je s podivem, že i přes skutečnost, že od roku 2005 byly různé oblasti ČR zasaženy povodněmi většího rozsahu, nebyla tato vyhláška prozatím aktualizována.

Množství vody zejména při povodňových stavech, které přehrady musí zadržovat, je enormní a, tomu odpovídá i naakumulovaná energie, která se v případě poškození takové

stavby uvolní a může velmi rychle ohrozit nejen majetek, ale hlavně životy obyvatel v oblastech pod vodním dílem.

Popis modelové situace

Třetí model (obrázek 12) znázorňuje mimořádnou situaci, v níž reálně hrozí protržení přehrady v blízkosti města.



Obrázek 12: Třetí modelová situace
Zdroj: vlastní zpracování

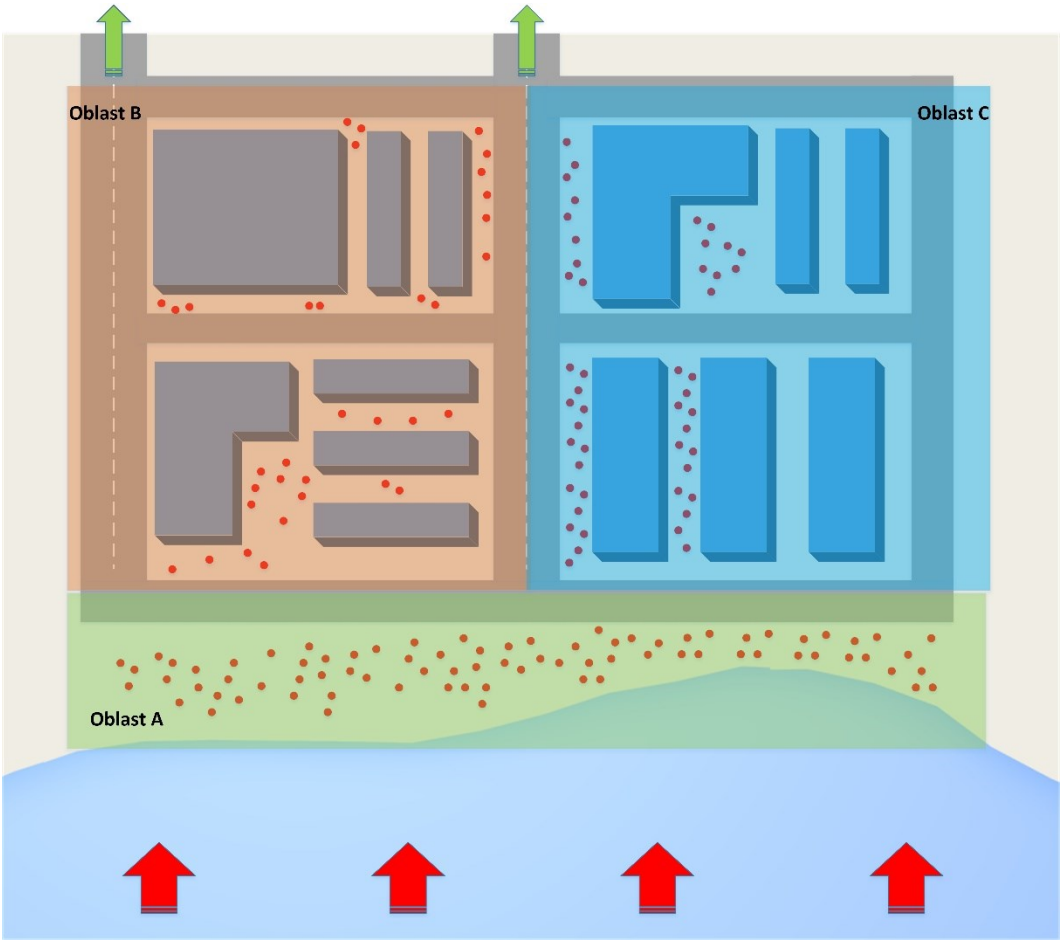
Přehrady jsou samozřejmě koncipovány tak, aby ani za „obvyklých“ mimořádných okolností nedošlo k jejich poškození. Nicméně hrozba protržení nastat může, a to například v důsledku dlouhotrvajících nepříznivých klimatických podmínek, nepředvídatelného teroristického útoku, případně kombinace několika negativních faktorů včetně přehlédnutého nedostatku stavebního charakteru.

Pokud by došlo k náhlému a nečekanému protržení přehrady, byla by situace kritická a čas na záchranu a evakuaci ohrožených částí blízkého města by byl minimální. V případě mimořádné události tohoto charakteru však není ohroženo jen nejbližší město, ale samozřejmě i další města a vesnice dále po proudu. Situace tedy vychází z předpokladu, že nebezpečí protržení přehrady je sice reálné, ale ne zcela bezprostřední (nastane-li, pak v průběhu několika hodin). V takovém případě je k dispozici určitý časový prostor pro organizaci a provedení evakuace. Pokud by ale evakuace probíhala chaoticky a hromadně, například v důsledku vyhlášení mimořádné situace běžnými prostředky JSVV nebo prostřednictvím médií, nemusela by být ani tato doba dostatečná.

Cílem je zajistit oddělenou, postupně řízenou evakuaci tak, aby nedocházelo ke směšování jednotlivých skupin obyvatel. Pro obyvatele z oblasti A je určena úniková cesta 1, analogicky pro obyvatele z oblasti B je to cesta 2. Plán zahrnuje i možnost, že Police ČR na základě posouzení závažnosti situace omezí na nutnou dobu provoz mobilních sítí a internetu – na základě § 39 „Rušení provozu elektronických komunikací“ zákona č. 273/2008 Sb. (Zákon o Policii České republiky). Následně příslušné operační středisko HZS ČR začne distribuovat do oblastí A a B pozičně šifrované varovné a koordinační zprávy v hlasové i textové verzi. Pro oblast A to znamená pokyny směřující k evakuaci únikovou cestou 1, pro oblast B pokyny k úniku cestou 2. Předpokládá se, že by většina obyvatel využila k opuštění města automobily.

4.4.2 Modelová situace pro přímořské lokality

Čtvrtá modelová situace (viz obrázek 13) spadá do oblasti mimořádných událostí způsobených přírodní katastrofou – konkrétně se jedná o řízenou evakuaci osob z pobřeží, které je ohroženo tsunami. Přestože je model konkrétně zaměřen na tsunami, lze ho zobecnit i pro další případy, kdy je nutná evakuace většího množství ohrožených osob. (Žižka, 2015a).



Obrázek 13: Čtvrtá modelová situace
Zdroj: vlastní zpracování

Situace vychází ze skutečnosti, že existují systémy (viz kapitola 2.2.7), které jsou za několik málo minut po vzniku tsunami schopné vyhodnotit tento jev a poměrně přesně určit, kdy a kde tsunami zasáhne pobřeží a jakou silou. Pokud je epicentrum zemětřesení, jehož důsledkem jev tsunami vzniká, daleko od pobřeží, je k dispozici určitý „reakční čas“ na organizaci zajištění bezpečnosti potenciálně ohrožených obyvatel a turistů. Tsunami se ve volném oceánu šíří rychlostí 900 km/h, ale směrem k pobřeží jeho rychlost klesá a při nárazu na pobřeží dosahuje rychlosti 25–35 km/h (International Tsunami Information Center, 2017). Regionální operátoři dostanou potřebné informace a poměrně přesné simulační modely za velmi krátký čas. Bohužel ale není zatím příliš efektivně řešen následující krok, a to evakuace obyvatelstva z oblasti, do které např. během dvou hodin tsunami udeří. Na několika místech oblastí s rizikem tsunami jsou v současné době rozmístěny tlampače, které mají v případě nebezpečí varovat obyvatelstvo. Problémem ale může být panika, která se velmi rychle šíří a v jejímž důsledku mnohdy dochází k ucpání silničních komunikací a přístupových cest. Navíc hrozí i to, že panika vznikne i na místech, která bezprostředně

ohrožena nejsou, čímž se propustnost směrem do centra určitého města (tedy pryč od pobřeží) ještě zhorší. (Skrbek, 2015)

Zde se tedy nabízí využít zmiňované distribuce informací s využitím pozičního šifrování, neboť lze zajistit, aby varovná zpráva určená pro konkrétní oblast nemohla být přijata na jiném místě. V důsledku toho by mohlo dojít k postupné evakuaci po určitých oblastech – zde např. nejprve oblast C, následně oblast B a nakonec oblast A. Tento krok by ale měl být doprovázen dalšími opatřeními, např. vypnutím mobilních sítí, neboť v případě, že by mobilní síť fungovala dále, nezabránilo by se výše popisovanému šíření paniky do dalších oblastí. Samotné evakuační scénáře by měla vypracovat města, územní celky apod. v závislosti na geografických možnostech a dalších aspektech.

5 Poziční šifrování

V této kapitole bude čtenář seznámen s principem šifrování založeným na poloze příjemce (dále jen poziční šifrování). Nejprve je ale nutné vymezit základní kryptografické pojmy, o které se princip pozičního šifrování opírá. Vzhledem k tomu, že se koncepce popisovaného varovného systému s atributem exkluzivity informace pro určitou lokalitu opírá zejména o principy symetrické kryptografie, budou se informace v této kapitole zaměřovat převážně na tento typ kryptografie.

5.1 Úvod do kryptografie

Počátky kryptografie spadají do období vzniku písma (přelom 4. a 3. tisíciletí př. n. l.). Současně se schopností lidstva zaznamenávat informace pomocí písma vznikla potřeba jejich zabezpečení s cílem, aby zapsané údaje byla schopna přečíst pouze oprávněná osoba. V tomto období vznikaly první utajovací kryptografické systémy, ale současně s nimi se rozvíjela i kryptoanalýza, které spočívala v pokusech o překonávání těchto systémů bez znalosti příslušného dešifrovacího klíče. Obě vědy se v historickém průběhu svého vývoje komplementárně stimulovaly. V případě vzniku nového kryptografického algoritmu vznikaly nové kryptoanalytické metody se snahou o jeho prolomení a naopak.

5.1.1 Základní kryptologické pojmy

Podle Burdy (2015) lze **kryptografii** definovat jako vědu, která se zabývá konstrukcí a aplikací matematických metod zajišťování důvěrnosti a autentičnosti zpráv. Komplementární vědou ke kryptografii je **kryptoanalýza**, která může být analogicky definována jako věda o překonávání matematických metod zajišťování důvěrnosti a autentičnosti zpráv. Společně pak kryptografie a kryptoanalýza tvoří vědu, která se nazývá **kryptologie**. Důvěrnost zprávy je stav, kdy je zpráva známa pouze jejímu odesílateli a příjemci. Autentičnost zprávy je stavem, ve kterém jsou předpoklady příjemce o odesílateli přijaté zprávy pravdivé.

Šifrovacím algoritmem v kryptografii rozumíme výpočetní postup k transformaci zprávy do podoby kryptogramu. Tato transformace se nazývá šifrovací funkce. **Kryptogram** je šifrovaný text, který vznikne z původní zprávy jako výsledek této transformace. Ke kryptogramu má obecně přístup kdokoli, tedy i útočník. Důvěrnost zprávy je zajištěna tím,

že pro provedení zpětné transformace kryptogramu na původní zprávu (tzv. otevřený text) je nutné, aby příjemce disponoval utajovanou informací, kterou nazýváme **šifrovací klíč**. Osoby bez znalosti šifrovacího klíče by neměly být zpětné transformace schopny. Šifrovací funkce musí být vytvořena tak, aby kryptogram odolal útočníkovi po určitou dobu, která se označuje jako **doba rezistence kryptogramu**. To znamená, že útočník bez znalosti dešifrovací funkce nesmí odvodit původní zprávu dříve než za stanovenou dobu rezistence.

Kryptografický protokol je algoritmus, na jehož provádění se podílí více stran (odesílatel a příjemce) a který by měl zajistit, aby byly splněny všechny podmínky pro zabezpečenou výměnu informací mezi odesílatelem a příjemcem. Kryptografickým systémem (kryptosystémem) je systém algoritmů určený k zajištění důvěrnosti a/nebo autentičnosti zprávy (Burda, 2013).

Kryptografické systémy lze rozdělit na následující typy:

- utajovací – zajišťují pouze důvěrnost zpráv;
- autentizační – zjišťují pouze autentičnost (důvěryhodnost) zpráv;
- hybridní – zajišťují důvěrnost i autentičnost zpráv.

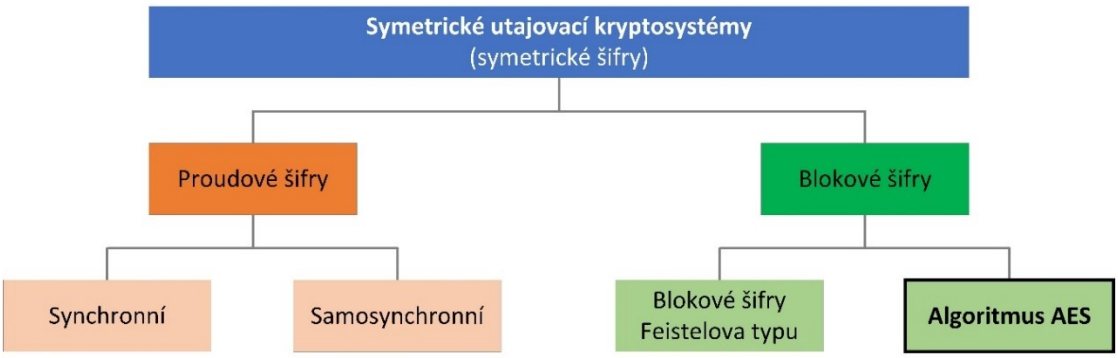
Základním principem kryptografie je to, že bezpečnost proti prolomení kryptografických systémů není závislá na použitých algoritmech, které mohou být veřejně známé, ale na klíčích, které se při šifrované komunikaci používají. To neznamená, že šifrovací algoritmy jsou vyvíjeny jako veřejně známé, ale že musí být navrženy tak, aby odolaly pokusu o útok v případě, že útočník zná velmi dobře jejich princip. Bezpečnost samotných kryptografických algoritmů tedy spočívá zejména v použití dostatečně dlouhých šifrovacích klíčů, které musí být vytvořeny tak, aby nebyly prolomeny ani po důkladném a sofistikovaném útoku.

Z pohledu šifrovacích klíčů můžeme rozdělit kryptografické metody do dvou základních kategorií: **symetrické** algoritmy a **asymetrické** algoritmy.

5.1.2 Symetrické kryptografické systémy

Symetrické algoritmy lze dále dělit na utajovací (šifrovací klíč a dešifrovací klíč) a autentizační (pečetící klíč a ověřovací klíč). V případě symetrických kryptosystémů jsou klíče všech zúčastněných stran tajné a používá se zpravidla stejný klíč pro šifrování

informace i pro její dešifrování. Zajištění tohoto klíče proti odcizení třetí stranou je zde klíčovým aspektem bezpečnosti, a vyvstává tedy otázka, „jak lze bezpečně sdílet šifrovací klíče?“.



Obrázek 14: Základní klasifikace symetrických kryptografických systémů
Zdroj: Vlastní zpracování

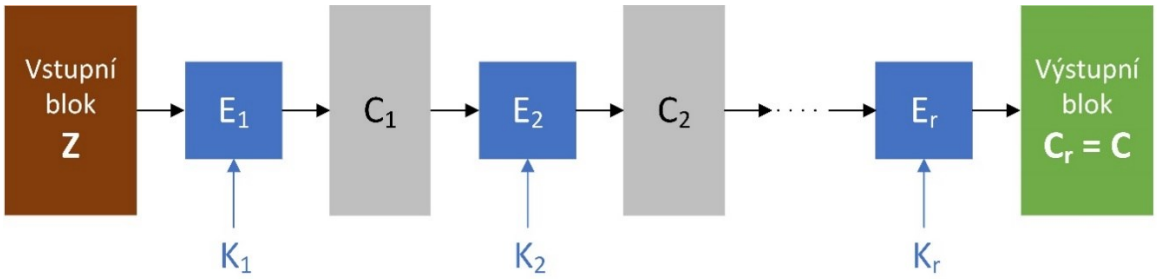
U proudových kryptosystémů se šifrování provádí po jednotlivých bitech, což lze formálně vyjádřit takto: $c_i = E(z_i, K)$, kde c_i je i-tý bit kryptogramu, z_i je i-tý bit zprávy, K je šifrovací klíč a E je šifrovací funkce.

Výhodou proudových šifer oproti blokovým symetrickým šifrám je skutečnost, že proudové šifry jsou implementačně jednodušší a proces šifrování i dešifrování zprávy je u nich rychlejší. Naopak jejich nevýhodou je slabší odolnost proti kryptoanalýze a jiným útokům. Z tohoto důvodu a vzhledem k míře, do jaké je současný výpočetní hardware výkonný, nejsou tím pádem výhody proudových šifer již tak významné, což v praxi vede k odklonu od jejich používání.

Blokové kryptosystémy využívají principu šifrování po blocích o pevné délce n bitů. Vstupní blok $Z = z_1, z_2, z_3, \ldots, z_n$ je n bitové číslo, jemuž šifrovací funkce E přiřadí n bitové číslo $C = c_1, c_2, c_3, \ldots, c_n$ (blok kryptogramu). To lze vyjádřit jako $C = E(Z, K)$, přičemž pro každý i-tý bit bloku kryptogramu platí $c_i = E_i(Z, K)$. Šifrovací funkce E je stanovena tak, že určení hodnoty každého i-tého bitu výstupního bloku kryptogramu C je závislé na všech n bitech vstupního bloku Z a na všech k bitech klíče K. Z toho vyplývá, že každý bit vstupního bloku ovlivňuje hodnotu všech n bitů výstupního bloku šifry. Tento rys blokových šifer se označuje jako **difuze** (*diffusion*). Stejně tak hodnota každého bitu klíče K ovlivňuje hodnotu všech n bitů výstupního bloku C, což je označeno jako **konfuze** (*confusion*). Difuze a konfuze

zvyšují odolnost blokových kryptografických algoritmů proti útokům, neboť pro případného útočníka je náročné odhadnout hodnoty *Z* nebo *K* z hodnoty *C*. (Burda, 2013)

Další typickou vlastností současných blokových kryptografických algoritmů je princip kaskády šifer. Tzv. kaskádová šifra (*product cipher*) je pojem, který se používá pro zřetězení *r* šifer. Výstupní blok každé *i*-té šifry ($1 \leq i \leq r$) je zároveň vstupním blokem šifry následující. Výstupní blok poslední r-té šifry je současně finálním kryptogramem. Tento princip je znázorněn na obrázku 15.



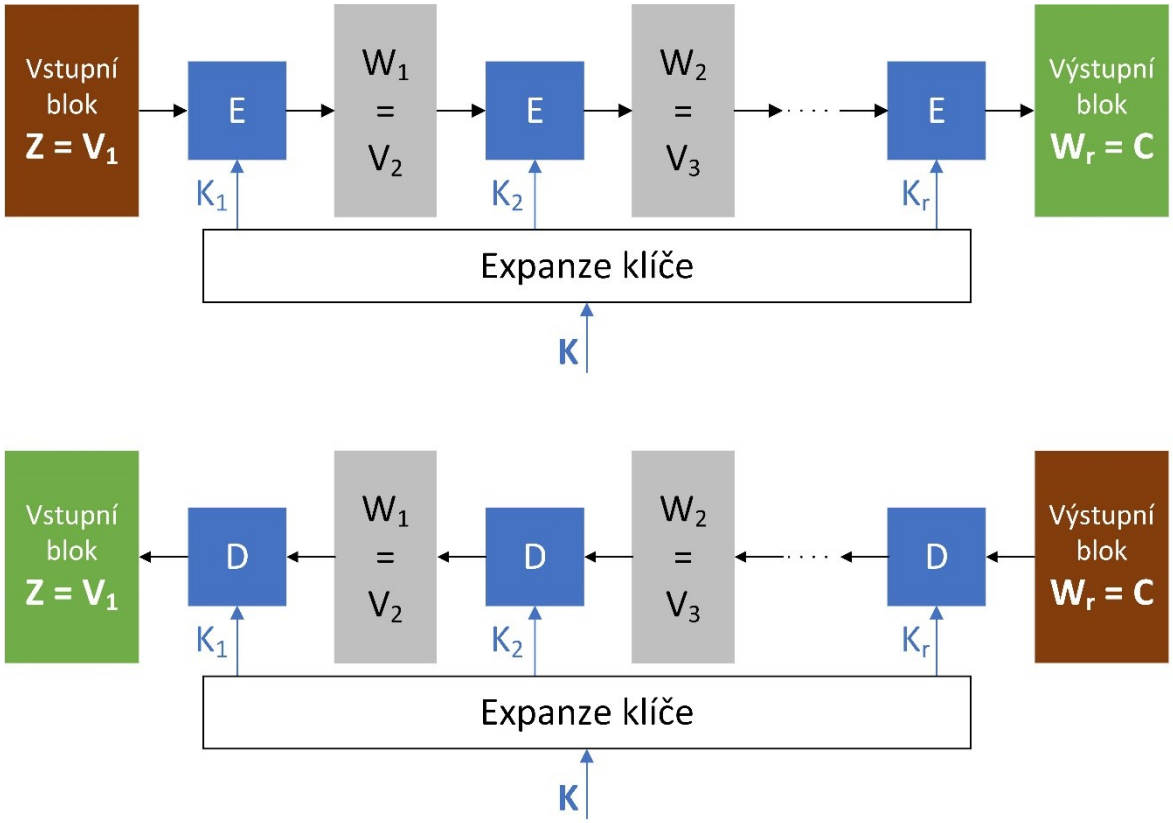
Obrázek 15: Princip kaskádové šifry
Zdroj: vlastní zpracování podle Burdy (2013)

V praktických aplikacích se často využívá speciální typ kaskádové šifry, tzv. iterovaná šifra, která je založena na principu zřetězení *r* stejných šifer.

Obecný algoritmus šifrování při využití iterované šifry je graficky znázorněn na obrázku 16 a je následující:

- blok expanze klíče: z šifrovacího klíče *K* se odvodí *r* dílčích klíčů (tzv. iterační nebo rundové klíče) => vzniknou klíče K_1 až K_r – šifrovací klíče pro opakovaně použitou (iterovanou) transformační funkci *E*, kterou nazýváme jako iteraci (tzv. round);
- vstupní blok šifry *Z* se nejprve přivede na vstup první iterace *E;*
- následně se během jednotlivých iterací provede v závislosti na iteračním klíči K_i transformace vstupního bloku bitů V_i do podoby výstupního bloku W_i – zde se využívají vhodné kombinace blokových operací, mezi které většinou patří substituce, permutace a aritmetické operace;
- po první iteraci je vstupní blok šifry $Z = V_1$ zašifrován do kryptogramu $W_1 = E(V_1 = Z, K_1)$;
- kryptogram v podobě bloku W_1 je zároveň vstupem V_2 pro další iteraci *E*;

- uvedený postup se opakuje do té doby, než proběhne poslední *r*-tá iterace, jejímž výstupem je výsledný kryptogram $W_r = C$.



Obrázek 16: Princip blokové iterované šifry při šifrování a dešifrování
Zdroj: vlastní zpracování podle Burdy (2013)

Mezi často využívané iterované blokové algoritmy patří tzv. Feistelova šifra. Princip šifer Feistelova typu spočívá v opakovaném (iterovaném, kaskádovém) použití jediné šifry. Tohoto principu využívají známé šifrovací algoritmy Blowfish, Camellia, DES (*Data Encryption Standard*), MARS, RC5, TEA, Triple DES, Twofish, XTEA nebo ruská šifra GOST 28147-89.

Obecný princip blokových šifer ale umožňuje i použití různých šifer v jednotlivých iteracích příslušného algoritmu (Schneier, 2015). Do této skupiny kryptografických algoritmů patří velmi významná bloková šifra AES (*Advanced Encryption Standard*). Tomuto algoritmu bude v dalším textu (kapitola 5.4.4) věnován prostor z důvodu jeho zamýšleného využití v popisovaném systému včasného varování.

5.1.3 Asymetrické kryptografické algoritmy

Asymetrické algoritmy patří mezi novější kryptografické metody a první informace o nich byly uvedeny v článku „New Directions in Cryptography“ (Diffie, Hellman) publikovaném v roce 1976. I asymetrické algoritmy lze dále dělit podle účelu použití na utajovací a autentizační. Asymetrické utajovací algoritmy využívají dva typy klíčů. První typ klíče, ke kterému má přístup prakticky každý, se nazývá veřejný šifrovací klíč (*public key*). Druhý klíč, který je označován jako soukromý dešifrovací klíč (*private key*), je znám pouze svému držiteli (příjemci informace), který ho musí udržet v tajnosti. Oba klíče jsou spolu spojené pomocí dvou speciálních matematických funkcí – pečetění a ověřování. Dále je pro kvalitní asymetrické kryptografické algoritmy typické, že musí být zpětně neproveditelný výpočet soukromého klíče z klíče veřejného. V současnosti je jednou z nejvíce populárních metod asymetrické kryptografie algoritmus RSA, který je pojmenovaný podle svých tvůrců Rivesta, Shamira a Adlemana (1978). Jeho bezpečnost je založena na obtížnosti řešení problému faktorizace velkých čísel. Dalším rozšířeným algoritmem spadajícím do této skupiny je Diffie-Hellmanův protokol, jehož bezpečnost spočívá v obtížnosti řešení problému tzv. diskrétního logaritmu. Nevýhodou asymetrických algoritmů je zejména jejich výpočetní náročnost, která je obvykle o několik řádů vyšší než u symetrických metod.

Proto se v praxi využívá kombinace těchto dvou uvedených kryptografických systémů, která se nazývá hybridní šifrování (*hybrid encryption algorithm*). Zde je navíc použit náhodný klíč (někdy nazývaný *session key*), který je vygenerován odesílatelem a zaslán příjemci pomocí asymetrického algoritmu. Asymetrický algoritmus slouží k zabezpečenému přenosu zmíněného náhodného klíče. Ten pak po úspěšném dešifrování použijí obě strany k tomu, aby zabezpečeně komunikovaly s využitím mnohem rychlejšího symetrického šifrování. Výhodou tohoto kombinovaného přístupu je to, že pomocí pomalejšího asymetrického algoritmu šifrujeme pouze klíč, který je zpravidla kratší než přenášená zpráva. Hybridní přístup našel široké uplatnění nejvíce na internetu, kde se tvoří základ pro zabezpečení prohlížečů pomocí protokolu SSL (Secure Socket Layer), případně protokolu TLS (Trasport Layer Security), a v zabezpečení e-mailové komunikace (např. aplikace PGP – Pretty Good Privacy). Právě hybridního principu využívá většina známých publikovaných šifrovacích algoritmů, ve kterých je šifrování založeno na pozici příjemce.

5.1.4 Bezpečnost kryptografických systémů

Jak bylo uvedeno v úvodu podkapitoly 5.1, kryptografie a kryptoanalýza se vyvíjely současně, což vždy vedlo k tomu, že prakticky každý nový kryptografický algoritmus byl kryptoanalytickými metodami dříve či později překonán. To mezi kryptology vedlo k úvaze, že neprolomitelný kryptografický systém nelze vytvořit. Tuto myšlenku vyvrátil Claude E. Shannon (1949) v článku *Communication Theory of Secrecy Systems*. Jak uvádí Burda (2015), Shannon v tomto článku uvedl a následně dokázal na základě pojmů z teorie informace, že utajovací kryptografické systémy lze rozdělit podle **stupně důvěrnosti** na systémy: 1) s maximální důvěrností (*perfect secrecy*), 2) s redukovanou důvěrností (*ideal secrecy*) a 3) s minimální důvěrností (*practical secrecy*).

Nejvyšší (maximální) stupeň důvěrnosti odpovídá situaci, kdy útočník získá dešifrováním všech kryptogramů pomocí všech klíčů všechny možné zprávy. Nejnižší (minimální) stupeň důvěrnosti znamená, že v případě, kdy útočník dešifruje jakýkoli kryptogram pomocí všech klíčů, obdrží pouze jedinou možnou zprávu, což vede k vyluštění kryptogramu.

Přestože byly provedeny důkazy, že lze na teoretické úrovni vytvořit kryptografické systémy s maximální i redukovanou důvěrností, v praxi se používají zejména kryptosystémy zajišťující pouze minimální stupeň důvěrnosti přenášených zpráv. V případě prvních dvou nejvyšších stupňů důvěrnosti definovaných Shannonem (1949) brání praktickým aplikacím vysoké nároky na správu klíčů. V praxi se používají zejména kryptografické systémy s nejnižším stupněm důvěrnosti. Jejich **bezpečné** použití i přes zjevnou slabinu je možné z důvodu, že množina všech možných klíčů je natolik rozsáhlá, že za stanovenou dobu rezistence kryptogramu není možné provést útok hrubou silou (Burda, 2015).

Rozdělení kryptografických systémů podle jejich odolnosti

Podle Burdy (2013) z pohledu možnosti prolomení a odolnosti dělíme kryptografické systémy na neprolomitelné a prolomitelné. Kryptosystémy, které odolají všem útokům i v případě, kdy útočník bude mít neomezenou výpočetní kapacitu, se klasifikují jako **neprolomitelné**. Mezi **teoreticky prolomitelné** nebo tzv. výpočetně bezpečné patří kryptosystémy, u kterých je výpočetní výkon potřebný k úspěšné kryptoanalýze mimo možnosti jakéhokoli útočníka. Všechny ostatní kryptosystémy pak spadají do skupiny tzv. prakticky prolomitelných kryptografických systémů.

Možné způsoby napadení kryptografických systémů

Jak uvádí Wróblewski (2015), mezi nejčastější metody napadení kryptografických systémů patří:

- **Krádež klíče**: může jít o fyzické odcizení klíče, ale častěji jde o situace, kdy si odesílatel informace a její příjemce vyměňují klíč elektronicky. Pokud je útočník schopen odposlouchávat příslušný komunikační kanál, může zachytit klíč během jeho přenosu od odesílatele k příjemci. V případě symetrické kryptografie může nastat situace, kdy útočník získaný klíč modifikuje a následně s odesílatelem i příjemcem informace provádí nezávislou výměnu klíčů a zároveň odposlouchává jejich komunikaci.
- **útok hrubou silou** *(brute force attack)*: útočník se snaží získat odesílanou zprávu v originální podobě tím, že postupně zkouší všechny možné kombinace klíčů. V současnosti se považuje délka klíče *n = 128 bitů* z pohledu útoku hrubou silou při využití výkonné výpočetní techniky za bezpečnou. Šifrovací klíče jsou bezpečné i proto, že mnoho systémů, které v dnešní době využívají nějaký kryptografický algoritmus, pracuje s dynamickými klíči, jež poměrně rychle ztrácejí platnost.

  Jak uvádí Sandeep (2017), v případě útoku hrubou silou by k prolomení algoritmu AES, při uvažované 128 bitové délce klíče, bylo zapotřebí 5×10^{21} let. Hrozbou pro soudobé kryptografické algoritmy by mohly být v budoucnu kvantové počítače. Podle výpočtů získaných na základě tzv. Groverova prohledávacího algoritmu (*Grover's algorithm*) by prolomení 128 bitové varianty AES (AES-128) v případě použití kvantové technologie trvalo pouhých šest měsíců. **Některé srovnávací analýzy ukazují, že doba potřebná k prolomení AES s 256 bitovým šifrovacím klíčem (AES-256) při použití kvantového počítače přibližně odpovídá době potřebné k prolomení AES-128 při využití soudobých výpočetních technologií.** Z toho důvodu je šifra AES-256 považována za bezpečnou i v budoucí sféře kvantových technologií (Sandeep, 2017).
- **dedukce provedená na základě obsahu celé zprávy nebo její části**: útočník se snaží odhadnout, zda přenášené informace neobsahují nějaké známé prvky (např. adresy a názvy v hlavičce). Na základě známé struktury se pak může pokusit rychleji prolomit algoritmus a narušit jeho strukturu.

Dalším bezpečnostním problémem kryptografie je také myšlenka, že „to, co je bezpečné dnes, nemusí být bezpečné zítra“. Při vývoji kryptografických systémů se vždy braly v potaz údaje o slabinách a nevýhodách předchozích algoritmů, které mnohdy vedly k jejich prolomení. Hůře se ale předvídají slabiny budoucí. S rozvojem vědy a nástupem nových technologií se objevují stále sofistikovanější útoky, které dříve nebyly známé nebo se o nich neuvažovalo jako o reálných hrozbách. Mezi takové hrozby patří například útok postranním kanálem (*side-channel attack*), který je kombinací softwarového (statistické výpočty) a hardwarového útoku (měření proudového odběru procesoru při různých kryptografických operacích) a může být reálnou hrozbou pro mnohé kryptografické algoritmy (De Mulder et al., 2018).

5.1.5 Matematické operace využívané v kryptografii

K základním matematickým operacím, které se využívají v kryptografii, patří logické operace na úrovni jednotlivých bitů neboli operace s proměnnými, které mohou mít hodnotu 0 nebo 1. Do této skupiny patří operace uvedené v tabulce 5, z nichž mezi nejpoužívanější patří exkluzivní disjunkce.

Tabulka 5: Základní logické operace používané v kryptografii

Název operace		Symbolicky	X	Y	¬ X	X ∨ Y	X ⊕ Y	X ∧ Y
negace	NOT	¬	0	0	1	0	0	0
disjunkce	OR	∨	0	1	1	1	1	0
exkluzivní disjunkce	XOR	⊕	1	0	0	1	1	0
konjunkce	AND	∧	1	1	0	1	0	1

Zdroj: Vlastní zpracování

Velmi často je v kryptografii nutné tyto operace používat na úrovni bloků různé délky. Například pokud $X = (1, 0, 0, 1)$, $Y = (1, 1, 1, 0)$, pak výsledkem exkluzivní disjunkce bude $X \oplus Y = (0, 1, 1, 1)$.

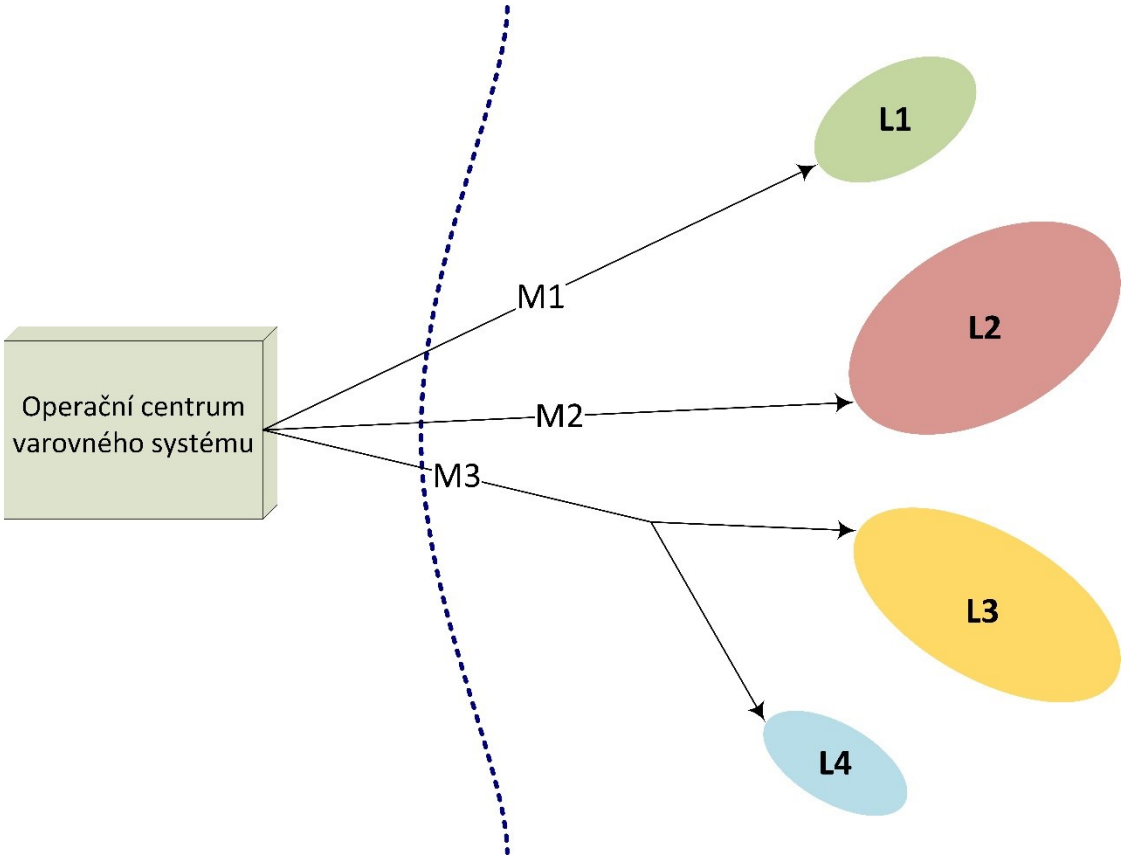
V kryptografii se dále používají následující operace:

- modulo *n* – zbytek po celočíselném dělení čísla *c* číslem *n;*
- zřetězení (*concatenation*, symbolicky ‖);
- kryptografická permutace, která se dále dělí na permutaci prostou, zúženou a rozšířenou;

- rotace vlevo o k bitů, rotace vpravo o k bitů – jedná se o speciální případy prosté permutace a musí platit, že $0 \leq k \leq n$, kde n je počet bitů bloku, ve kterém se rotace provádí;
- posun bloku V o k bitů vpravo (*Shift on Right*) nebo vlevo (*Shift on Left*);
- výběr nejvíce významných bitů (MSB – *Most Significant Bits*) a výběr nejméně významných bitů (LSB – *Least Significant Bits*);
- substituce – operace vycházející většinou z určitého pravidla nebo tzv. substituční tabulky, podle které vstupní hodnotě x přiřadíme jinou hodnotu tak, že $y = S(x)$;

5.2 Princip pozičního šifrování

Obecným principem pozičního šifrování je algoritmus, který zajistí, aby šifrovaná informace mohla být dešifrována pouze na určitém, odesílatelem vymezeném místě. Pokud se někdo pokusí zprávu dešifrovat na jiném místě (potenciální útočník), dešifrovací proces selže a neprezentují se žádné detaily o původní informaci. Tento princip umožňuje, aby data byla pozičně zašifrována, a tím vyhrazena pouze pro určitou vymezenou lokalitu. V kombinaci se systémem Radio-Help lze navíc docílit toho, že je možné šířit různé informace do několika vymezených lokalit ve stejném časovém okamžiku. Pro každou z těchto lokalit je možné zprávu zašifrovat pomocí šifrovacího klíče, který je odvozen pomocí geografických souřadnic této vymezené lokality. Základní koncepce pozičního šifrování je zobrazena na obrázku 17. Elipsy L1 až L4 znázorňují oblasti, do kterých je nutné vyslat šifrovanou varovnou zprávu navíc s požadavkem, že zpráva M1 ≠ M2 ≠ M3 a současně zpráva M3 musí být distribuována do oblasti L3 a L4. Dále musí být zajištěna exkluzivita zpráv v jednotlivých oblastech. To znamená, že zpráva M1 může být úspěšně dešifrována pouze v oblasti L1, zpráva M2 pouze v oblasti L2, zpráva M3 v oblastech L3 a L4 – stejnou zprávu lze ve stejný časový okamžik odeslat i do oblastí, které spolu přímo nesousedí.



Obrázek 17: Základní koncepce pozičního šifrování
Zdroj: vlastní zpracování

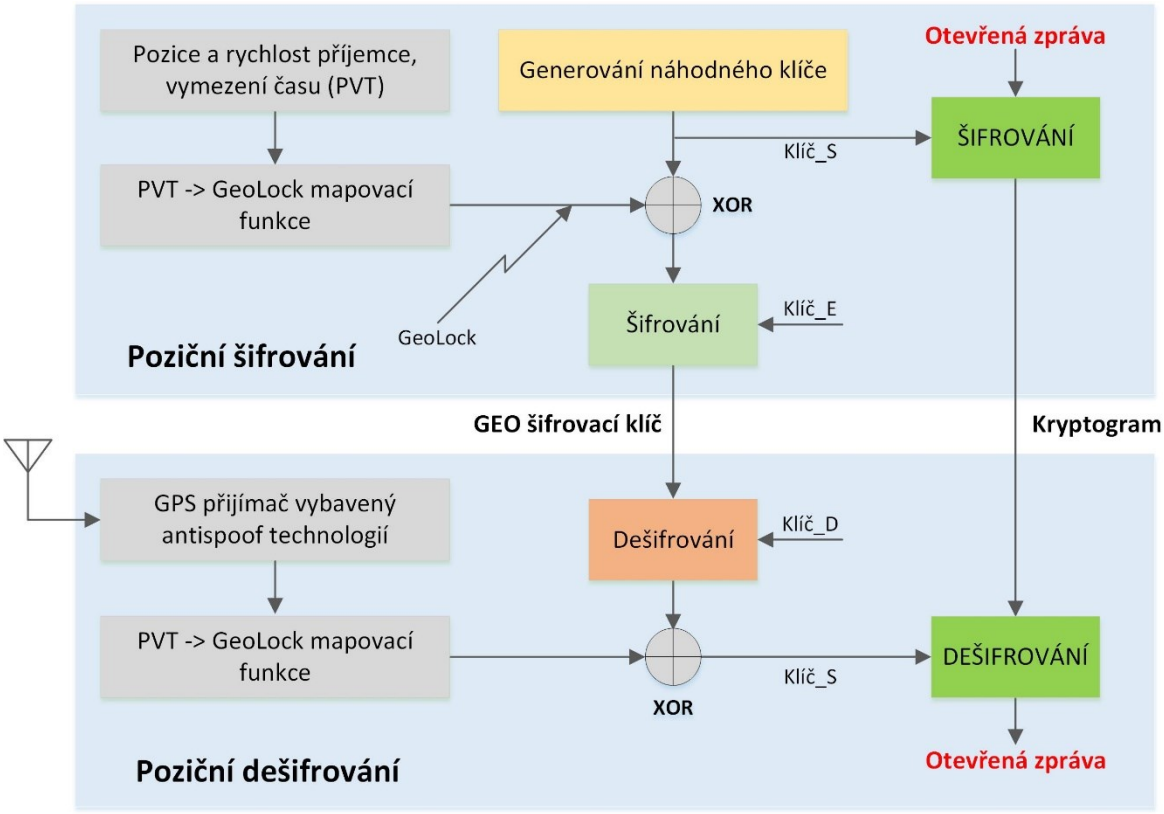
Stávající publikované metody pozičního šifrování berou většinou v úvahu rizika, která mohou zejména ze strany případných útočníků nastat. Jedním z těchto rizik je podvržení geografické polohy přijímače (tzv. *GPS spoofing*), a tím šance varovnou zprávu získat v její originální podobě i v jiné lokalitě, než pro jakou byla určena. Dalším problémem může být snaha o lokální přerušení pozičního signálu pomocí rušiček (tzv. *GPS jamming*). V případě využití pozičního šifrování pro uvedené modelové situace a jim podobné lze předpokládat, že útočníci nebudou např. z časových důvodů podvrhovat na svých mobilních telefonech geografickou pozici za jinou, než ve které se aktuálně nachází. První modelová situace vychází z myšlenky, že útočník (hledaný zločinec) neví o tom, že byl spatřen. V případě teroristických útoků je samozřejmě situace komplikovanější. Pokud by se jednalo o sofistikovaný a dlouho připravovaný útok, lze předpokládat, že útočníci budou znát technologie, kterými disponují záchranné složky včetně policie a armády, a budou na ně připraveni. Nicméně poslední teroristické ofenzívy charakter takto sofistikovaných útoků neměly a z toho důvodu je i v těchto situacích potenciál pro využití pozičního šifrování založeného na symetrických kryptografických metodách. V situaci, kdy by poziční šifrování mohlo pomoci k zajištění řízené evakuace při přírodních katastrofách a živelných

pohromách ohrožujících rozsáhlejší oblasti, lze téměř s jistotou říci, že lidé nebudou mít důvod zkoušet ve svých zařízeních podvrhnout geografickou pozici.

5.3 Aplikace pozičního šifrování

V současné době se pro kryptografické přístupy, které jsou založené na výše uvedeném principu pozičního šifrování informací, používají pojmy *Geo-Encryption*, *Location Based Encryption*, případně *Location Dependent Data Encryption*. Obecně lze konstatovat, že poziční šifrování si neklade za cíl nahradit konvenční kryptografické systémy, ale nabízí zajímavou možnost přidat další vrstvu zabezpečení pro přenášené informace.

Algoritmus pozičního šifrování publikovaný v roce 2003 pod názvem Geo-Encryption (Scott & Denning) vychází z hybridního principu kryptografie. Blokové schéma tohoto algoritmu znázorňuje obrázek 18. Tento algoritmus byl konkrétně testován pro využití šifrované digitální distribuce filmů za účelem snížení porušování autorských práv.



Obrázek 18: Blokové schéma algoritmu pozičního šifrování
Zdroj: zpracováno podle Scotta (2003b)

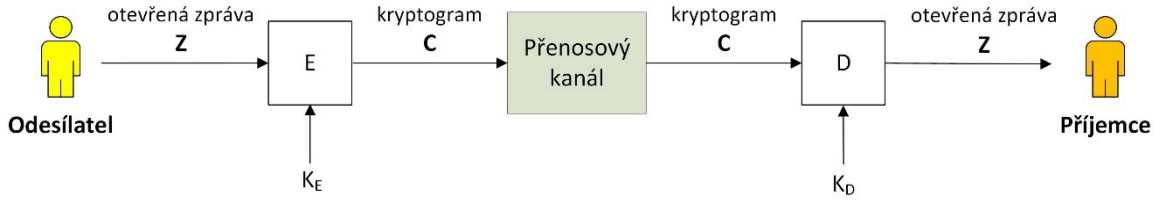
Uvedený algoritmus využívá hybridní princip šifrování a je vhodný pro situace, kdy příjemce není anonymní (tj. je dopředu znám). Hlavním důvodem je to, že odesílatel informace musí disponovat klíčem veřejným a příjemce (resp. jeho zařízení – mobilní telefon) klíčem soukromým. To jsou rysy charakteristické pro asymetrickou kryptografii, která se u hybridního principu používá pro přenos náhodného klíče (Klíč S). Samotná zpráva je pak šifrována pomocí symetrického kryptografického algoritmu.

V článku publikovaném autory Al-Fuqaha et al. (2007) byl původní Scottův algoritmus Geo-Encryption rozšířen. Je zde zohledněna situace, kdy se předpokládá pohyb příjemců zprávy vzhledem k vymezené oblasti. Tento rozšířený algoritmus předpokládá výměnu koordinačních zpráv mezi odesílatelem a příjemcem – i zde se využívá princip hybridního šifrování. Vzhledem k tomu, že systém Radio-Help je koncipován jako jednosměrný, to znamená, že varovná komunikace probíhá ve směru od odesílatele k příjemci, je tato rozšířená verze algoritmu Geo-Encryption nevyužitelná. Nicméně některé principy vymezení cílové oblasti uvedené ve výše zmíněném článku jsou inspirativní a jeví se jako využitelné i v případě symetrického šifrování, které je základem pro návrh systému pozičně šifrovaného vysílání varovných zpráv. Vyřešení této situace je součástí následujícího výzkumu, ve kterém se řeší také matematická interpretace algoritmu s ohledem na konkrétní případy jeho využitelnosti.

Pro účely systému včasného varování a pro rychlou distribuci „pozičně cílených“ varovných zpráv, u kterých je navíc žádoucí přidat faktor důvěrnosti vztažený k určité lokalitě, je ovšem hybridní kryptografický princip nevhodný. Zamýšlená komunikace je ryze jednosměrná a navíc příjemce není dopředu znám. Z toho důvodu nelze použít asymetrický kryptografický princip, při kterém se pro zabezpečenou distribuci informací musí využít veřejný i soukromý klíč.

Z výše uvedených důvodů připadají pro rozšíření systému Radio-Help o možnost pozičního šifrování v úvahu zejména **symetrické utajovací kryptografické systémy**. Často uváděná nevýhoda symetrických algoritmů, a to problémy spojené s bezpečným doručením klíče odesílateli i příjemci, je zde do jisté míry eliminována, neboť k předávání klíče nedochází. V případě, že má anonymní příjemce právo zprávu přijmout, což znamená, že se nachází v oblasti vymezené pro příjem dešifrované informace, má správný dešifrovací klíč (geografické souřadnice) v ten okamžik dostupný ve svém zařízení.

Blokové schéma utajovacího kryptosystému je znázorněno na obrázku 19. Na straně odesílatele zprávy je dána šifrovací funkce E, která je určena šifrovacím klíčem K_E. Tato funkce zajistí transformaci otevřené zprávy Z do podoby kryptogramu C. Formálně lze šifrování vyjádřit tímto způsobem: $C = E(Z, K_E)$. Šifrovací funkce musí být vytvořena tak, aby útočník nebyl schopen z daného kryptogramu bez znalosti šifrovacího klíče odvodit zprávu dříve, než je stanovená doba rezistence kryptogramu. Doba rezistence kryptogramu závisí na potřebách konkrétní implementace. V případě zpráv varujících před akutním nebezpečím postačí doba rezistence kryptogramu řádově v minutách. Šifrovací klíč K_E je v případě pozičního šifrování vhodným způsobem odvozen od geografických souřadnic lokality, v níž mají potenciální příjemci obdržet originální korektně dešifrovanou zprávu.

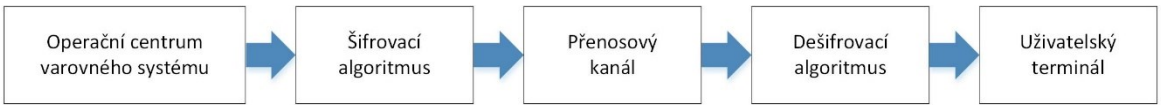


Obrázek 19: Blokové schéma obecného utajovacího kryptografického systému
Zdroj: zpracováno podle Burdy (2015)

Na straně příjemce zprávy je nutné provést dešifrování zprávy. Dešifrovací funkce D je inverzní k šifrovací funkci E. Dešifrování lze formálně vyjádřit takto: $D(C, K_D) = Z$. Ke zjištění původní otevřené zprávy je tedy zapotřebí znalost dešifrovacího klíče K_D. Mezi šifrovacím klíčem K_E a dešifrovacím klíčem K_D existuje závislost, kterou lze vyjádřit funkcí $K_D = f(K_E)$. Pokud je prakticky možné v průběhu doby rezistence kryptogramu zjistit hodnotu K_D z hodnoty K_E, pak oba klíče musí být tajné. Kryptografické systémy, u kterých platí, že klíče K_E a K_D mají z hlediska utajení stejné neboli symetrické postavení, označujeme jako symetrické utajovací kryptosystémy (utajovací systémy s tajným klíčem).

5.4 Aspekty systému pro pozičně šifrované vysílání informací

Systém pro poziční šifrované vysílání je zamýšlen jako rozšíření koncepce systému Radio-Help, který je blíže popsán v kapitole 3.3, a jeho cílem je zajistit, aby varovná informace byla distribuována do určité oblasti s atributem exkluzivity. Celý systém, který má ambice univerzálního využití, se skládá ze základních částí, které jsou schematicky znázorněny na obrázku 20.



Obrázek 20: Základní části systému pro pozičně šifrované vysílání informací
Zdroj: vlastní zpracování

5.4.1 Operační centrum varovného systému

Operační centrum varovného systému je středisko, které by mělo sloužit GŘ HZS nebo podobné instituci ke sběru vstupních informací a dat, k tvorbě scénářů pro distribuci varovných informací, k vymezení oblastí pro nucený příjem adresného vysílání a k dalším koordinačním činnostem. Personál (tj. operační manažeři, odborníci na různé typy mimořádných situací) zajišťující chod tohoto centra musí být schopen flexibilně a včasně reagovat na vzniklé mimořádné události, rozhodovat o podobě varovných zpráv a také o tom, zda se využije možnosti zprávu zašifrovat. V případě událostí ohrožujících větší územní celky je nutné, aby důležitá rozhodnutí učinily kompetentní osoby (hejtman, předseda vlády apod.).

5.4.2 Uživatelský terminál

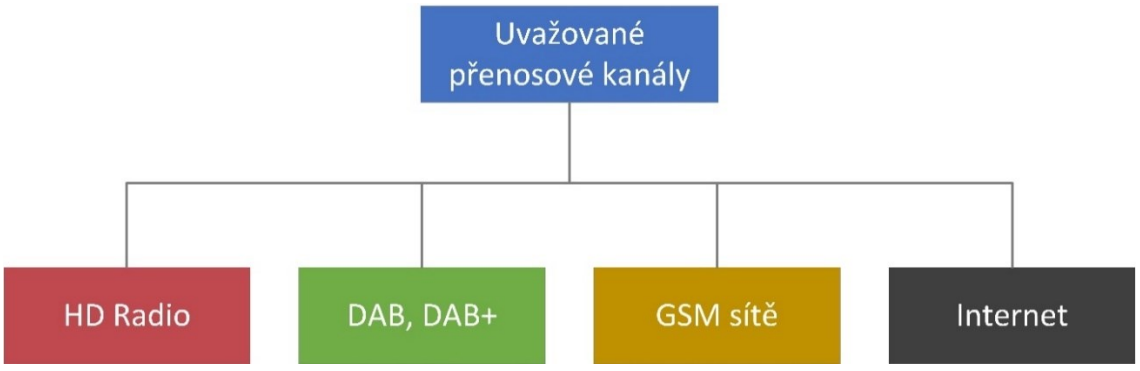
Uživatelským terminálem může být jakékoli zařízení (v současné době nejčastěji mobilní telefon), které je schopno zaměřit svou polohu pomocí běžně dostupných metod. Nejběžnější z těchto metod je systém GPS, pomocí kterého lze poměrně přesně zaměřit konkrétní zařízení nezávisle na mobilních sítích. Nevýhodou je skutečnost, že signál z družící systému GPS je hůře zachytitelný uvnitř budov, v podzemních prostorách apod., což lze částečně eliminovat posledním pozičním údajem. Samozřejmě je také nutné počítat s tím, že některé telefony stále i v dnešní době nemusí být vybaveny funkcí GPS nebo může mít uživatel zařízení funkci GPS vypnutou například z důvodu šetření výdrže baterie.

Další možností zaměření je zjištění polohy pomocí mobilní sítě. Výhodou této metody je relativně silný GSM signál, který se dostane i do míst, kde nelze možné zaměřit polohu pomocí GPS – tedy dovnitř budov. Nevýhodou je zde ale nepřesnost (v porovnání s GPS), a to zejména v řidčeji obydlených oblastech, ve kterých je telefon v dosahu pouze jedné stanice BTS. Přesnost této metody roste s větším počtem BTS stanic, jež jsou současně v dosahu mobilního zařízení. Je nutné si ovšem uvědomit, že policie má zákonnou možnost v určitých případech ohrožujících bezpečnost státu rušit telefonní, datový

a radiokomunikační provoz, který zajišťují zejména mobilní operátoři. V těchto případech tedy nelze počítat s tím, že v případě vypnuté funkce GPS v zařízení a vypnuté mobilní sítě bude poziční varovná zpráva úspěšně doručena příjemci. S touto možností je nutné počítat i v případě první modelové situace. Nicméně, i při těchto omezeních by se varovná zpráva dostala k velké skupině obyvatel, neboť lze předpokládat, že systém GPS bude aktivní u větší části zařízení v oblasti, pro kterou bude varovná zpráva určena, a že nebudou vypnuty všechny dostupné komunikační kanály (některý z nich bude ponechán právě pro případ využití varovného systému).

5.4.3 Přenosový kanál

Celá koncepce systému Radio-Help je založena na nuceném příjmu varovných informací v určité předem vymezené oblasti. V případě vzniklé mimořádné události by operační centrum zajistilo přenos varovné informace do vymezené oblasti. Výhodou této koncepce je možnost ve stejném okamžiku odeslat několik různých zpráv do různých geografických lokalit. Pokud se poloha uživatele terminálu, který bude splňovat požadavky pro příjem nucených varovných zpráv, bude shodovat s vymezenou oblastí, pak zařízení uživatele přijme textovou zprávu, která může být navíc doprovázena hlasovou relací, nebo pouze hlasovou varovnou zprávu.



Obrázek 21: Uvažované přenosové kanály
Zdroj: Vlastní zpracování

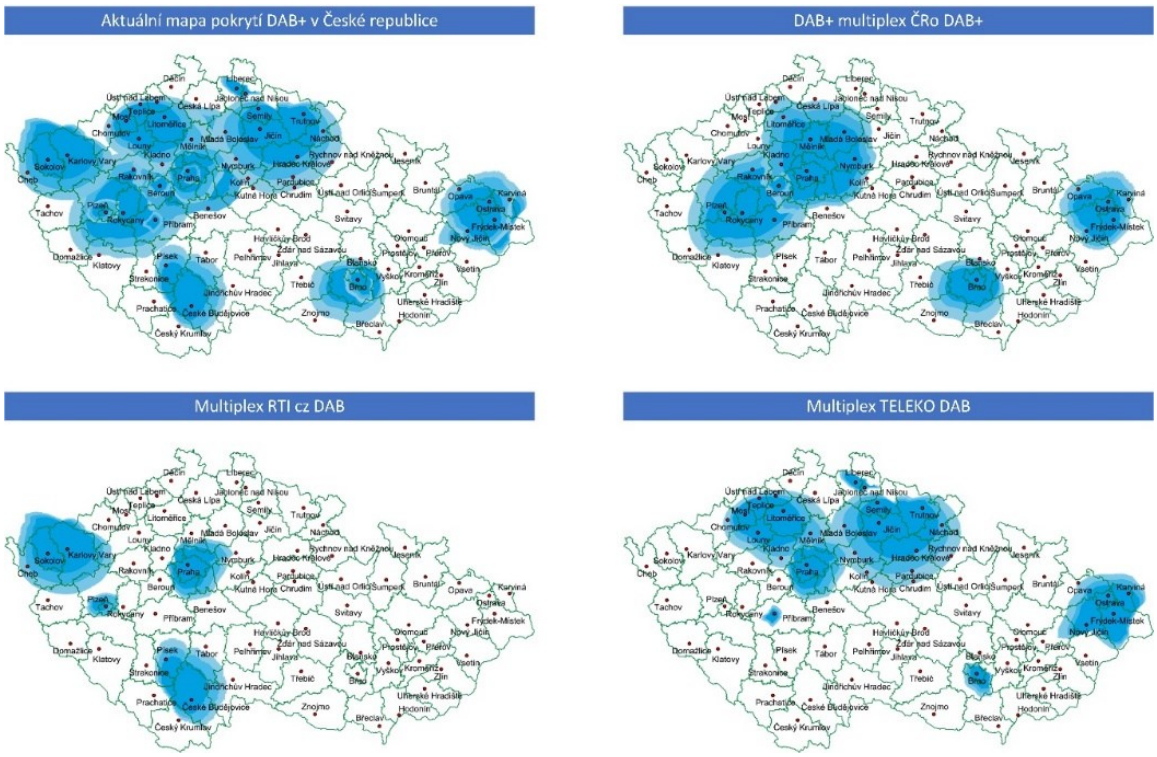
V případě původní koncepce systému Radio-Help, tedy využití rádiové technologie pro přenos varovných informací, lze do výčtu možných a zároveň vhodných přenosových kanálů zahrnout technologie pro digitální rozhlasové vysílání. Podle dokumentu s názvem „Koncepce rozvoje digitálního rozhlasového vysílání“ dodržel Český rozhlas plán a v roce 2017 spustil, paralelně s klasickým analogovým vysíláním, řádné digitální vysílání celoplošných stanic a speciálních digitálních programů a kanálů (Pracovní komise

Strategické rady Českého rozhlasu pro digitální rozhlasové vysílání, 2014). V uvedeném dokumentu byla také deklarována představa, že nejpozději od roku 2025 je plánováno ukončení analogového vysílání a přechod na plné digitální vysílání programů Českého rozhlasu. Jak je v dokumentu uvedeno, tento harmonogram může být případně aktualizován dle vývoje legislativního rámce a postupu jednání a spolupráce s dalšími provozovateli vysílání, státními a regulačními orgány a dalšími subjekty. Případné využití uvedených technologií pro potřeby zde popisovaného varovného systému se samozřejmě neobejde bez jednání se zástupci mobilních operátorů a Českého rozhlasu.

Z pohledu digitalizace rozhlasové sítě existují dvě základní koncepce, a to HD Radio a DAB, resp. DAB+. Technologie HD Radio se používá zejména v USA a některých zemích Střední Ameriky. Z pohledu využití pro distribuci varovných informací je hlavní výhodou této technologie možnost využít stávající (tj. dlouhovlnné, středovlnné a VKV) vysílače analogového signálu, do jehož modulace může být superponován digitální signál formátu HD Radio (Skrbek, 2013). K pokrytí ČR analogovým signálem s digitální složkou by pak postačoval v případě dlouhých vln **jeden vysílač** nebo dva vysílače, pokud by se uvažovalo o vysílání v pásmu středních vln. Uvedená skutečnost je hlavní výhodou této koncepce, protože v případě válečného ohrožení nebo hrozby teroristického útoku by bylo možné území (pozemní i vzdušné) kolem příslušného vysílače efektivně bránit. Podobně lze uvažovat o mimořádné situaci rozsáhlého blackoutu, který může nastat i v důsledku teroristického útoku. Pro jeden dlouhovlnný vysílač lze zajistit potřebné energetické požadavky na jeho provoz ze záložních energetických zdrojů i po delší dobu. Bohužel rozšíření technologie HD Radio v České republice je v dohledné době nepravděpodobné.

V České republice, podobně jako ve většině států EU, byl pro digitalizaci plošného rozhlasového vysílání zvolen systém DAB (*Digital Audio Broadcasting*), který je koncipován jako plně digitální rozhlasová technologie. V současné době se používá formát DAB+, který oproti původnímu DAB zvyšuje efektivitu díky použití kodeku AAC+. V ČR zajišťují provoz digitálního rozhlasového vysílání společnosti RTI cz s.r.o, TELEKO s.r.o. a České Radiokomunikace a.s. Poslední jmenovaná společnost zajišťuje provoz DAB+ digitálního multiplexu pro Český rozhlas. Ostrý provoz veřejnoprávního multiplexu DAB+ ČRo byl zahájen 1. června 2017. Podle údajů Českého rozhlasu (Bumbálková, listopad 2017) pokryje digitální multiplex ČRo DAB+ signálem 40 % obyvatel. Celkově je podle údajů společnosti RTI cz s.r.o. (RTI cz, 2018) pokryto příjmem signálu DAB+ v České republice

plocha odpovídající 6,6 milionu obyvatel, v září 2016 to bylo 5,7 milionu. Úroveň pokrytí signálem DAB+ pro ČR demonstruje obrázek 22. Z celoevropského pohledu je zajímavá informace, že první zemí, která přešla na pozemní digitální rozhlasové vysílání a současně dne 13. 12. 2017 eliminovala na minimum provoz analogového rozhlasového vysílání na velmi krátkých vlnách, je Norsko (Armstrong, 2017).



Obrázek 22: Mapa pokrytí ČR systémem DAB+ (leden 2018)
Zdroj: http://www.digitalradiodab.cz/mapy-pokryti.html

Prozatím se pro platformu DAB+ v ČR využívají dvě frekvenční pásma. Pro pásmo **III–Band** jsou vyhrazeny frekvence 174–230 MHz. Vysílačů zajišťujících provoz v tomto pásmu je šestnáct. Počet vysílačů v pásmu **L-Band** je devět. Pro toto pásmo je vymezen frekvenční rozsah 1452–1492 MHz. Dosah vysílačů DAB+ se v závislosti na výkonu, umístění vysílače a reliéfních podmínkách pohybuje řádově v desítkách kilometrů (Český telekomunikační úřad, 2018).

Vzhledem ke snaze provozovatelů o co nejširší pokrytí ČR signálem DAB+ a rostoucí nabídce přijímačů DAB+ se jeví tento přenosový kanál pro účely systému popisovaného v této práci jako reálně využitelný. Nicméně univerzálnímu nasazení brání jednak oblasti ČR, které zůstávají zatím zcela bez pokrytí, a také zdrženlivost výrobců mobilních telefonů

implementovat DAB+ čipy do svých zařízení (Polák, 2018). V následující tabulce 6 je uvedeno shrnutí předností a nedostatků platformy DAB+ z pohledu systému pro poziční šifrované vysílání varovných informací.

Tabulka 6: Přednosti a nedostatky komunikačního kanálu DAB+

Přednosti technologie DAB+	Nedostatky technologie DAB+
• Dynamicky rozvíjející se infrastruktura, u které lze předpokládat celoplošné rozšíření v rámci ČR *(konkrétní termín pokrytí celé ČR ale není znám)* • Nezávislost na mobilních sítích a Internetu • Stoupající počet přenosných i stolních audio zařízení podporujících příjem signálu DAB+ (včetně autorádií nebo adaptérů pro rozšíření funkčnosti stávajících zařízení)	• Zdrženlivost výrobců mobilních telefonů k implementaci DAB+ tunerů do svých výrobků • Oproti technologii HD Radio v pásmu středních vln několikanásobně menší dosah vysílačů • V současné době zatím zůstávají zcela bez pokrytí některé oblasti ČR – Kraj Vysočina, Zlínský kraj, Olomoucký kraj, část Pardubického kraje a část Moravskoslezského kraje • Systém DAB+ není celosvětově rozšířená technologie

Zdroj: Vlastní zpracování

GSM sítě a Internet jsou prozatím pouze okrajové platformy pro zamýšlené využití v rámci varovného systému zejména z důvodů zmíněných v kapitole 3.1, neboť právě v případě mimořádných událostí mohou tyto kanály selhat nebo být vypnuty. Proto je vhodné navrhnout systém včasného varování tak, aby na nich byl nezávislý, což se ale nevylučuje s možností je v rámci systému využít jako paralelní distribuční kanál. Nicméně i v GSM síti lze principy pozičního šifrování aplikovat (Vijay a Godase, 2014).

5.4.4 Šifrovací algoritmus

Princip pozičního šifrování navržený Scottem et al. v roce 2003, který využívá principu hybridního šifrování (viz kap. 5.3), je efektivní v případě, že odesílatel zprávy zná příjemce, jeho umístění a také čas, ve kterém příjemce bude v cílové lokalitě. Tento princip nelze využít pro účely pozičně šifrovaného varování, protože v těchto případech je nutné zprávu rozšířit do vymezené lokality mezi co nejvíce anonymních příjemců, kteří se v ní nacházejí. Navíc se v těchto případech jedná o jednosměrnou komunikaci. V první modelové situaci je navíc nutné počítat s tím, že oblast pro příjem dešifrované zprávy bude vymezena jako poměrně široká a navíc se zde předpokládá mobilita potenciálních příjemců varovné zprávy

(resp. jejich zařízení) zahrnující i obyvatele, kteří se v době vysílání ještě nevyskytovali v dané oblasti. Mezi vhodné kryptografické metody patří z výše zmíněných důvodů symetrické utajovací kryptografické algoritmy. Jedním z dominantních algoritmů patřících do této kategorie je AES (*Advanced Encryption Standard*).

Jedna z prvních ucelených prací s popisem algoritmu AES vyšla v roce 1999 pod názvem „*AES Proposal: Rijndael*“ (Daemen a Rijmen, 1999). Tento algoritmus byl zvolen v USA jako vítěz veřejné soutěže Národního institutu standardů a technologií (*NIST – National Institute of Standards and Technology*) o nalezení nového bezpečného federálního šifrovacího standardu. Detailní popis algoritmu je zpracován v dokumentu *„Announcing the ADVANCED ENCRYPTION STANDARD (AES)“*, který byl vydán v roce 2001 úřadem NIST po přijetí šifry státní správou USA. Předpoklad, že AES bude platným šifrovacím standardem na delší dobu, se ve své podstatě vyplnil, neboť je tato bloková šifra v současné době skutečně široce využívána. Mezi výhody patřila již v době vzniku tohoto algoritmu nízká hardwarová a paměťová náročnost, malá velikost zdrojového kódu, možnost zpracování na různých typech procesorů a možnost paralelního zpracování. V roce 1997, kdy rychlost procesorů byla 200 – 300 MHz, bylo dosaženo rychlosti 30 – 70 Mb/s v závislosti na použitém programovacím jazyku a délkách klíče.

Výhodou algoritmu AES je i fakt, že ho lze navrhnout na softwarové i hardwarové úrovni (Mali, 2005; Singh, 2016). Hardwarová implementace je vhodnější pro aplikace s vysokými nároky na rychlé šifrování v reálném čase. Do zařízení určených pro příjem varovných zpráv by tak mohl být implementován čip, který by šifrování zajišťoval. Pokud by se jednalo o čip, který by kompletně zajišťoval všechny funkce spojené s šifrování, mělo by toto řešení výhodu ve snížení výpočetní zátěže procesoru. Novější mobilní procesory obsahují instrukce pro hardwarovou akceleraci AES, která by v telefonech s operačním systémem Android měla být nativně zapnutá pro šifrování souborů. Při uvedení nové verze operačního systému Android 7.0 Nougat v roce 2016 byl společností Google stanoven požadavek nativní HW podpory šifrování souborů AES. Pokud některé zařízení tento požadavek nesplňovalo (např. telefony se staršími procesory Snapdragon 800/801), nemohla na něj být oficiální cestou nainstalována nová uvedená verze operačního systému (Sims, 2016).

Následující tabulka 7 poukazuje především na přednosti algoritmu AES, které odůvodňují, proč byl algoritmus AES zvažován jako preferovaný kandidát pro účely systému včasného

varování s funkcí pozičního šifrování. Mezi další uvažované šifrovací algoritmy patřila šifra DES, 3DES (Triple DES) a proudové šifry. Proudové šifry jsou sice rychlejší, ale možnost prolomení je vyšší než u blokových kryptografických algoritmů. Při dnešním výkonu desktopových i mobilních platforem ztrácí výhoda rychlosti význam, neboť je důležitější, aby šifra byla bezpečná. Bloková šifra DES byla zavržena z důvodu slabé bezpečnosti, protože je u ní použit pouze 64bitový klíč. Další uvažovaný blokový algoritmus Triple DES z DES vychází. Jedná se v podstatě o trojnásobnou aplikaci algoritmu DES. Jeho bezpečnost proti prolomení je vysoká, ale oproti AES má podstatnou nevýhodu v rychlosti. Jeho implementace zejména na softwarové úrovni jsou v porovnání s AES výkonově pomalejší (Khiyal et al., 2011).

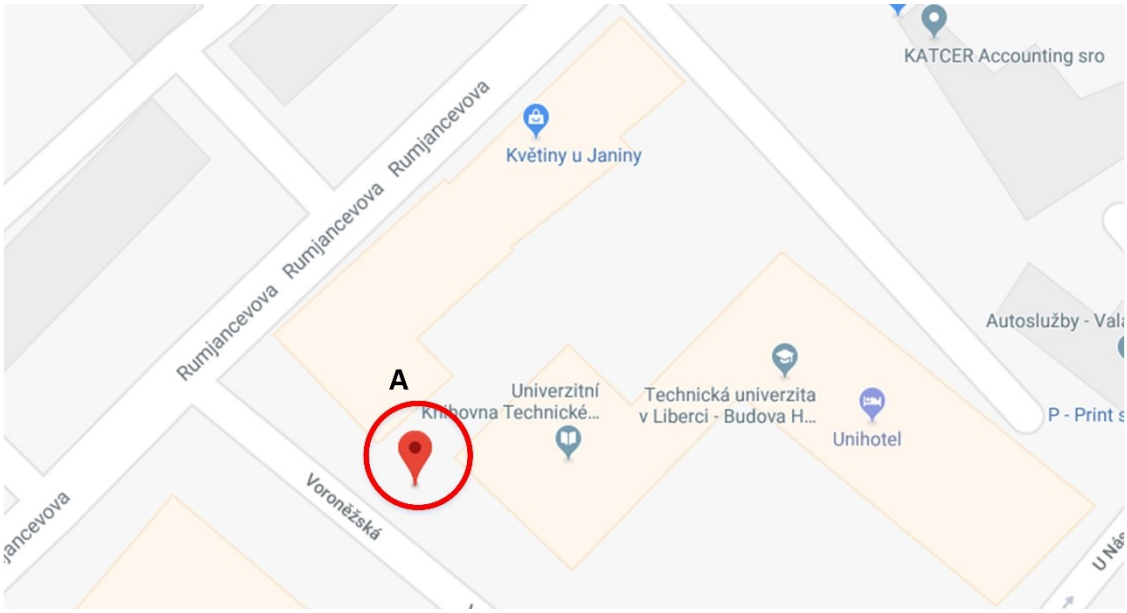
Tabulka 7: Přednosti a nedostatky kryptografického algoritmu AES

Přednosti AES	Nedostatky AES
• poměrně snadná implementace a zároveň poskytuje robustní bezpečnost, díky čemuž je široce rozšířen • rozsáhlá dokumentace • možnost softwarové i čistě hardwarové implementace • vysoká míra „neprolomitelnosti“ i při možném nasazení výkonnějších počítačových systémů (např. kvantových počítačů) z důvodu možnosti využití 256bitového klíče	• v případě použití 128bitového klíče – možnost prolomení algoritmu metodou *brute force attack* při použití výkonnějších počítačových systémů (např. kvantových počítačů) • časté pokusy (dosud neúspěšné) o prolomení šifry AES související s tím, že se jedná v praktických aplikacích o jeden z nejpoužívanějších algoritmů

Zdroj: Vlastní zpracování

6 Využití algoritmu AES pro šifrování varovné zprávy

Stěžejním aspektem systému pozičního šifrování informací vhodného pro distribuci varovných zpráv je algoritmus pro vytvoření šifrovací funkce *E* na základě šifrovacího klíče *K*, který bude odvozen od zeměpisných souřadnic (koordinát – zeměpisná šířka a délka) bodu, jenž bude vymezovat místo, kam má být směřováno šifrované vysílání. Vezměme tedy např. souřadnice 50°46'19.4"N, 15°03'37.8"E, jejichž průnik vymezuje konkrétní zeměpisný bod A (viz obrázek 23).



Obrázek 23: Vymezení konkrétního zeměpisného bodu
Zdroj: Vlastní zpracování s využitím mapových podkladů společnosti Google

6.1 Souřadnicový systém WGS84

Předtím, než bude vysvětlen princip pozičního šifrování algoritmem AES, je nutné zmínit některé teoretické aspekty práce se souřadnicovým systémem, který bude dále používán. Pro další účely byl zvolen systém **WGS84** (*World Geodetic System 1984*), který patří mezi světově nejrozšířenější geodetické systémy.

Pro určení polohy zařízení, obecně pro určení přesného místa na povrchu Země, je nutné určit průsečík koordinát (zeměpisných souřadnic), a to **zeměpisné šířky** (φ) – úhlové vzdálenosti od rovníku a **zeměpisné délky** (λ) – úhlové vzdálenosti od nultého poledníku.

Systém WGS84 využívá zobrazení ve stupních, minutách a vteřinách. Aby nebylo nutné v rámci souřadnicového systému pracovat se zápornými hodnotami, používá se v rámci WGS84 označení pomocí písmen **N** (severní šířka) pro severní polokouli, **S** (jižní šířka) pro jižní polokouli, **E** (východní délka) pro východní polokouli a **W** (západní délka) pro západní polokouli (XU, 2016).

Ve většině přístrojů, jejichž součástí je GPS přijímač, je možné pracovat s následujícími třemi způsoby zobrazení souřadnicového systému WGS84 (Hojgr, 2007):

- formát **hddd.dddd°** – zobrazení stupňů a jeho desetin, setin, tisícin atd. (např. 50.772°N, 15.061°E);
- formát **hddd°mm.mmm'** – zobrazení stupňů a minut v desetinném tvaru (např. 50°46.323'N, 15°03.630'E);
- formát **hddd°mm'ss.s"** – zobrazení stupňů, minut, vteřin a desetin vteřin (např. 50°46'19.4"N, 15°03'37.8"E).

6.2 Příklad šifrování varovné zprávy algoritmem AES

Již bylo uvedeno v předchozím textu, že navrhovaný systém pozičního šifrování bude založen na některém ze symetrických utajovacích kryptografických systémů. Mezi vhodné kandidáty na šifrovací algoritmus lze zcela určitě zařadit blokovou šifru AES (Advanced Encryption Standard). Šifra AES, která byla původně určena pro státní správu USA (po prolomení šifry DES), je v dnešní době jednou z nejčastěji používaných symetrických šifer. Délka bloku šifry je $n = 128$ bitů a délka klíče k je volitelná z těchto hodnot: 128, 192 a 256 bitů. Uvažujme přesnost vymezení polohy v řádu desetin vteřin, což je přesnost dostatečná pro účely varovného systému z toho důvodu, že nejmenší oblasti pro příjem zpráv s nuceným šifrováním by neměly být menší než desítky m^2. S touto uvažovanou přesností bychom mohli při formátu souřadnic *stupně minuty vteřiny* použít délku klíče $k = 128$ bitů (16 bytů), neboť pro každou část souřadnice v této přesnosti musíme vyhradit 8 bytů – šifra AES vyhrazuje pro znak šifrovacího klíče 1 byte (8 bitů). V případě těchto konkrétních souřadnic 50°46'19.4"N, 15°03'37.8"E by se šifrovací klíč skládal z těchto 16 znaků 5046194N1503378E. Pokud by došlo k zpřesnění zadávání souřadnic řádově na setiny vteřin a výše, bylo by nutné pro klíč použít velikost $k = 192$ bitů, případně $k = 256$ bitů.

Před začátkem šifrování se provede převod znaků klíče a znaků varovné zprávy do formátu, který je vhodný pro algoritmus AES. Algoritmus AES patří mezi moderní kryptografické systémy a je transparentní. To znamená, že řetězec 128 bitů na vstupu šifrátoru je stejný jako odpovídající řetězec bitů na výstupu dešifrátoru a je pouze na dohodě mezi odesílatelem a příjemcem, jaký význam těmto bitům přisoudí. Mohou to být znaky podle ASCII tabulky, znaky podle UTF-8, pixely obrázku BMP, zvuky podle formátu MP3 atd. Často se používá hexadecimální formát kódování znaků, kdy se znaky zakódují do hexadecimální podoby pomocí ASCII tabulky (např. znak A se tedy zakóduje jako 41_H). Ukázku takového převodu demonstruje tabulka 2 v následující podkapitole. Šifrovacím klíčem jsou výše uvedené souřadnice a text varovné zprávy může znít např. takto: *Pozor na náměstí bude probíhat policejní akce proti ozbrojenému zločinci!*

6.2.1 Přípravná fáze

Text zprávy je rozdělen do bloků po 128 bitech, což znamená, že je pro jeden ASCII znak vyhrazen 1 byte. Varovná zpráva ***„Pozor na náměstí bude probíhat policejní zásah proti ozbrojenému zločinci!“*** se rozdělí do 5 bloků (viz tabulka 8).

Tabulka 8: Rozdělení zprávy do bloků

Blok 1	**P**	**o**	**z**	**o**	**r**		**n**	**a**		**n**	**a**	**m**	**e**	**s**	**t**	**i**
Blok 2		b	u	d	e		p	r	o	b	i	h	a	t		p
Blok 3	o	l	i	c	e	j	n	i		z	a	s	a	h		p
Blok 4	r	o	t	i		o	z	b	r	o	j	e	n	e	m	u
Blok 5		z	l	o	c	i	n	c	i	!						

Zdroj: Vlastní zpracování

Jak již bylo řečeno, základní délka šifrovacího klíče je 128 bitů. V případě použití 16 ASCII znaků je pro každý znak vyhrazen 1 byte (8 bitů). Jednotlivé znaky klíče (zeměpisné souřadnice) se převedou pomocí ASCII tabulky na jejich hexadecimální reprezentaci (viz tabulka 9). Podobně jako u klíče, převedeme i jednotlivé ASCII znaky zprávy na jejich hexadecimální reprezentaci (viz tabulka 9). Příklad podrobně analyzuje šifrování prvního bloku zprávy.

Tabulka 9: Převod šifrovacího klíče a textu zprávy do hexadecimálního formátu

Převod klíče do hexadecimálního formátu pomocí ASCII tabulky															
5	0	4	6	1	9	4	N	1	5	0	3	3	7	8	E
35	**30**	**34**	**36**	**31**	**39**	**34**	**4E**	**31**	**35**	**30**	**33**	**33**	**37**	**38**	**45**
Převod textu zprávy do hexadecimálního formátu pomocí ASCII tabulky															
P	o	z	o	r		n	a		n	a	m	e	s	t	i
50	**6F**	**7A**	**6F**	**72**	**20**	**6E**	**61**	**20**	**6E**	**61**	**6D**	**65**	**73**	**74**	**69**

Zdroj: Vlastní zpracování

Následný postup šifrování pomocí algoritmu AES spočívá ve dvou hlavních krocích. Nejprve se musí provést expanze klíče a poté je na řadě samotný proces šifrování zprávy. V případě, že délka šifrovacího klíče bude 128 bitů, se musí provést speciální transformace, po kterých vznikne jedenáct dílčích klíčů, kdy každý klíč má formát maticový 4 × 4 byty. V případě 192bitového klíče vznikne třináct dílčích klíčů a u 256bitového klíče je to patnáct dílčích klíčů. AES patří mezi šifry blokové, což v tomto případě znamená, že zpráva je rozdělena na bloky o délce n = 128 bitů (16 bytů). Každý z těchto bloků se zapíše po sloupcích zleva doprava a odshora dolů do tzv. stavové matice formátu 4 × 4 byty, která je ústřední datovou jednotkou šifry. Nad touto stavovou maticí se postupně pro každý blok zvlášť provedou následující operace:

- substituce bytů (*SubBytes*) prováděná pomocí speciální tabulky, která se nazývá S-BOX,
- rotace řádků (*ShiftRows*),
- substituce sloupců (*MixColumns*),
- přičtení dílčího iteračního klíče (*AddRoundKey*),

6.2.2 Expanze klíče K_E

První důležitou skupinu operací algoritmu AES tvoří expanze klíče K_E, která se dále člení na 11 dílčích iterací (*rounds*). Po jejich provedení vznikne 11 dílčích klíčů.

Šifrovací klíč se zapíše po bytech do matice 4 × 4. Jednotlivé byty klíče se do matice zapisují postupně shora dolů (viz tabulka 10). Se sloupcem $w[3]$ se provede operace ***RotWord*** – rotace bytů o jednu pozici směrem nahoru. Následně se na byty tohoto sloupce aplikuje

substituce ***SubBytes*** – záměna bytů sloupce *w*[3] za hodnoty dané substituční tabulkou (tabulka **S-Box** – viz příloha 1). Poslední z dílčích operací prováděných nad sloupcem *w*[3] je přidání iterační konstanty ***Rcon*** k tomuto sloupci, což znamená, že se provede logická operace XOR (exkluzivní disjunkce – v dalším textu reprezentovaná operátorem ⊕) sloupce *w*[3] a konstanty *Rcon*, která má pro každou iteraci jinou hodnotu. Pro první iteraci vypadá konstanta *Rcon* takto: (01, 00, 00, 00). Poslední tři byty této konstanty jsou vždy nulové.

Tabulka 10: operace g(w[3]) – RotWord, SubBytes, Rcon

Původní klíč				Operace **RotWord**				Operace **SubBytes**											
w[0]	w[1]	w[2]	w[3]	w[0]	w[1]	w[2]	w[3]	w[0]	w[1]	w[2]	w[3]		Rcon(1)		w[0]	w[1]	w[2]	g(w[3])
35	31	31	33	35	31	31	37	35	31	31	9A		01		35	31	31	**9B**
30	39	35	37	30	39	35	38	30	39	35	07	⊕	00	=	30	39	35	07
34	34	30	38	34	34	30	45	34	34	30	6E		00		34	34	30	6E
36	4E	33	45	36	4E	33	33	36	4E	33	C3		00		36	4E	33	C3

Zdroj: Vlastní zpracování

Dalším krokem je výpočet sloupců w[4], w[5], w[6] a w[7] pro další matici, která bude reprezentovat první iterační klíč. Jedná se o následující operace:

- $w[4] = w[0] \oplus g(w[3])$
- $w[5] = w[4] \oplus w[1]$
- $w[6] = w[5] \oplus w[2]$
- $w[7] = w[6] \oplus w[3]$

Detailní rozbor výpočtu prvního iteračního klíče je znázorněn v tabulce 11. Další iterační klíče vzniknou stejným postupem. Základem pro výpočet druhého iteračního klíče jsou sloupce matice *w*[4], *w*[5], *w*[6] a *w*[7] atd. Po výpočtu všech iteračních klíčů vznikne matice o rozměru 4 řádky × 44 sloupců. Obecně se tedy sloupce, pro jejichž index *i* platí, že $\boldsymbol{i \bmod 4 \neq 0}$, vypočítají podle předpisu $\boldsymbol{w[i] = w[i-1] \oplus w[i-4]}$.

Sloupce, pro jejichž index *i* platí, že $\boldsymbol{i \bmod 4 = 0}$, se určí podle následujícího předpisu $\boldsymbol{w[i] = g(w[i-1]) \oplus w[i-4]}$, kde zápis *g*(*w*[*i-1*]) reprezentuje již popsané operace *RotWord*, *SubBytes* a *Rcon*, které se provedou nad *i-1* sloupcem.

Tabulka 11: Příklad výpočtu prvního iteračního klíče

	3	5	3	0	3	4	3	6
	0 0 1 1	0 1 0 1	0 0 1 1	0 0 0 0	0 0 1 1	0 1 0 0	0 0 1 1	0 1 1 0
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
	1 0 0 1	1 0 1 1	0 0 0 0	0 1 1 1	0 1 1 0	1 1 1 0	1 1 0 0	0 0 1 1
	9	B	0	7	6	E	C	3
w[4]	1 0 1 0	1 1 1 0	0 0 1 1	0 1 1 1	0 1 0 1	1 0 1 0	1 1 1 1	0 1 0 1
	A	E	3	7	5	A	F	5
	A	E	3	7	5	A	F	5
	1 0 1 0	1 1 1 0	0 0 1 1	0 1 1 1	0 1 0 1	1 0 1 0	1 1 1 1	0 1 0 1
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
	0 0 1 1	0 0 0 1	0 0 1 1	1 0 0 1	0 0 1 1	0 1 0 0	0 1 0 0	1 1 1 0
	3	1	3	9	3	4	4	E
w[5]	1 0 0 1	1 1 1 1	0 0 0 0	1 1 1 0	0 1 1 0	1 1 1 0	1 0 1 1	1 0 1 1
	9	F	0	E	6	E	B	B
	9	F	0	E	6	E	B	B
	1 0 0 1	1 1 1 1	0 0 0 0	1 1 1 0	0 1 1 0	1 1 1 0	1 0 1 1	1 0 1 1
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
	0 0 1 1	0 0 0 1	0 0 1 1	0 1 0 1	0 0 1 1	0 0 0 0	0 0 1 1	0 0 1 1
	3	1	3	5	3	0	3	3
w[6]	1 0 1 0	1 1 1 0	0 0 1 1	1 0 1 1	0 1 0 1	1 1 1 0	1 0 0 0	1 0 0 0
	A	E	3	B	5	E	8	8
	A	E	3	B	5	E	8	8
	1 0 1 0	1 1 1 0	0 0 1 1	1 0 1 1	0 1 0 1	1 1 1 0	1 0 0 0	1 0 0 0
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
	0 0 1 1	0 0 1 1	0 0 1 1	0 1 1 1	0 0 1 1	1 0 0 0	0 1 0 0	0 1 0 1
	3	3	3	7	3	8	4	5
w[6]	1 0 0 1	1 1 0 1	0 0 0 0	1 1 0 0	0 1 1 0	0 1 1 0	1 1 0 0	1 1 0 1
	9	D	0	C	6	6	C	D

w[4] = w[0] ⊕ g(w[3])	**w[5] = w[4] ⊕ w[1]**	**w[6] = w[5] ⊕ w[2]**	**w[7] = w[6] ⊕ w[3]**
AE	9F	AE	9D
37	0E	3B	0C
5A	6E	5E	66
F5	BB	88	CD

Zdroj: Vlastní zpracování

Klíče (zapsané do řádků) pro první a další iterace vypadají pro referenční příklad takto:

```
Klíč 0  (iterace 0):  35 30 34 36 31 39 34 4E 31 35 30 33 33 37 38 45
Klíč 1  (iterace 1):  AE 37 5A F5 9F 0E 6E BB AE 3B 5E 88 9D 0C 66 CD
Klíč 2  (iterace 2):  52 04 E7 AB CD 0A 89 10 63 31 D7 98 FE 3D B1 55
Klíč 3  (iterace 3):  71 CC 1B 10 BC C6 92 00 DF F7 45 98 21 CA F4 CD
Klíč 4  (iterace 4):  0D 73 A6 ED B1 B5 34 ED 6E 42 71 75 4F 88 85 B8
Klíč 5  (iterace 5):  D9 E4 CA 69 68 51 FE 84 06 13 8F F1 49 9B 0A 49
Klíč 6  (iterace 6):  ED 83 F1 52 85 D2 0F D6 83 C1 80 27 CA 5A 8A 6E
Klíč 7  (iterace 7):  13 FD 6E 26 96 2F 61 F0 15 EE E1 D7 DF B4 6B B9
Klíč 8  (iterace 8):  1E 82 38 B8 88 AD 59 48 9D 43 B8 9F 42 F7 D3 26
Klíč 9  (iterace 9):  6D E4 CF 94 E5 49 96 DC 78 0A 2E 43 3A FD FD 65
Klíč 10 (iterace 10): 0F B0 82 14 EA F9 14 C8 92 F3 3A 8B A8 0E C7 EE
```

6.2.3 Šifrování zprávy *Z*

Druhou důležitou skupinu operací tvoří **samotný proces šifrování otevřené (původní) zprávy**. Nejprve se jednotlivé byty zprávy zapíší do stavové matice o rozměru 4 × 4. Následně se provede iniciační šifrovací operace a ke stavové matici se přičte (operace XOR) původní klíč.

Tabulka 12: Iniciační šifra

Původní zpráva Z					**Původní klíč K_E**					**Iniciační šifra**			
stavová matice					w[0]	w[1]	w[2]	w[3]		nová stavová matice			
50	72	20	65	⊕	35	31	31	33	=	65	43	11	56
6F	20	6E	73		30	39	35	37		5F	19	5B	44
7A	6E	61	74		34	34	30	38		4E	5A	51	4C
6F	61	6D	69		36	4E	33	45		59	2F	5E	2C

Zdroj: Vlastní zpracování

Dalším krokem je substituce bytů nové stavové matice (operace ***SubBytes***). Stejně jako v případě expanze klíče, i zde se využije substituční tabulka S-Box. Následuje operace ***ShiftRows***, při které dojde u druhého řádku k rotaci o jeden byte vlevo, u třetího řádku o dva byty vlevo a u čtvrtého řádku o tři byty vlevo. U prvního řádku se rotace neprovádí.

Další operace nazvaná ***MixColumns*** spočívá v substituci sloupců stavové matice, která se provede vynásobením mixovací matice *M* a jednotlivých sloupců stavové matice. Z povahy prováděných operací vyplývá, že tuto substituci lze popsat lineárními vztahy, což znamená, že hodnota každého bytu transformovaného sloupce je lineárně závislá na hodnotě všech

čtyř bytů sloupce původní matice. Princip operací *SubBytes*, *ShiftRows* a *MixColumns* dokládají tabulky 13, 14 a 15.

Tabulka 13: operace SubBytes a ShiftRows

Iniciační šifra nová stavová matice				**SubBytes** S-Box				**ShiftRows** rotace řádků			
65	43	11	56	4D	1A	82	B1	4D	1A	82	B1
5F	19	5B	44	CF	D4	39	1B	D4	39	1B	CF
4E	5A	51	4C	2F	BE	D1	29	D1	29	2F	BE
59	2F	5E	2C	CB	15	58	71	71	CB	15	58

Zdroj: Vlastní zpracování

Tabulka 14: operace MixColumns obecný zápis

M					**S**		**S'**	
02	03	01	01	×	$S_{1,c}$	=	$S'_{1,c}$	= $(\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c} \oplus S_{4,c}$
01	02	03	01		$S_{2,c}$		$S'_{2,c}$	$S_{1,c} \oplus (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c}) \oplus S_{4,c}$
01	01	02	03		$S_{3,c}$		$S'_{3,c}$	$S_{1,c} \oplus S_{2,c} \oplus (\{02\} \bullet S_{3,c}) \oplus (\{03\} \bullet S_{4,c})$
03	01	01	02		$S_{4,c}$		$S'_{4,c}$	$(\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c} \oplus (\{02\} \bullet S_{4,c})$

Zdroj: Vlastní zpracování

Tabulka 15: operace MixColumns pro referenční příklad

Mixovací matice M					**Matice po operaci ShiftRows**					**Matice po operaci MixColumns**			
02	03	01	01	x	4D	1A	82	B1	=	5D	9D	08	D5
01	02	03	01		D4	39	1B	CF		E7	D8	D0	B5
01	01	02	03		D1	29	2F	BE		B3	37	F8	F1
03	01	01	02		71	CB	15	58		30	B3	83	09

Zdroj: Vlastní zpracování

Poslední dílčí operací je **AddRoundKey**, při které se provede operace XOR se stavovou maticí a maticí odpovídající dílčímu klíči K_i, která vznikla při *i-té* iteraci expanze klíče.

Tabulka 16: operace AddRoundKey

Stavová matice po operaci MixColumns					**Klíč 1**					**Stavová matice po operaci AddRoundKey**			
5D	9D	08	D5	⊕	AE	9F	AE	9D	=	F3	02	A6	48
E7	D8	D0	B5		37	0E	3B	0C		D0	D6	EB	B9
B3	37	F8	F1		5A	6E	5E	66		E9	59	A6	97
30	B3	83	09		F5	BB	88	CD		C5	08	0B	C4

Zdroj: Vlastní zpracování

Nová stavová matice se použije při další iteraci šifrování. Popsaný postup, kdy se provádí operace *SubBytes*, *ShifRows*, *MixColumns* a *AddRoundKey,* se aplikuje celkem devětkrát a označuje se jako **hlavní šifra**. Poté následuje šifra finální, při které se provedou operace *SubBytes*, *ShiftRows* a *AddRoundKey*. Výsledkem je stavová matice, v níž jsou uloženy jednotlivé byty kryptogramu *C*.

Jednotlivé byty stavových matic zapsané do řádků vypadají pro referenční příklad takto:

```
Iterace 0:  50 6F 7A 6F 72 20 6E 61 20 6E 61 6D 65 73 74 69
Iterace 1:  F3 D0 E9 C5 02 D6 59 08 A6 EB A6 0B 48 B9 97 C4
Iterace 2:  71 8E 70 56 2D 91 ED BF FF AB C9 DC 2A E2 63 4E
Iterace 3:  46 25 E9 EC FB 7D 0D 93 19 31 71 7B 08 64 33 A2
Iterace 4:  3A 08 10 2B F0 BF 28 7F DA EE A5 EC 98 85 5C 42
Iterace 5:  F0 52 3A A4 A8 A2 C6 90 12 E6 AD EA 6F 2F 5D 00
Iterace 6:  56 BC D3 B4 96 8A 00 DB D5 D9 E7 32 B2 B2 C3 2C
Iterace 7:  0D 66 01 E6 51 2A 14 41 95 90 C9 EA 5E CF 9A A0
Iterace 8:  A2 18 90 39 A7 E1 0A FF B3 61 7E 0A DA 5B C5 12
Iterace 9:  30 F2 B0 58 C3 33 44 55 9F A3 80 81 78 25 60 98
Iterace 10: 0B 73 4F 52 C4 F3 C4 A2 49 CC DD 77 14 87 DC E2
```

Původní zpráva, která se v hexadecimální reprezentaci skládá z těchto bytů:
50 6F 7A 6F 72 20 6E 61 20 6E 61 6D 65 73 74 69 se při použití algoritmu AES
a klíče *35 30 34 36 31 39 34 4E 31 35 30 33 33 37 38 45* zašifruje do kryptogramu
0B 73 4F 52 C4 F3 C4 A2 49 CC DD 77 14 87 DC E2.

Proces dešifrování do podoby původní, a tím do zprávy *Z* srozumitelné pro příjemce, bude úspěšně proveden pouze tehdy, pokud se příjemce zprávy bude nacházet v oblasti vymezené šifrovacím klíčem K_E.

Při dešifrování zprávy zašifrované pomocí AES se postupuje v inverzním pořadí a používají se inverzní transformace *InvSubBytes*, *InvShiftRows*. Transformace *AddRoundKey* je inverzní sama k sobě, neboť odečítání v použitém tělese je totožné s přičítáním (Burda, 2013). Dešifrování začíná provedením *AddRoundKey* – zde se použije *klíč 10*. Poté se devětkrát provedou transformace hlavního dešifrování *InvShiftRows*, *InvSubBytes*, *AddRoundKey* a *InvMixColumns*. Finální dešifrování je zakončeno transformacemi *InvShiftRows*, *InvSubBytes* a transformací *AddRoundKey*, při které se použije *klíč 0*.

7 Návrh konceptuálního řešení

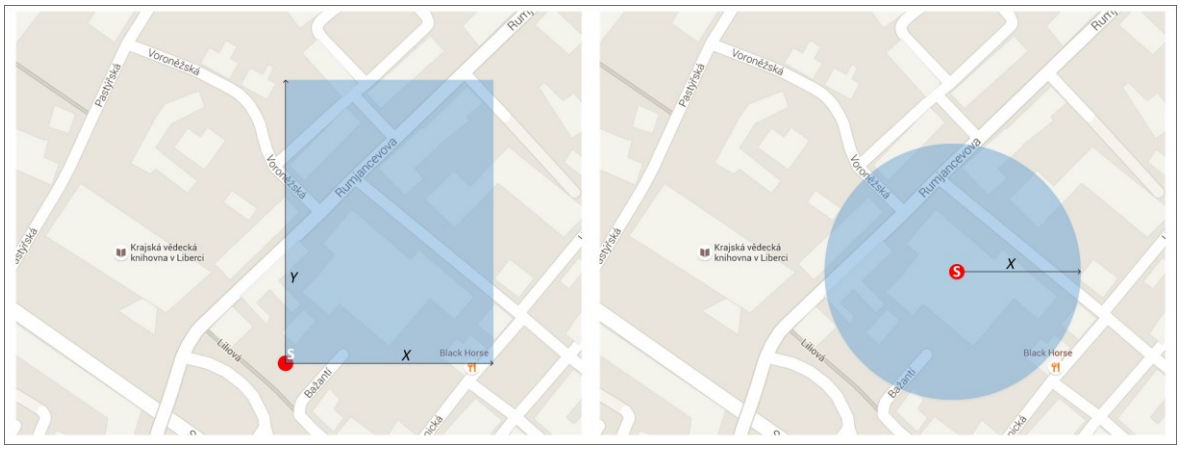
Jak bylo uvedeno v předchozích kapitolách, primárním cílem disertační práce je návrh konceptuálního řešení systému pro distribuci pozičně šifrovaných varovných informací. Navržené řešení by mělo být obecně využitelné, tedy i nezávislé na použité platformě. Počáteční rozbor možností vymezení oblasti pro příjem dešifrované zprávy, který je důležitý pro vytvoření šifrovacího klíče, je uveden v následující podkapitole 7.1. V podkapitole 7.2 je pak rozpracován návrh konceptuálního modelu pomocí modelování UML, konkrétně se jedná o metody *use case diagram* a *activity diagram.*

7.1 Vymezení oblasti pro příjem dešifrované varovné zprávy

Dalším stěžejním bodem pro vytvoření koncepce varovného systému, který bude schopen zajistit exkluzivitu informací pro určitou lokalitu, je navrhnout řešení, pomocí něhož bude možné vymezit lokalitu pro příjem varovné zprávy v dešifrované podobě. To znamená, že je nutné stanovit rozsah oblasti, ve které bude potenciální příjemce schopen získat zprávu v originální podobě (tj. správně dešifrovanou).

Šifrovací klíč, který se na základě příslušné šifrovací funkce aplikuje na otevřenou (původní) zprávu před jejím přenosem, se vztahuje k jednomu konkrétnímu bodu (bod *S*) – jedná se o průsečík zeměpisné šířky a délky. Pokud se osoba disponující odpovídajícím zařízením pro příjem varovné zprávy bude nacházet přesně v tomto bodě, resp. GPS přijímač vyhodnotí aktuální pozici jako pozici shodnou se šifrovacím klíčem, mělo by zařízení (nebo aplikace v něm) zajistit dešifrování a následné zobrazení, případně hlasovou interpretaci zprávy v původním (originálním) znění.

Následně je důležité navrhnout vhodný postup pro vymezení rozšířené oblasti, jejímž základem bude bod S, který je současně i dešifrovacím klíčem. Tento postup by měl zajistit, aby varovná zpráva mohla být dešifrována **v rozšířeném okolí bodu S**, nikoliv pouze v jednom konkrétním bodě, neboť cílem je varovat co nejvíce osob v určité oblasti a zároveň zamezit zobrazení zprávy v ostatních lokalitách.



Obrázek 24: Vymezení obdélníkové a kruhové oblasti pro příjem dešifrované zprávy
Zdroj: Vlastní zpracování

Oblast pro příjem zprávy bude definována parametrem, který může být nazván jako **dosah zprávy** (*DZ*). Tento parametr se ale musí distribuovat v nezašifrované části zprávy. V úvahu připadá několik způsobů, pomocí kterých lze vymezit oblast rozsáhlejší než jeden konkrétní zeměpisný bod. Jedná se o tyto způsoby:

- vymezení oblasti na základě **předem definované přesnosti** – bod *S* se může nacházet uvnitř i na hranici vymezené oblasti,
- vymezení pomocí **čtvercové** (případně obdélníkové) plochy – bod *S* je hraničním bodem vymezené oblasti,
- vymezení pomocí **kruhové** (případně eliptické) plochy – bod *S* se nachází uvnitř vymezené oblasti,
- vymezení pomocí polygonu.

7.1.1 Vymezení oblasti na základě předem definované přesnosti určení bodu

Základními používanými metodami budou trigonometrické výpočty pro určení vzdálenosti dvou geografických bodů. Výpočet vzdálenosti dvou bodů je klíčový pro určení výchozí přesnosti, na jejímž základě se stanoví velikost vymezené oblasti. **Cílem je najít množinu takových geografických bodů, které budou mít nějakou společnou vlastnost.** Nejprve bude provedeno posouzení tří trigonometrických metod pro výpočet vzdálenosti mezi dvěma body, a to: a) *Haversine formula*, b) *Spherical Law of Cosines,* c) *Equirectangular approximation*.

a) Haversine formula

Vzorec (1) je klasickou verzí tzv. Haversinova vzorce, který na základě vstupních hodnot, jimiž jsou zeměpisné souřadnice dvou bodů a poloměr Země, určí nejkratší kruhovou vzdálenost mezi dvěma body, přičemž se ignoruje georeliéf zemského povrchu. Určitá nepřesnost této metody spočívá v tom, že výpočty jsou založeny na předpokladu kulového modelu Země. Ve skutečnosti tvar Země odpovídá fyzikálnímu modelu, který se nazývá geoid. Pro účely satelitní navigace a geodézie se používá model nazvaný referenční elipsoid. Nicméně zmíněná nepřesnost je pro účely vymezení oblasti pro příjem šifrované varovné zprávy zanedbatelná.

$$d = 2 * R_Z * \arcsin\left(\sqrt{\sin^2\left(\frac{\varphi_2-\varphi_1}{2}\right) + \cos\varphi_1 * \cos\varphi_2 * \sin^2\left(\frac{\lambda_2-\lambda_1}{2}\right)}\right) \qquad (1)$$

V roce 1984 byl vzorec (1) upraven pro účely zpracování na počítačích (Sinnott, 1984). V současné době se v různých aplikacích používá reprezentace pomocí vzorců (2), (3) a (4), s využitím funkce *arctg2* (*atan2*), která je dostupná ve většině programovacích jazyků.

$$a = \sin^2\left(\frac{\varphi_2-\varphi_1}{2}\right) + \cos\varphi_1 * \cos\varphi_2 * \sin^2\left(\frac{\lambda_2-\lambda_1}{2}\right) \qquad (2)$$

$$c = 2 * \text{arctg2}\left(\sqrt{a}, \sqrt{(1-a)}\right) \text{ nebo také } c = 2 * \arcsin(\sqrt{a}) \qquad (3)$$

$$d = R_Z * \text{c} \qquad (4)$$

d ... vzdálenost mezi dvěma body, φ ... zemská šířka, λ ... zemská délka, R_z ... poloměr zeměkoule

b) Spherical Law of Cosines

Alternativou vzorce *Haversine formula* je analogie kosinové věty pro trojúhelník v rovině, která je platná pro trojúhelník na kulové ploše. Tato metoda se nazývá *Spherical Law of Cosines* (kosinová věta pro sférický trojúhelník) a vzdálenost dvou bodů se vypočítá podle vzorce (5).

$$d = \arccos(\sin\varphi_1 * \sin\varphi_2 + \cos\varphi_1 * \cos\varphi_2 * \cos(\lambda_2 - \lambda_1)) * R_Z \qquad (5)$$

d ... vzdálenost mezi dvěma body, φ ... zemská šířka, λ ... zemská délka, R_z ... poloměr zeměkoule

c) Equirectangular approximation

Pokud je kladen důraz na rychlost strojového výpočtu, lze pro výpočet vzdálenosti dvou bodů použít metodu *Equirectangular approximation* (rovnoběžná aproximace). Je založena na aplikaci Pythagorovy věty na rovnoběžnou projekci a její přesnost je stále dostatečná. Postup výpočtu je patrný ze vzorců (6), (7) a (8).

$$x = (\lambda_2 - \lambda_1) * \cos(\frac{\varphi_1 + \varphi_2}{2}) \quad (6)$$

$$y = (\varphi_2 - \varphi_1) \quad (7)$$

$$d = R_z * \sqrt{x^2 + y^2} \quad (8)$$

d ... vzdálenost mezi dvěma body, φ ... zemská šířka, λ ... zemská délka, R_z ... poloměr zeměkoule

Pro úplnost lze uvést metodu ***Vincenty's formula***, kterou Thaddeus Vincenty publikoval v roce 1975. Její pomocí lze vypočítat vzdálenost mezi dvěma body s přesností na milimetry (jednotky milimetrů i pro velké vzdálenosti). Na rozdíl od předchozích výpočtů je tato metoda založena na výpočtech vzdálenosti dvou bodů na referenčním elipsoidu a nikoliv na kulové ploše. Nevýhodou je vyšší náročnost na hardwarové prostředky. S ohledem na přesnost pozičních systémů a potřeby vymezení pozice nemá využívání této metody pro daný účel opodstatnění.

Testovací výpočty byly provedeny pro čtyři různé úrovně vzdálenosti. Velká vzdálenost odpovídala řádově stovkám kilometrů, střední vzdálenost jednotkám kilometrů, malá vzdálenost stovkám metrů a velmi malá vzdálenost desítkám metrů. Bylo zjištěno, že rozdíl ve výpočtech mezi použitými trigonometrickými metodami je pro účely varovného systému zanedbatelný. Konkrétní data jsou uvedena v tabulce 17. V dalších výpočtech bude dále aplikována pouze metoda *Spherical Law of Cosines*.

Dalším úkolem bylo stanovit vzdálenosti mezi tzv. **sousedními** body pro různé úrovně přesnosti. Pro tyto účely byl vybrán souřadnicový systém WGS84 (viz kapitola 6.1), konkrétně formát zobrazení stupňů a minut v desetinném tvaru (hddd°mm.mmm'). Byl stanoven **výchozí (referenční) bod A** o souřadnicích N50°25.91868', E15°48.61177', který se nachází v ČR (Dvůr Králové nad Labem), a pomocí metody *Spherical Law of Cosines* byla pro různé úrovně přesnosti určena vzdálenost k sousednímu bodu B.

Tabulka 17: Komparace trigonometrických metod pro výpočet vzdálenosti dvou bodů

Velká vzdálenost	*hddd°mm.mmm'*		Vzdálenost [m] **SLoC**	Vzdálenost [m] **HF**	Vzdálenost [m] **EA**
Bod A (ČR)	φ	N50 26.11868	**1064345,55820898**	**1064345,55820899**	**1064345,59354475**
	λ	E15 48.61177			
Bod B (Švédsko)	φ	**N60 00.43094**			
	λ	E15 **50**.61177			

Rozdíly ve výpočtech	**SLoC**	**HF**	**EA**
SLoC		4,424E-09	3,534E-02
HF	-4,424E-09		3,534E-02
EA	-3,534E-02	-3,534E-02	

Střední vzdálenost	*hddd°mm.mmm'*		Vzdálenost [m] **SLoC**	Vzdálenost [m] **HF**	Vzdálenost [m] **EA**
Bod A (ČR)	φ	N50 25.91868	**7506,272900650**	**7506,272900565**	**7506,272957470**
	λ	E15 48.61177			
Bod B (ČR)	φ	N50 2**9**.91868			
	λ	E15 4**9**.61177			

Rozdíly ve výpočtech	**SLoC**	**HF**	**EA**
SLoC		-8,468E-08	5,682E-05
HF	8,468E-08		5,690E-05
EA	-5,682E-05	-5,690E-05	

Malá vzdálenost	*hddd°mm.mmm'*		Vzdálenost [m] **SLoC**	Vzdálenost [m] **HF**	Vzdálenost [m] **EA**
Bod A (ČR)	φ	N50 25.91868	**300,1520238592**	**300,1520367880**	**300,1520368389**
	λ	E15 48.61177			
Bod B (ČR)	φ	N50 25.**8**1868			
	λ	E15 48.**8**1177			

Rozdíly ve výpočtech	**SLoC**	**HF**	**EA**
SLoC		1,293E-05	1,298E-05
HF	-1,293E-05		5,088E-08
EA	-1,298E-05	-5,088E-08	

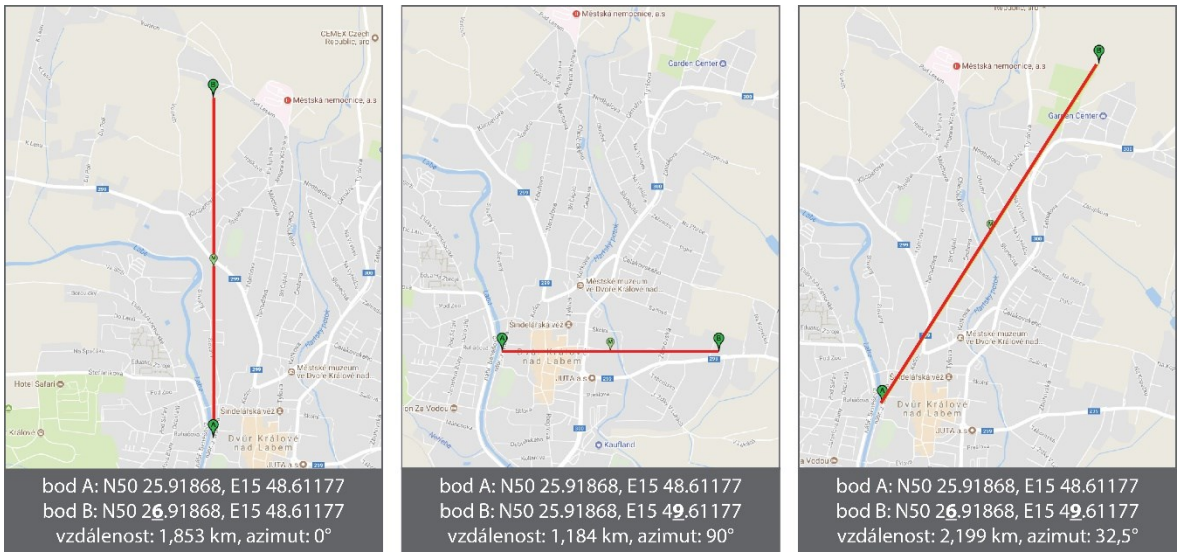
Velmi malá vzdálenost	*hddd°mm.mmm'*		Vzdálenost [m] **SLoC**	Vzdálenost [m] **HF**	Vzdálenost [m] **EA**
Bod A (ČR)	φ	N50 25.91868	**87,8918351206**	**87,8918491997**	**87,8918492005**
	λ	E15 48.61177			
Bod B (ČR)	φ	N50 25.9**5**868			
	λ	E15 48.6**5**177			

Rozdíly ve výpočtech	**SLoC**	**HF**	**EA**
SLoC		1,408E-05	1,408E-05
HF	-1,408E-05		8,569E-10
EA	-1,408E-05	-8,569E-10	

φ - zem. šířka, **λ** - zem. délka, **SLoC** - *Spherical Law of Cosines* , **HF** - *Haversine formula* , **EA** - *Equirectangular approximation*

Zdroj: Vlastní zpracování

Sousedním bodem výchozího bodu A na úrovni přesnosti „jednotek minut“ je například bod B o souřadnicích N50 2**6**.91868, E15 48.61177. Jelikož změna v hodnotách souřadnic proběhla pouze na **úrovni zemské šířky**, a to konkrétně o jednu minutu směrem na sever, nachází se bod B ve vzdálenosti 1,853 km severně od bodu A, což odpovídá azimutu 0°. Obdobně, pokud se **zvětší zemská délka** o jednu minutu, budou souřadnice bodu B následující: N50 25.91868, E15 4**9**.61177. Bod B bude ležet 1,184 km východním směrem (azimut 90°) od bodu A. Pokud dojde u bodu B ke zvětšení zemské šířky i délky o jednu minutu, bude mít bod B souřadnice N50 2**6**.91868, E15 4**9**.61177. Vzdálenost mezi body je v tomto případě 2,199 km s azimutem 32,5°. Tyto vzdálenosti jsou graficky znázorněny na obrázku 25. Vypočítané hodnoty vzdálenosti mezi dvěma sousedními body pro různé úrovně přesnosti jsou uvedeny v tabulce 18.



Obrázek 25: Vzdálenost mezi body odpovídající změně o jednu minutu
Zdroj: Vlastní zpracování

V případě použitého souřadnicového formátu hddd°mm.mmm' změna o jednu setinu minuty v souřadnici zemské šířky (tj. severním nebo jižním směrem) odpovídá, bez ohledu na zeměpisnou šířku, metrické vzdálenosti cca 18,5 metru. Ve východním, případně západním směru na úrovni 50. rovnoběžky odpovídá změna o jednu setinu minuty v souřadnici zemské délky vzdálenosti cca 11,8 m.

Pro srovnání: zeměpisné souřadnice N60°00.43094', E15°48.61177' odpovídají bodu, který se nachází ve městě Fagersta ve Švédsku. Zeměpisná délka tohoto místa je stejná jako v případě bodu A, ale leží od něj ve vzdálenosti 1065 km severním směrem. Změna o jednu setinu minuty souřadnice zemské délky zde odpovídá vzdálenosti 9,2 m. Tato hodnota se bude směrem k severnímu pólu zmenšovat. Například na ostrově Špicberky (N79°25.91868', E15°48.61177') je to vzdálenost 3,4 m.

Tabulka 18: Výpočet vzdálenosti mezi „sousedními“ body pro různé úrovně přesnosti

	Místo	Souřadnice hddd°mm.mmm'		Azimut [°]	Vypočítaná vzdálenost [m] **SLoC**
kilometry	Bod A	φ	N50 25.91868	0	1853,249
		λ	E15 48.61177		
	Bod B	φ	N50 26.91868		
		λ	E15 48.61177		
	Bod A	φ	N50 25.91868	90	1180,508
		λ	E15 48.61177		
	Bod B	φ	N50 25.91868		
		λ	E15 49.61177		
	Bod A	φ	N50 25.91868	32,5	2197,189
		λ	E15 48.61177		
	Bod B	φ	N50 26.91868		
		λ	E15 49.61177		
stovky metrů	Bod A	φ	N50 25.91868	180	185,325
		λ	E15 48.61177		
	Bod B	φ	N50 25.81868		
		λ	E15 48.61177		
	Bod A	φ	N50 25.91868	270	118,051
		λ	E15 48.61177		
	Bod B	φ	N50 25.91868		
		λ	E15 48.51177		
	Bod A	φ	N50 25.91868	212,5	219,731
		λ	E15 48.61177		
	Bod B	φ	N50 25.81868		
		λ	E15 48.51177		

	Místo	Souřadnice hddd°mm.mmm'		Azimut [°]	Vypočítaná vzdálenost [m] **SLoC**
desítky metrů	Bod A	φ	N50 25.91868	0	18,533
		λ	E15 48.61177		
	Bod B	φ	N50 25.92868		
		λ	E15 48.61177		
	Bod A	φ	N50 25.91868	90	11,805
		λ	E15 48.61177		
	Bod B	φ	N50 25.91868		
		λ	E15 48.62177		
	Bod A	φ	N50 25.91868	32,5	21,973
		λ	E15 48.61177		
	Bod B	φ	N50 25.92868		
		λ	E15 48.62177		
jednotky metrů	Bod A	φ	N50 25.91868	0	1,851
		λ	E15 48.61177		
	Bod B	φ	N50 25.91968		
		λ	E15 48.61177		
	Bod A	φ	N50 25.91868	90	1,178
		λ	E15 48.61177		
	Bod B	φ	N50 25.91868		
		λ	E15 48.61277		
	Bod A	φ	N50 25.91868	32,5	2,196
		λ	E15 48.61177		
	Bod B	φ	N50 25.91968		
		λ	E15 48.61277		

φ - zem. šířka, **λ** - zem. délka, **SLoC** - výpočet *Spherical Law of Cosines*

Zdroj: Vlastní zpracování

Postup vymezení oblasti, ve které bude přijata zpráva s atributem exkluzivity

Základem pro vymezení oblasti dále navrhovaným způsobem je generování množiny bodů (matice/síť 10 x 10 bodů), která bude tvarem odpovídat pravoúhlému polygonu. Na tuto množinu je kladen požadavek, aby body, které budou tvořit vymezenou oblast (hraniční i vnitřní), měly nějakou **společnou vlastnost**, která bude využita pro vytvoření šifrovacího klíče. Na začátku přenosu zprávy bude pro účely šifrování nejprve definován parametr „**přesnost**“ (**PR**), který určí, které číselné pozice zeměpisných souřadnic budou konstantní a které se budou měnit. Kromě toho, tento parametr také nepřímo přibližně vymezuje velikost oblasti exkluzivního příjmu. Využitelné jsou pro účely uvažovaného systému zejména přesnosti, které jsou barevně zvýrazněné v tabulce 19. Nejvhodnější z nich bude pro praktické využití zřejmě přesnost nazvaná „setiny minut“, pomocí níž lze vymezit oblast

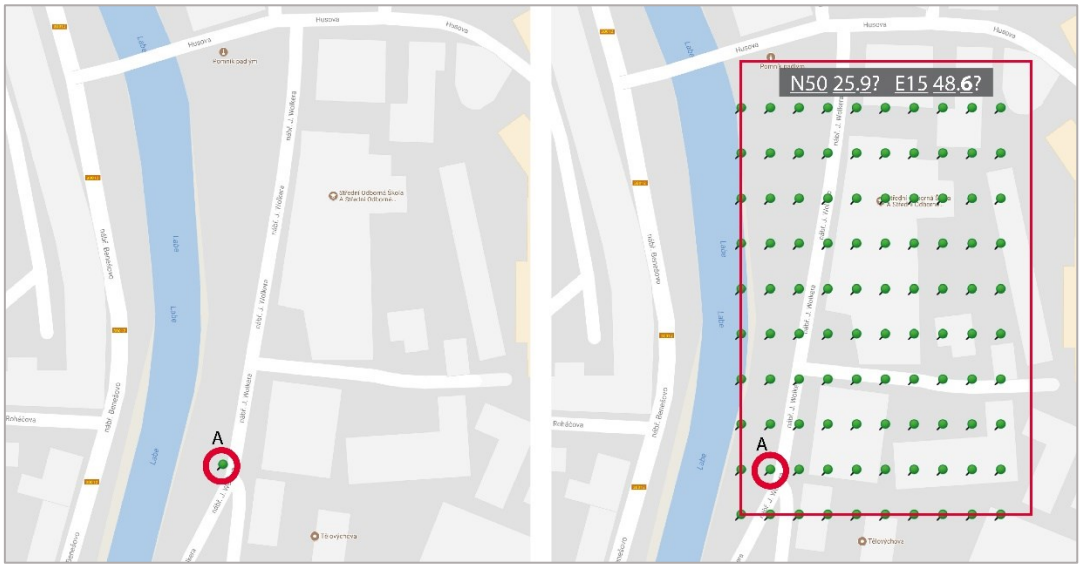
velikosti 185 × 118 m (21 830 m^2). Pro srovnání – na výše zmíněném místě ve Švédsku se jedná o velikost 185 × 92 m (17 020 m^2), na jihu ČR na souřadnicích kolem bodu N48° 52.91868', E15° 48.61177' půjde o oblast 185 × 121 m (22 385 m^2).

Tabulka 19: Velikost vymezené oblasti pro různé úrovně přesnosti

Přesnost (PR)		Pozice změny v souřadnicích	Velikost vymezené oblasti
Kód	Popis		
x0xxxxxx	Desítky stupňů	N5? 25.918, E1? 48.611	1111,4 × 708,3 [km]
xx0xxxxx	Desítky minut	N50 ?5.918, E15 ?8.611	185,3 × 118,9 [km]
xxx0xxxx	Jednotky minut	N50 2?.918, E15 4?.611	18,5 × 11,8 [km]
xxxx0xxx	Desetiny minut	N50 25.?18, E15 48.?11	1,85 × 1,18 [km]
xxxxx0xx	Setiny minut	N50 25.9?8, E15 48.6?1	185 × 118 [m]
xxxxxx0x	Tisíciny minut	N50 25.91?, E15 48.61?	18,5 × 11,8 [m]

Zdroj: Vlastní zpracování

Pokud se stanoví, že přesnost je „jedna setina minuty“, tedy *PR* = xxxxx0xx, znamená to, že kombinace všech číselných možností na úrovni setin minuty vytvoří čtyřúhelník, který bude na každé straně ohraničený deseti zeměpisnými body. Celkově bude vygenerováno 100 bodů, z nich 81 bude ležet uvnitř.



Obrázek 26: Vymezení oblasti pro příjem dešifrované zprávy
Zdroj: Vlastní zpracování s využitím nástroje Incomplete coordinates

Samotný postup generování jednotlivých bodů spočívá v principu tzv. neúplných souřadnic (*incomplete coordinates*). Při uvažované přesnosti budou v souřadnicích referenčního bodu A (N50 25.918, E15 48.611) číslice na pozicích setin minut nahrazeny otazníky. Vznikne

bod A´ o neúplných souřadnicích N50 25.9?, E15 48.6?. Cifry za stanovenou přesností (tj. tisíciny minut a případně další) jsou v tuto chvíli nepodstatné.

Tabulka 20: Souřadnice bodů definující oblast pro příjem dešifrované zprávy

		φ									
		0	1	2	3	4	5	6	7	8	9
λ	9	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99	N50 25.99
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	8	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98	N50 25.98
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	7	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97	N50 25.97
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	6	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96	N50 25.96
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	5	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95	N50 25.95
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	4	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94	N50 25.94
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	3	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93	N50 25.93
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	2	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92	N50 25.92
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	1	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91	N50 25.91
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69
	0	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90	N50 25.90
		E15 48.60	E15 48.61	E15 48.62	E15 48.63	E15 48.64	E15 48.65	E15 48.66	E15 48.67	E15 48.68	E15 48.69

Zdroj: Vlastní zpracování

Pro modelový příklad je stanovena přesnost pro účely šifrování například na úroveň setin minut. Následně budou za otazníky v neúplných souřadnicích N50° 25.9?', E15° 48.6?' postupně dosazovány hodnoty od 0 do 9. Kombinace všech možností na úrovni setin minut vytvoří „obdélníkovou“ síť 100 bodů o rozměrech cca 166,5 m × 106,2 m. Ve skutečnosti se nejedná o ryze obdélníkovou oblast, neboť vzdálenost mezi krajními body se směrem na sever zmenšuje. S přihlédnutím k přesnosti pozičních systémů je pro zde uvedené účely vymezování tato skutečnost zanedbatelná. Při uvažované přesnosti je rozdíl ve vzdálenostech mezi spodními krajními body a horními krajními body 0,003 m. Celková velikost vymezené oblasti odpovídá vzdálenosti cca 185 x 118 m a na obrázku 26 je vyznačena červeným obdélníkem. Konkrétní souřadnice všech 100 bodů jsou uvedeny v tabulce 20. Z tabulky a obrázku je nyní zřejmá hledaná společná vlastnost bodů, která je důležitá pro vytvoření šifrovacího klíče. Všechny body zobrazené na obrázku 26 budou mít požadovanou společnou vlastnost, jíž je pro modelový příklad prvních pět číslic souřadnice zeměpisné šířky a délky, tj. všechny body budou mít na prvních pěti pozicích souřadnice zeměpisné šířky číslice **50259** a na pozicích souřadnice zeměpisné délky **15486**.

Tyto cifry jsou základem pro stanovení 128bitového šifrovacího klíče, který bude pro modelový příklad vypadat následovně: **50259##N15486##N**. Znak # je součástí klíče a jedná se o příznak, že pozice, na které se znak # vyskytuje v rámci souřadnice, je nepodstatná pro dešifrování zprávy. Místo tohoto znaku lze do šifrovacího klíče dosadit jakýkoli jiný znak. Pokud by se přesnost vymezení oblasti zvýšila na úroveň tisícin minut, mohl by šifrovací klíč vypadat takto **502591#N154865#N**, což by odpovídalo souřadnicím N50° 25.91?', E15° 48.65?'.

Pomocí tohoto klíče bude s využitím postupu uvedeného v kapitole 6.2 (algoritmus AES) zašifrována varovná zpráva do podoby kryptogramu. Následně bude zpráva distribuována zvoleným komunikačním kanálem a správně ji dešifrovat budou moci pouze uživatelé těch zařízení, jejichž pozice odpovídá souřadnicím N50° 52.9?' E15° 48.6?'.

Obrázek 27: Vymezení prostoru střední velikosti
Zdroj: Vlastní zpracování s využitím mapových podkladů Google a mapy.cz

Na obrázku 27 je zobrazena názorná situace, kdy operační manažer příslušného vysílacího centra vymezí pětici bodů, do kterých bude chtít distribuovat cílenou, pro ostatní oblasti zašifrovanou zprávu o blížícím se nebezpečí. Vypočítané vzdálenosti mezi body jsou uvedeny v tabulce 21. Z této tabulky je zřejmé, že vymezenou oblast neobsáhne při stanovené úrovni přesnosti na setinu minuty pouze jeden „obdélník“ o rozměrech 185 × 118 m. Uvažovanou oblast lze pokrýt pomocí dvou obdélníků. V tomto případě se budou vysílat dvě zprávy, ovšem pro každou oblast bude použit jiný šifrovací klíč. Pro oblast

danou zeleným obdélníkem na obrázku 28 se bude jednat o klíč 50259##N15486##N, pro oblast odpovídající červenému obdélníku to bude klíč 50259##N15487##N. Rozdíl je sice pouze v jednom znaku klíče, ale vytvořený kryptogram v případě použití algoritmu AES bude zcela rozdílný.

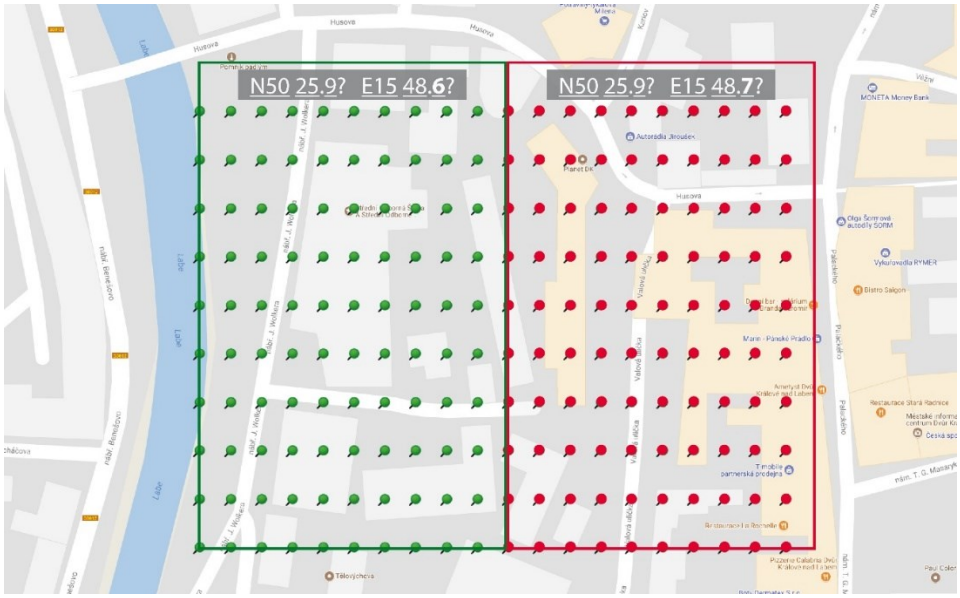
Například pro slovo Pozor vypadá v případě prvního klíče kryptogram takto: `CbqkVJLYibLLUj/XuQyBEw==`. Při použití druhého klíče je kryptogram následující: `0tCkucysYMhmKKf7kluSxg==`.

Tabulka 21: Vzdálenost mezi body, které tvoří oblast vymezenou pro příjem zprávy

		Dvůr Králové nad Labem - Google						
		hddd.dddd°	hddd°mm.mmm'		hddd° mm'ss.s"			Vzdálenost
		Stupně	Stupně	Minuty	Stupně	Minuty	Vteřiny	SLoC [m]
Bod A	φ	50.431978	50	25.91868	50	25	55.122	**od bodu E**
	λ	15.810196	15	48.61176	15	48	36.707	137,9512129
Bod B	φ	50.433612	50	26.01672	50	26	1.002	**od bodu A**
	λ	15.810468	15	48.62808	15	48	37.685	182,7237415
Bod C	φ	50.433511	50	26.01066	50	26	0.641	**od bodu B**
	λ	15.811794	15	48.70764	15	48	42.458	93,91759549
Bod D	φ	50.433109	50	25.98654	50	25	59.194	**od bodu C**
	λ	15.812251	15	48.73506	15	48	44.103	55,41489713
Bod E	φ	50.431817	50	25.90902	50	25	54.54	**Od bodu D**
	λ	15.812124	15	48.72744	15	48	43.646	143,0123302

φ - zem. šířka, **λ** - zem. délka, **SLoC** - výpočet *Spherical Law of Cosines*

Zdroj: Vlastní zpracování



Obrázek 28: Vymezení dvou sousedních oblastí
Zdroj: Vlastní zpracování s využitím nástroje Incomplete coordinates

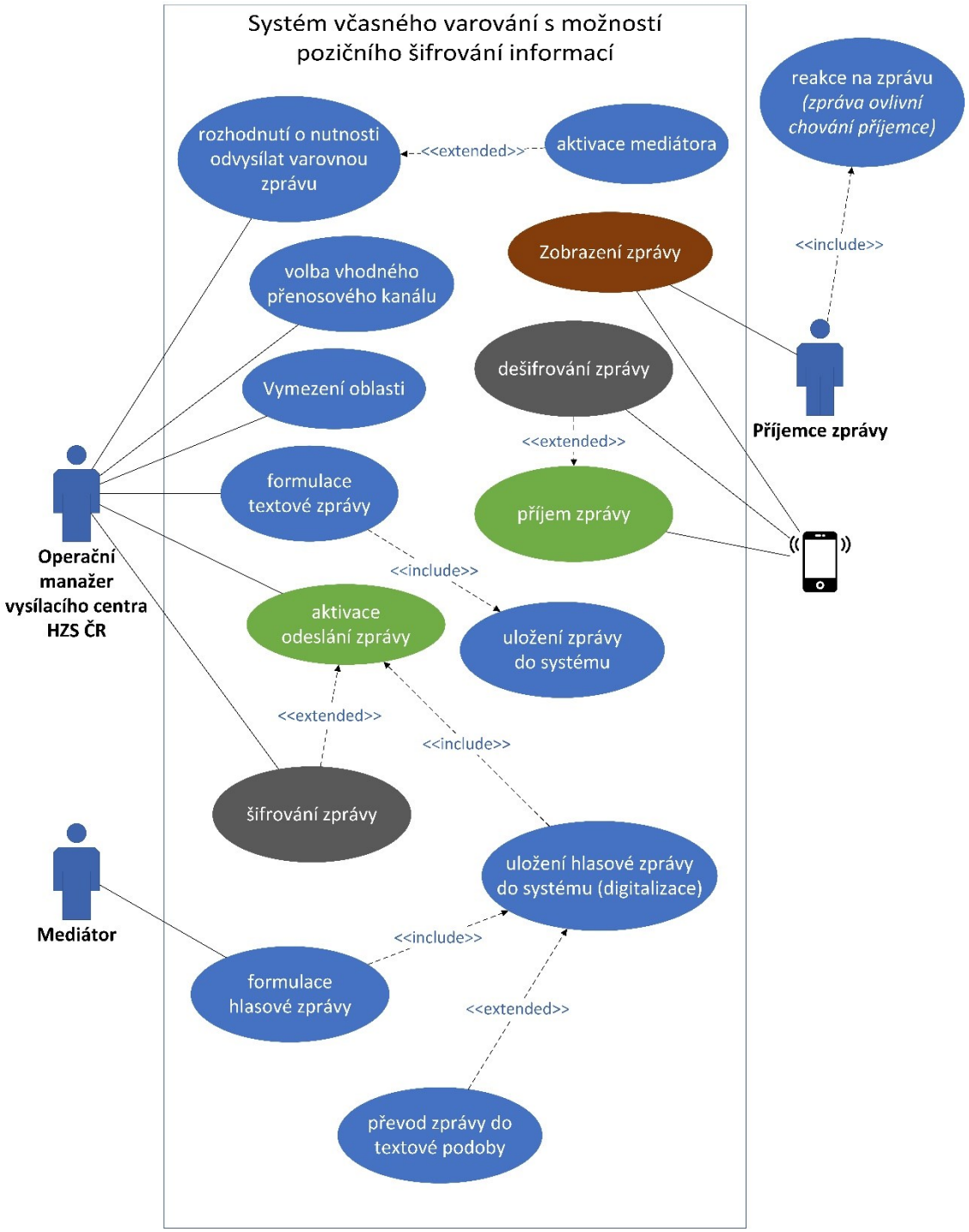
Předpokladem je, že by celý proces fungoval automaticky. To znamená, že operační manažer si na dotykové obrazovce pomocí „mapové“ aplikace vymezí body, které budou tvořit oblast pro příjem varovné zprávy. Následně aplikace na pozadí vytvoří dostatečný počet čtyřúhelníků pro pokrytí vymezené oblasti a pro každý z nich zároveň vygeneruje šifrovací klíč. **Úroveň přesnosti (PR), na jejímž základě se stanoví finální podoba šifrovacího klíče, musí být odvysílána na začátku zprávy nezašifrovaná.** Vývoj testovací aplikace a další metody vymezení oblasti pro příjem šifrované zprávy (a následné dešifrování) a s tím související určení šifrovacího klíče budou předmětem dalšího výzkumu.

7.2 Konceptuální modely

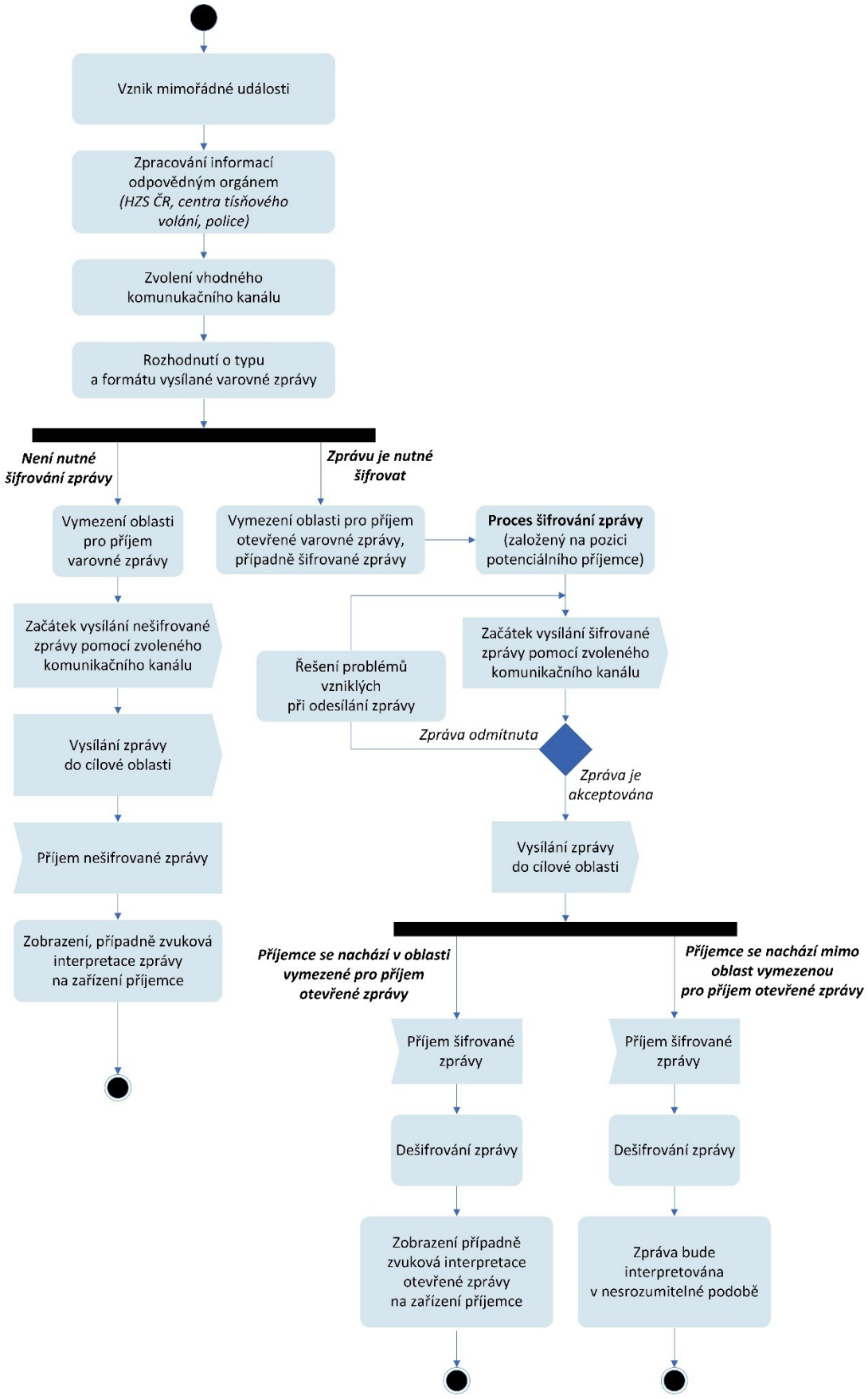
Pro znázornění interakce jednotlivých uživatelských rolí se systémem včasného varování s funkcí pozičního šifrování informací byl použit *use case* diagram (diagram případů užití). Jedná se o jeden z nejpoužívanějších diagramů chování, které patří pod jazyk UML (*Unified Modeling Language*), což je soubor grafických metod, které se používají v softwarovém a systémovém inženýrství.

Diagram na obrázku 29 navazuje na blokové schéma začlenění systému Radio-Help do struktury HZS ČR (obrázek 8), které znázorňuje harmonický způsob, jakým by mohl být zde konceptuálně popisovaný systém začleněn do stávajícího systému IZS, jehož garantem a základní součástí je HZS ČR. Hlavní úlohu na straně distributora informace má **operační manažer vysílacího centra HZS ČR** (reálně se bude jednat spíše o tým), který rozhoduje na základě vstupních informací (vznik mimořádné události, pokyny od některého subjektu státní správy) o tom, zda je v dané situaci nutné odvysílat do potenciálně ohrožených lokalit varovnou zprávu. Pokud ano, rozhoduje dále o vymezení oblasti (může se jednat o více nesouvislých lokalit ve stejný čas), volbě vhodného přenosového kanálu a formulaci zprávy. Dále je v kompetenci operačního manažera aktivovat tzv. mediátora. Mediátor je součástí centrální redakce systému Radio-Help. Mělo by se z pohledu občanů jednat o osobu známou a hlavně důvěryhodnou (hlasatel, moderátor, herec, oblíbený politik, krizový manažer). Hlavním úkolem mediátora v souvislosti s uvažovaným systémem je předat jednotnou, včasnou, kvalifikovanou a srozumitelnou verbální informaci (Skrbek, 2013) takovým způsobem, aby příjemce buď vhodným způsobem aktivovala, pokud jsou ohroženi, nebo naopak uklidňovala v případě sdělení, že ohroženi nejsou.

Operační manažer také rozhoduje o tom, zda je nutné zprávu při konkrétní mimořádné události šifrovat, či nikoli. Pokud ano, využije k tomu postupu zmíněného na konci kapitoly 7.1. Druhým UML diagramem (obrázek 30), který je použit pro znázornění procesní logiky systému včasného varování s funkcí pozičního šifrování, je diagram aktivit (Activity diagram).



Obrázek 29: Use case diagram
Zdroj: Vlastní zpracování



Obrázek 30: UML diagram aktivit – procesní logika systému
Zdroj: vlastní zpracování

8 Ekonomicko-implementační hledisko

8.1 Zavedení systému jako inovace v rámci používaného systému včasného varování

Navrhovaný systém je koncepčně založen na myšlence harmonického začlenění do stávajícího systému IZS, jehož garantem je HZS ČR. Idea systému Radio-Help byla v minulosti prezentována manažerům Českého rozhlasu i HZS. Oslovené instituce přes deklarovaný zájem dosud neprovedly reálné kroky směřující k implementaci cílené distribuce informací do svých řešení krizové komunikace. Důvodem může být i fakt, že inovace IZS v uplynulé dekádě se zaměřovaly spíše na vyrozumění orgánů krizového řízení a složek IZS (viz systém eCall). Jak ale dokazuje již zmíněné lednové sympózium „Ochrana obyvatelstva – Zdravotní záchranářství 2018“ (Hartmann, 2018), je problematika vyšší efektivity a inovací v oblasti varování obyvatelstva nyní velmi aktuální. To nabízí vyšší šanci, že by v budoucnosti mohl někdo kompetentní projevit zájem o koncepční řešení založené na systému Radio-Help.

V úvahu připadá i možnost, že by se realizace systému adresného varování a vyrozumění mohla ujmout soukromá organizace (např. výrobce mobilních telefonů), která by dále poskytovala varovný systém jako placenou službu.

Proces, jakým byl zaváděn systém eCall, může být v některých aspektech inspirací i pro zde navrhovaný systém včasného varování s funkcí pozičního šifrování. Jak dokládají slova některých zúčastněných (kap. 2.2.4), nešlo o jednoduchou proceduru zejména proto, že se jednalo o systém zaváděný v rámci EU. Na uvedení eCallu do praxe pracovaly mezinárodní týmy složené jak z politiků, tak i z odborníků na dopravní problematiku a informační technologie. V rámci podobných jednání obvykle dochází k názorové rozdílnosti a hledání přijatelných kompromisů, což spuštění systému zpravidla oddaluje, a tím i zvyšuje ekonomické náklady.

Navrhovaný systém včasného varování má vzhledem ke koncepčně výrazně odlišným řešením v jednotlivých zemích EU ambice uplatnit se v rámci ČR. Pozitivní skutečností je, že uvažovaná komunikační infrastruktura je de facto již vybudovaná. Pro implementaci je však nezbytné, aby navrhovaný systém našel podporu státu a byl zahrnut do programu příslušných ministerstev. Rovněž by bylo třeba získat pro tuto myšlenku a s ní spojené

technické řešení systému Radio-Help provozovatele uvažovaných distribučních kanálů (např. DAB+) a v neposlední řadě výrobce vhodných audiovizuálních zařízení, do kterých by se implementoval čip pro příjem potřebného signálu. Stejně jako v případě systému eCall by mohlo být hypoteticky podpořeno platnou legislativou, aby se od určitého data začala všechna vhodná zařízení (chytré telefony, autorádia, mp3 přehrávače aj.) vybavovat modulem pro příjem potřebného signálu, který by se mohl implementovat přímo jako součást základní desky (čipu) konkrétního zařízení. Bez zájmu státu jako nositele legislativy, příslušných složek IZS a realizátorů technické stránky systému může navrhovaná koncepce navždy zapadnout, případně by její realizace trvala dlouhé roky.

8.2 Postupně řízená evakuace a její ekonomické zhodnocení

Postupně řízená evakuace může mít smysl například při mimořádných událostech, které byly rozpracovány jako modelové situace v kapitole 4.4. V podmínkách ČR se jedná např. o ohrožení související s narušením hrází vodohospodářských děl. To, že se katastrofa podobného rozsahu v ČR stala naposledy před více než 100 lety (Přehrada Desná, 1916), neznamená, že nemůže, i přes důsledné kontrolní procesy stavu přehrad, znovu nastat. Proto je důležité, aby složky záchranného systému disponovaly technologiemi, které se nemusí využívat příliš často, ale mohou být velmi užitečné zejména v situacích, kdy jsou ohroženy životy většího množství obyvatel. Podle metodiky Nejvyššího soudu byla pro rok 2017 (Vojtek, 2017) stanovena hodnota zmařeného lidského života, která je vyčíslena jako 400násobek průměrného platu, na 11 035 600 Kč. V případě mladého člověka se může jednat o částku vyšší. Pokud by systém včasného varování založený na principu Radio-Help disponoval funkcí pozičního šifrování a byl efektivně využit pro účely řízené evakuace, s vysokou pravděpodobností by bylo možné zvýšit šanci ohrožených občanů na únik z oblastí zkázy a na záchranu životů. To by bylo možné s ohledem na rozsah a formu katastrofy vyčíslit i ekonomicky.

Závěr

V dnešním světě moderních technologií je k dispozici rozmanitá komunikační infrastruktura, kterou je možné využít k tomu, aby aktuálně potřebné informace mohly být včas předány zamýšleným příjemcům. Systémy včasného varování, které jsou určené k tomu, aby zajistily včasné doručení mnohdy kritických informací k příjemci, v některých případech selhávají i přesto, že jsou do nich vložené nemalé finanční prostředky.

Primárním cílem disertační práce v tomto kontextu byl návrh konceptuálního řešení systému, který bude schopen distribuovat varovné informace do určité předem vymezené oblasti s atributem exkluzivity. Exkluzivitou je zde myšleno utajení zprávy před příjemci, kteří by chtěli komunikaci odposlouchávat na jiném místě, než je určeno. Tato metoda se nazývá poziční šifrování a jejím obecným principem je šifrovací algoritmus, který zajistí, aby šifrovaná informace mohla být dešifrována pouze na určitém místě stanoveném odesílatelem. Šifrovací klíč je v tomto případě odvozen od geografických souřadnic cílové oblasti. Motivací pro návrh takto koncipovaného systému byly úvahy, jak vylepšit některé nedostatky stávajících systémů včasného varování s cílem efektivnějšího informování potenciálně ohrožených občanů. Základem systému, který by zajistil exkluzivitu zprávy pro předem vymezené místo, by mohl být systém Radio-Help, jenž je navržen primárně pro adresné varování obyvatel v případě mimořádných událostí. Nadstavbovou funkcí tohoto systému by mohla být právě možnost pozičního šifrování varovných informací.

V rámci této problematiky bylo stanoveno pět výzkumných otázek, které jsou formulovány v kapitole 1.1.2. Nedostatkem stávajících řešení je zejména dosah koncových prvků JSVV a závislost na jednom přenosovém kanálu, jako je tomu v případě varovných SMS zpráv. Předkládané řešení založené na systému Radio-Help počítá s využitím více přenosových kanálů současně. Dominantním přenosovým kanálem systému Radio-Help je rozhlasové vysílání. Jedna z technologií, která je využitelná pro Radio-Help a současně pro princip distribuce pozičně šifrovaných informací, je DAB+. Vzhledem ke snaze provozovatelů o co nejširší pokrytí ČR signálem DAB+ a rostoucí nabídce přijímačů DAB+ se jeví tento přenosový kanál pro účely systému popisovaného v této práci jako využitelný. Nicméně optimálnější z pohledu pokrytí celé ČR by bylo využít princip HD Radia, který funguje hlavně v USA. Hlavní výhodou technologie HD Radio je možnost využití stávajících vysílačů analogového signálu, do jehož modulace může být superponován digitální signál.

Tato koncepce je výhodnější zejména z toho důvodu, že k pokrytí ČR by postačovaly dva středovlnné vysílače. U vysílačů systému DAB+ je dosah bohužel mnohem nižší.

Hlavním přínosem práce je naznačená možnost, jak zprostředkovat novým, dosud nerealizovaným způsobem aktuální potřebné informace odpovídající skutečné míře momentálního nebezpečí adresným příjemcům. Princip pozičního šifrování je v kapitole 4 využit pro návrh modelových situací, které ukazují různé možnosti jeho využití. Jedním z dílčích cílů práce bylo zvolit vhodný algoritmus, který zašifruje varovnou informaci do podoby kryptogramu na základě šifrovacího klíče odvozeného od geografických souřadnic cílové oblasti. Preferovaným algoritmem pro tyto účely je symetrická šifra AES (*Advanced Encryption Standard*). Důvody pro výběr tohoto algoritmu jsou shrnuty v kapitole 5.4.4. Podrobnému rozboru šifrování zprávy pomocí šifry AES se věnuje kapitola 6. Dalším dílčím cílem byl návrh řešení, pomocí něhož by bylo možné vymezit lokalitu pro příjem varovné zprávy v dešifrované podobě.

Dalším stěžejním bodem pro vytvoření koncepce varovného systému schopného zajistit exkluzivitu informací pro určitou lokalitu je navrhnout odpověď na otázku, jak vymezit oblast pro příjem varovné zprávy v dešifrované podobě. Této problematice se podrobně věnuje kapitola 7.1 a řešení je založeno na předem definované přesnosti určení bodu. Tato přesnost je součástí nešifrované části zprávy. Dalším způsobům vymezování oblasti pro účely pozičního šifrování bude věnován následný výzkum. Cílená distribuce varovných informací s atributem exkluzivity se jeví jako využitelná zejména pro účely hromadných a centrálně řízených evakuací. Právě možnost pozičně šifrovat informaci se v těchto případech zdá velmi efektivní a tímto způsobem lze eliminovat některé negativní faktory, které při evakuaci mohou nastat (např. panika). Podrobněji se principu řízené evakuace věnuje kapitola 4.4. Výčet modelových situací není konečný a také této problematice bude věnována pozornost v dalším výzkumu.

Navrhovaný systém je koncipován pro řešení "standardních" mimořádných událostí – tj. takových, které lze s určitou pravděpodobností předpokládat a dle míry pravděpodobnosti i připravovat scénáře pro jejich řešení a řízení. Zároveň však umožňuje předávat potřebné informace a instrukce jednotlivým subjektům i v případě unikátních, jedinečných mimořádných situací, kdy jsou "standardní" komunikační prostředky nefunkční nebo předávání pozičně exkluzivních informací neumožňují.

Seznam použité literatury

AL-FUQAHA, Ala a Omar AL-IBRAHIM. 2007. Geo-Encryption protocol for mobile networks. *Computer Communications Journal*. **30**(11-12): s. 2510–2517, ISSN: 0140-3664.

ANTUŠÁK, Emil. 2009. *Krizový management: hrozby - krize - příležitosti*. Praha: Wolters Kluwer ČR. ISBN 978-80-7357-488-8.

ANTUŠÁK, Emil a Josef VILÁŠEK, 2016. *Základy teorie krizového managementu*. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum. ISBN 978-80-246-3443-2.

ARLOW, Jim a Ila NEUSTADT. 2007. *UML 2 a unifikovaný proces vývoje aplikací: objektově orientovaná analýza a návrh prakticky*. 2., aktualiz. a dopl. vyd. Brno: Computer Press. ISBN 978-80-251-1503-9.

ARMSTRONG, Mark. 2017. *Norway becomes the first country to switch off FM signal* [online]. [cit. 2018-01-15]. Dostupné z: http://www.euronews.com/2017/12/15/norway-becomes-the-first-country-to-switch-off-fm-signal

BUCHALCEVOVÁ, Alena a Iva STANOVSKÁ. 2013. *Příklady modelů analýzy a návrhu aplikace v UML*. Praha: Oeconomica. ISBN 978-80-245-1922-7.

BUMBÁLKOVÁ, Blanka. 2017. *Český rozhlas rozšířil digitální vysílání v Brně, Ostravě a Plzni* [online]. [cit. 2017-12-15]. Dostupné z: http://www.rozhlas.cz/informace/press/_zprava/cesky-rozhlas-rozsiril-digitalni-vysilani-v-brne-ostrave-a-plzni--1773082

BURDA, Karel. 2013. *Aplikovaná kryptografie*. Brno: VUTIUM. ISBN 978-80-214-4612-0.

BURDA, Karel. 2015. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-925-7.

COOMBS, Timothy W. a Sherry J. HOLLADAY. 2012. *The handbook of crisis communication*. Chichester, U. K: Wiley-Blackwell, ISBN 978-1-4443-6190-2.

Český telekomunikační úřad. 2018. *Zemské digitální televizní a rozhlasové vysílání v ČR* [online]. [cit. 2018-02-04]. Dostupné z: http://dtv.ctu.cz/

DAEMEN, Joan a Vincent RIJMEN. 1999. *AES Proposal: Rijndael*. AES Algorithm Submission. Dostupné z: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

DE MULDER, Elke, Thomas EISENBARTH a Patrick SCHAUMONT. 2018. Identifying and Eliminating Side-Channel Leaks in Programmable Systems. *IEEE Design & Test*. **35**(1): 74–89. ISSN 2168-2356. Dostupné také z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8081798

DIFFIE, Whitfield a Martin E. HELLMAN. 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*. **22**(6): 644–654. DOI: 10.1109/TIT.1976.1055638. Dostupné také z: https://ee.stanford.edu/~hellman/publications/24.pdf

FOWLER, Martin. 2009. *Destilované UML*. Praha: Grada. Knihovna programátora (Grada). ISBN 978-80-247-2062-3.

GREINER, Lena. 2016. So funktioniert Katwarn - oder auch nicht [online]. [cit. 2018-02-08]. Dostupné z: http://www.spiegel.de/netzwelt/apps/katwarn-so-funktioniert-das-warnsystem-und-das-sind-die-probleme-a-1104421.html

HARTMANN, David. 2018. Nové trendy systémů varování a vyrozumění obyvatelstva. *Časopis 112* [online]. **17**(3) [cit. 2018-02-20]. Dostupné z: http://www.hzscr.cz/clanek/casopis-112-rocnik-xvii-cislo-3-2018.aspx?q=Y2hudW09MTQ%3d

HZS ČR. 2014. *O sirénách – Varování obyvatelstva* [online]. [cit. 2017-10-20]. Dostupné z: http://www.hzscr.cz/clanek/sireny.aspx

HZS LK. 2016. *Koncové prvky varování* [online]. [cit. 2017-10-20]. Dostupné z: http://www.hzslk.cz/397-koncove-prvky-varovani.html

HZS ČR. 2018. *Varování obyvatelstva* [online]. [cit. 2018-02-04]. Dostupné z: http://www.hzscr.cz/clanek/varovani-obyvatelstva-603225.aspx

HOJGR, Radek a Jan STANKOVIČ. 2007. *GPS: praktická uživatelská příručka*. Brno: Computer Press, ISBN 978-80-251-1734-7.

CHAUDHARI, Smita, Samadhan YANGAD, Ashish JHA a Ashish SURWASE. 2017. "Geo-encryption lite" – A location based Encryption Application for Android. *International Journal of Computer Applications*, 165(4): 13–17. ISSN: 0975-8887.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2001. *Announcing the Advanced Encryption Standard (AES)*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Dostupné z: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

INTERNATIONAL TSUNAMI INFORMATION CENTER – IOC/UNESCO. 2017. *November 5 is World Tsunami Awareness Day* [online]. [cit. 2017-12-10]. Dostupné z: http://itic.ioc-unesco.org/index.php

IOTIC (INDIAN OCEAN TSUNAMI INFORMATION CENTER). 2017. *What is IOTWS* [online]. [cit 2016-08-28]. Dostupné z: http://iotic.ioc-unesco.org/indian-ocean-tsunami-warning-system/16/what-is-iotws

iROZHLAS. 2018. *„Kalamitní stav v dopravě. Dálnice blokují na řadě míst hromadné dopravní nehody“* [online]. [cit. 2018-02-08]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nehody-na-d1-blokuji-dalnici-smerem-na-prahu-na-99-kilometru-havarovalo-10_1801161335_dp

ISMAIL-ZADEH, Alik. 2014. *Extreme natural hazards, disaster risks and societal implications*. New York: Cambridge University Press. ISBN 978-1-107-03386-3.

KHIYAL, Malik S. H., Aihab KHAN a Khansa SHABBIR. 2011. Performance evaluation of encryption techniques for confidentiality of very large databases. *International Journal of Computer Theory and Engineering*. **3**(6): 789–793. ISSN 1793-820. Dostupné také z: http://www.ijcte.org/papers/410-G1188.pdf

MALI, Marko, Franc NOVAK a Anton BIASIZZO. 2005. Hardware Implementation of AES Algorithm. *Journal of ELECTRICAL ENGINEERING*. **56**(9–10): 265–269. ISSN 1335-3632. Dostupné také z: http://cs.ijs.si/novak/k2005-01.pdf

MAREŠ, Miroslav, Jaroslav REKTOŘÍK, JAN ŠELEŠOVSKÝ, et al. 2013. *Krizový management: případové bezpečnostní studie*. Praha: Ekopress. ISBN 978-80-86929-92-7.

MOLNÁR, Zdeněk. 2012. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.

SINGH, Kirat P. a Dod SHIWANI. 2016. An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm. *International Journal of Recent Advances in Engineering & Technology*. **4**(2): 5–9. ISSN 0975-5462. Dostupné také z: https://eprint.iacr.org/2016/789.pdf

PIPER, Fred a Sean MURPHY. 2006. *Kryptografie: průvodce pro každého*. Praha: Dokořán. ISBN 80-7363-074-5.

POLÁK, Lukáš. 2018. *Výrobci mobilních telefonů se k implementaci DAB+ staví zdrženlivě* [online]. [cit. 2018-02-20]. Dostupné z: http://www.rozhlas.cz/digital/digital/_zprava/vyrobci-mobilnich-telefonu-se-k-implementaci-dab-stavi-zdrzenlive--1782153

Pracovní komise Strategické rady Českého rozhlasu pro digitální rozhlasové vysílání. 2014. *Koncepce rozvoje digitálního rozhlasového vysílání.* Dostupné z: http://media.rozhlas.cz/_binary/03330075.pdf

RIVEST, Ronald L., Adi SHAMIR a Leonard M. ADLEMAN. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM.* **21**(2): 120–126. ISSN 0001-0782. Dostupné z: https://dl.acm.org/citation.cfm?id=359342

RTI cz. 2018. *Digitální rozhlas DAB+* [online]. [cit. 2018-02-12]. Dostupné z: http://www.digitalradiodab.cz/files/DAB-brozura_v-01-2018_cz.pdf

SANDEEP, Kumar R., et al. 2017. The AES-256 Cryptosystem Resists Quantum Attacks. *International Journal of Advanced Research in Computer Science*. **8**(3): 404–408. ISSN 0976-5697. Dostupné také z: https://www.researchgate.net/publication/316284124_ The_AES-256_Cryptosystem_Resists_Quantum_Attacks

SCOTT, Logan a Dorothy E. DENNING. 2003a. Geo-Encryption: Using GPS to Enhance Data Security. *GPS World*. (4): 40–49. Dostupné z: http://calhoun.nps.edu/bitstream/handle/ 10945/37168/GPSWorld.pdf?sequence=1&isAllowed=y

SCOTT, Logan a Dorothy E. DENNING. 2003b. Location Based Encryption & Its Role in DigitalCinema Distribution. *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*. Portland: Oregon Convention Center, s. 288–297.

SHANNON, Claude E. 1948. A mathematical theory of communication. *Bell System Technical Journal*. **27**(3): 379–423, 623–656. ISSN 0005-8580.

SHANNON, Claude E. 1949. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. **28**(4): 656–715. ISSN 0005-8580.

SCHNEIER, Bruce. 2015. *Applied cryptography: protocols, algorithms, and source code in C*. 20th anniversary edition. Indianapolis, IN: Wiley. ISBN 978-1119096726.

SIMS, Gary. 2016. *Why Android 7.0 won't officially come to Snapdragon 800/801 devices* [online]. Android Authority. [cit. 2017-04-20]. Dostupné z: https://www.android authority.com/android-7-0-snapdragon-800-801-712930/

SINNOTT, Roger W. 1984. Virtues of the Haversines. *Sky and Telescope* [online]. **68**(2): s. 159 [cit. 2017-11-02]. Dostupné z: http://daimi.au.dk/~dam/thesis/Sky_and_ Telescope_1984.pdf

SKRBEK, Jan. 2010. Informační služby ve specifických situacích. In: Petr DOUCEK (ed.). *Informační management*. Praha: Professional Publishing, s. 129–146. ISBN 978-80-7431-010-2.

SKRBEK, Jan. 2011. Radio-Help as a Smart Early Warning and Notification System. In: *Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences*, UK: University of Hull Business School, 14 s. ISSN 1999-6918. Dostupné z: http://journals.isss.org/index.php/proceedings55th/article/view/1723

SKRBEK, Jan. 2013. Management informačních služeb při řešení mimořádných událostí. In: Petr DOUCEK, Miloš MARYŠKA, Leo NEDOMOVÁ, et al. *Informační management v informační společnosti*. Praha: Professional Publishing, 195–226. ISBN 978-80-7431-097-3.

SKRBEK, Jan. 2015. Last Mile – the Neglected Element of Early Warning Systems: In: *Proceedings of the ISIS Summit Vienna 2015 – The Information Society at the Crossroads.* Vienna, Austria, 14. s. Dostupné z: http://sciforum.net/conference/70/paper/2886

THE ECONOMIST. 2015. Gooing Dark. *The Economist*. **2015**(3): 11–12.

UN DEVELOPMENT PROGRAMME. 2014. *Leading the Way in Early Warning* [online]. [cit. 2016-09-04]. Dostupné z: https://reliefweb.int/report/world/leading-way-early-warning

UNEP. 2012. *Early Warning Systems: A State of the Art Analysis and Future Directions*. Division of Early Warning and Assessment (DEWA). United Nations Environment Programme (UNEP), Nairobi.

VENESS, Chris. 2017. *Movable Type Scripts. Calculate distance, bearing and more between Latitude/Longitude points* [online]. [cit. 2017-11-25]. Dostupné z: http://www.movable-type.co.uk/scripts/latlong.html

VEVERKA, Ivan. 2003. *Vybrané kapitoly krizového řízení pro záchranářství*. Praha: Vydavatelství PA ČR. ISBN 978-80-7251-126-6.

VIJAY, More a Uma R. GODASE. 2014. Implementation of Location based Encryption in GSM Cellular Network using OPNET. *International Journal of Science and Research (IJSR)*. **3**(7): 1360–1367. ISSN 2319-7064. Dostupné také z: http://www.ijsr.net/archive/v3i7/MDIwMTQxMjcxMQ%3D%3D.pdf

VINCENTY, Thaddeus. 1975. Direct and inverse solutions of geodesics on the ellipsoid with application of nested equations. *Survey Review*. **22**(176): 88–93 [cit 2017-11-05]. Dostupné z: https://www.ngs.noaa.gov/PUBS_LIB/inverse.pdf

VOJTEK, Petr. 2017. *Náhrada škody a nemajetkové újmy ve zdravotnictví* [online]. [cit. 2018-03-04]. Dostupné z: http://konference.klub-personalistu.cz/files/59d23ab427983-Vojtek-Zdravotnictvi.pdf

WRÓBLEWSKI, Piotr. 2015. *Algoritmy*. Brno: Computer Press. ISBN 978-80-251-4126-7.

ZAORALOVÁ, Nicole. 2017. *Systém eCall byl spuštěn, tísňová linka zvládne přijmout automatický hovor z havarovaného vozidla* [online]. [cit. 2017-11-28]. Dostupné z: https://www.pozary.cz/clanek/175120-system-ecall-byl-spusten-tisnova-linka-zvladne-prijmout-automaticky-hovor-z-havarovaneho-vozidla/

ŽID, Norbert, Jiří SVOBODA et al. 1998. Orientace ve světě informatiky. Praha: Management Press. ISBN 80-85943-58-1.

ŽIŽKA, Tomáš a Jan SKRBEK. 2015a. Model Scenarios for Effective Distribution of Information During Crisis Situations. In: *Innovation Management and Sustainable Economic Competitive Advantage: From Regional Development to Global Growth - Proceedings of the 26th International Business Information Management Association Conference*. Madrid: International Business Information Management Association, s. 2340–2346. ISBN 978-0-9860419-5-2.

ŽIŽKA, Tomáš, Jan SKRBEK a Tereza SEMERÁDOVÁ. 2015b. New Aspects of Positionaly Encrypted Forced Broadcasting in Special Emergency Situations. In: *IDIMT 2015: Information Technology and Society - Interaction and Interdependence - 23rd Interdisciplinary Information Management Talks*. Linz, Österreich: Johannes Kepler Universitat Linz, s. 53–61. ISBN 9783990333952.

Zákony

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

Zákon č. 273/2008 Sb., Zákon o Policii České republiky

Přehled publikační činnosti autora

ŽIŽKA, Tomáš. 2017. Using Symmetric Cryptography for Evacuation Control During Naturogenic Emergencies. In: *Liberec Economic Forum 2017.* Liberec: Technical University of Liberec, s. 547–554. ISBN 978-80-7494-349-2.

PODARAS, Athanasios a Tomáš ŽIŽKA. 2017. Requirement Analysis of Agile Information Systems and Business Processes: an Agricultural Case Study. In: *Scientific Papers of University of Pardubice*. Pardubice: University of Pardubice, Faculty of Economics and Administration. **24**(3): 110–122. ISSN 1211-555X.

PODARAS, Athanasios, Dana NEJEDLOVÁ a Tomáš ŽIŽKA. 2017. Analyzing Business Process Requirements for a Software Based Execution of Business Continuity Tasks. In: *Liberec Economic Forum 2017*. Liberec: Technical University of Liberec, s. 372–380. ISBN 978-80-7494-349-2.

ŽIŽKA, Tomáš a David KUBÁT. 2016. Early warning information spread with the aspect of exclusivity during emergency events. In: *Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth.* Seville, Spain: International Business Information Management Association, s. 1675–1681. ISBN 978-0-9860419-8-3.

PODARAS, Athanasios a Tomáš ŽIŽKA. 2016. *Business Continuity Points Software (Version 1)* [software]. Dostupné z: https://multiedu.tul.cz/index.php?content=multi_uziv&ident=166

KUBÁT, David a Tomáš Žižka. 2016. Early warning in traffic: Current and novel approaches and methods. In: *Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth* Seville, Spain: International Business Information Management Association, s. 1682–1687. ISBN 978-0-9860419-8-3.

ŽIŽKA, Tomáš a Jan SKRBEK. 2015. Model Scenarios for Effective Distribution of Information During Crisis Situations. In: *Innovation Management and Sustainable Economic Competitive Advantage: From Regional Development to Global Growth - Proceedings of the 26th International Business Information Management Association Conference*. Madrid: International Business Information Management Association, s. 2340–2346. ISBN 978-0-9860419-5-2.

ŽIŽKA, Tomáš, Jan SKRBEK a Tereza SEMERÁDOVÁ. 2015. New Aspects of Positionaly Encrypted Forced Broadcasting in Special Emergency Situations. In: *IDIMT 2015: Information Technology and Society - Interaction and Interdependence - 23rd Interdisciplinary Information Management Talks*. Linz, Österreich: Johannes Kepler Universitat Linz, s. 53–61. ISBN 9783990333952.

ŽIŽKA, Tomáš, Aleš KOCOUREK a Jana ŠIMANOVÁ. 2015. *Strukturovaná výpočtová databáze regionálních cenových indexů pro měření regionálních cenových hladin v členění dle CZ-COICOP* [software]. Dostupné z: http://vyzkum.ef.tul.cz/td020047/index.php?content=databaze

ŽIŽKA, Tomáš. 2014. The Use of Cryptography for Distribution of Information During Crisis Situations. In: *IDIMT 2014: Networking Societies – Cooperation and Conflict, 21nd Interdisciplinary Information Management Talks*. Linz: Johannes Kepler Universität, s. 45–52. ISBN 9783990333402.

ŽIŽKA, Tomáš. a Athanasios PODARAS. 2014. Effective Dissemination of Emergency Information. In: *IBIMA 2014: Crafting Global Competitive Economies: 2020 Vision Strategic Planning & Smart Implementation - Proceedings of the 24th International Business Information Management Association Conference*. Milano: International Business Information Management Association (IBIMA), s. 1697–1705. ISBN 978-0-9860419-3-8.

ŽIŽKA, Tomáš. 2014. Possibilities of Information Distribution During Emergencies and Crisis Situations. In: *Quaere 2014 vol. IV - Reviewed Proceedings of the Interdisciplinary Scientific International Conference for PhD students and assistants*. Hradec Králové: Magnanimitas, s. 1288–1295. ISBN 9788087952047.

ŽIŽKA, Tomáš a David KUBÁT. 2014. Šíření varovných zpráv s využitím šifrování. In: *IMEA 2014 – 14. mezinárodní konference pro doktorandy a vědecké pracovníky se zaměřením na informatiku, management, ekonomii a veřejnou zprávu*. Liberec: Technická univerzita v Liberci, s. 264–270. ISBN 9788074941061.

PODARAS, Athanasios, Jan MRÁZEK a Tomáš ŽIŽKA. 2014. A Risk Analysis Method For The Determination Of The Extended Acceptable Timeframe Of Interruption In An Enterprises' Information System. In: *System Approaches '14, Systems Thinking And Global Problems Of The World, 20th International Conference*. Praha: University Of Economics, Prague, Publishing Oeconomica, s. 60–67. ISBN 978- 80-245-2074-2.

ŽIŽKA, Tomáš a Jan SKRBEK. 2013. Contribution to System Appcontribution to System Approach to Notification and Information of Civilians in Emergencies, Disasters and Crisess. In: *System approaches & Systems thinking and global problems of the world*. Praha: Vysoká škola ekonomická v Praze, s. 75–81. ISBN 978-80-245-1982-1.

ŽIŽKA, Tomáš a Athanasios PODARAS. 2013. Positionally Exclusive Broadcasting. In: *Proceedings of AMBIENT 2013 - The Third International Conference on Ambient Computing, Applications, Services and Technologies*. Porto: International Academy, Research, and Industry Association, s. 68–73. ISBN 978-1-61208-309-4.

PODARAS, Athanasios a Tomáš ŽIŽKA. 2013. Criticality Estimation of It Business Functions with the Business Continuity Testing Points Method for Implementing Effective Recovery Exercises of Crisis Scenarios. In: *International Journal of Computer Science Issues*. 4. vyd. Mahebourg: International Journal of Computer Science Issues. (4): 248–256. ISSN 1694-0784.

ŽIŽKA, Tomáš, Jan SKRBEK, et al. 2012. Ambient Traffic Services Based on the use of Agile Warning and Notification System Radio-Help. In: *AMBIENT 2012 - The Second International Conference on Ambient Computing, Applications, Services and Technologies*. Barcelona: International Academy, Research, and Industry Association, s. 7–11. ISBN 9781612082356.

SKRBEK, Jan, David KUBÁT, Jiří KVÍZ a Tomáš Žižka. 2012. Distributing Emergency Traffic Information. In: *IDIMT 2012 - ICT Support for Complex Systems*. Linz: Johannes Kepler Universität, s. 33–39. ISBN 9783990330227.

Příloha A: Substituční tabulka S-Box pro operaci SubBytes

		y															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
x	**0**	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16