TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

CÍLENÁ DISTRIBUCE INFORMACÍ

Autoreferát disertační práce

Studijní program: P6209 – Systémové inženýrství a informatika

Studiní obor: 6209V003 – Ekonomická informatika

Autor práce: **Mgr. Tomáš Žižka**

Školitel: doc. Ing. Jan Skrbek, Dr.

Disertační práce byla vypracována v kombinované formě doktorského studia na katedře informatiky Ekonomické fakulty Technické univerzity v Liberci.

Uchazeč: Mgr. Tomáš Žižka
Ekonomická fakulta Technické univerzity v Liberci
Katedra informatiky
Voroněžská 13
461 17 Liberec 1

Školitel: doc. Ing. Jan Skrbek, Dr.
Ekonomická fakulta Technické univerzity v Liberci
Katedra informatiky
Voroněžská 13
461 17 Liberec 1

Autoreferát byl rozeslán dne:

Obhajoba disertační práce se koná dne 17. 5. 2018 před komisí na Ekonomické fakultě Technické univerzity v Liberci, Voroněžská 13, Liberec 1 v zasedací místnosti děkanátu Ekonomické fakulty.

S disertační prací je možno se seznámit na katedře informatiky Ekonomické fakulty Technické univerzity v Liberci.

doc. Ing. Jan Skrbek, Dr.
předseda oborové rady
DSP Ekonomická informatika

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.

Obsah

Seznam zkratek

AES	*Advanced Encryption Standard*
DAB	*Digital Audio Broadcasting*
GPS	*Global Positioning System*
GSM	Globální systém pro mobilní komunikaci
HZS ČR	Hasičský záchranný sbor České republiky
IZS	Integrovaný záchranný systém
JSVV	Jednotný systém varování a vyrozumění obyvatelstva
MU	Mimořádná událost
MVČR	Ministerstvo vnitra České republiky
NIST	*National Institute of Standards and Technology* (Americký Národní institut standardu a technologií)
RH	Radio-Help
SVV	Systém včasného varování

Seznam obrázků

Seznam tabulek

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 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 této kapitole 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.

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).

Mimořádná událost

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.

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
- biotické mimořádné události – jsou způsobené živou přírodou

Antropogenní mimořádné události dále dělíme na:

- technogenní mimořádné události – provozní havárie a havárie spojené s infrastrukturou
- sociogenní mimořádné události interní – vnitrostátní společenské, sociální a ekonomické krize
- sociogenní mimořádné události externí – vojenské krizové situace
- agrogenní mimořádné události – spojené se zemědělstvím a půdou

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.

2.1.3 Krizová komunikace

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

2.2.1 Jednotný systém varování a vyrozumění (JSVV)

Bezprostřední varování obyvatelstva zabezpečují koncové prvky, kterými jsou zejména poplachové sirény a obecní rozhlasy dálkově ovládané připojením k JSVV.

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.

2.2.3 Systém eCall

Systému eCall (emergency call) je „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.

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

2.2.4 KATWARN

KATWARN je německý varovný a informační systém, který se začal v praxi testovat v roce 2011. Komunikačním kanály tohoto systému jsou SMS zprávy, mobilní aplikace nitifikačního charakteru a sociální sítě.

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)

3 Požadavky na efektivní systém včasného varování

3.1 Kritické zhodnocení stávajících systémů

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

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.

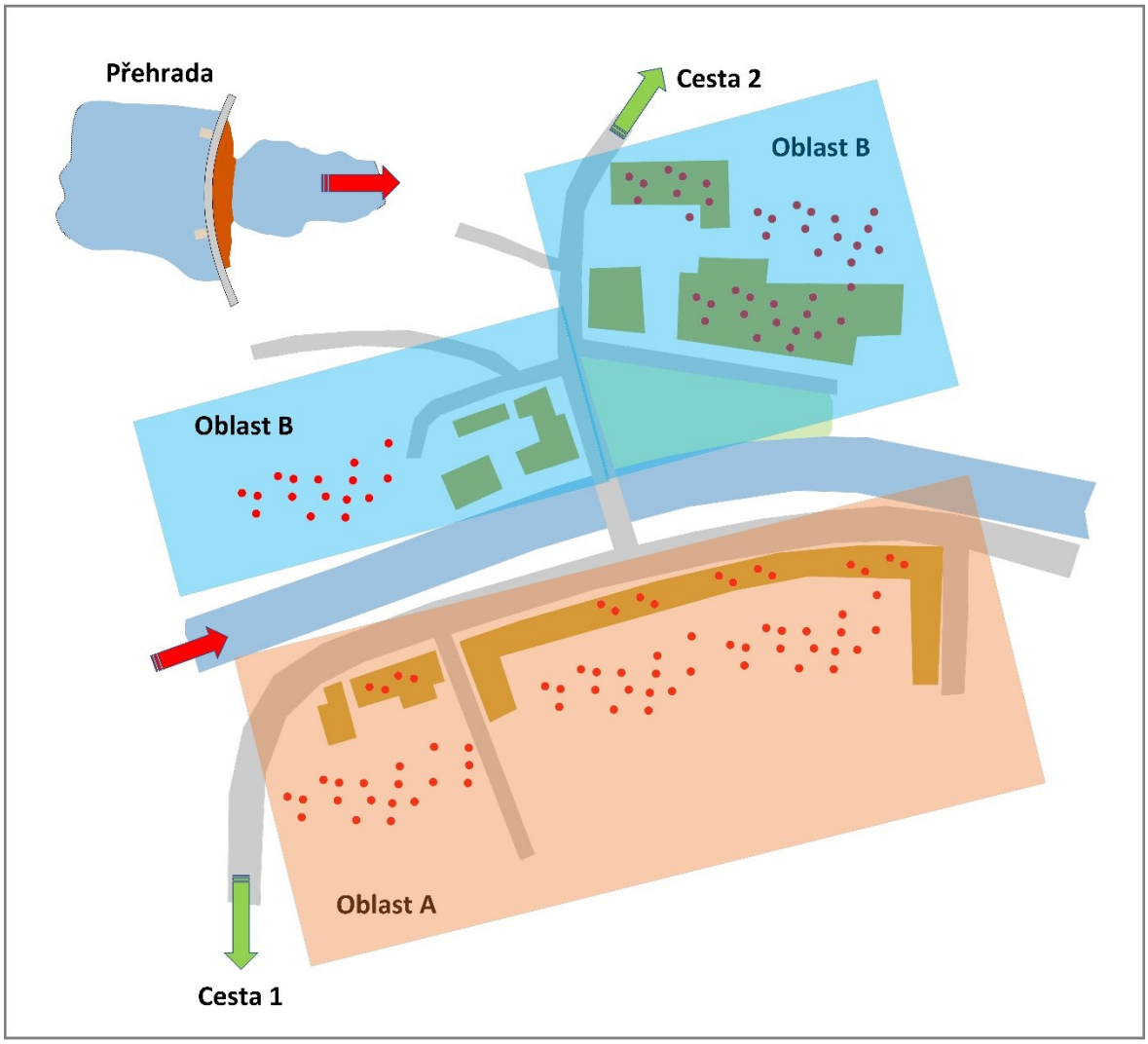
3.3 Radio-Help

Základem systému, který by zajistil exkluzivitu zprávy pro předem vymezené místo, by mohl být systém Radio-Help (Skrbek, 2010), jenž je navržen primárně pro adresné 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.

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.

4 Modelové situace

Modelová situace – ohrožení vzniklé poškozením vodního díla



Obrázek 1: Modelová situace

Zdroj: vlastní zpracování

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,

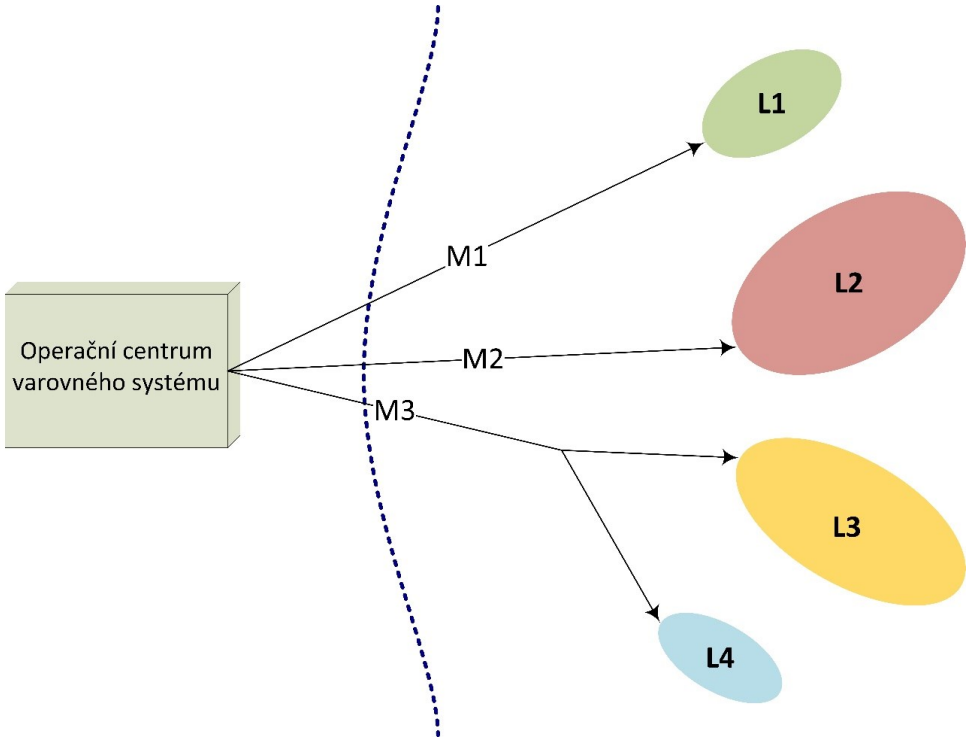
například v důsledku vyhlášení mimořádné situace běžnými prostředky JSVV nebo prostřednictvím médií, nemusela by být ani tato doba dostatečná.

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.

5 Poziční šifrování

5.1 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.



Obrázek 2: Základní koncepce pozičního šifrování
Zdroj: vlastní zpracování

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 2. 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

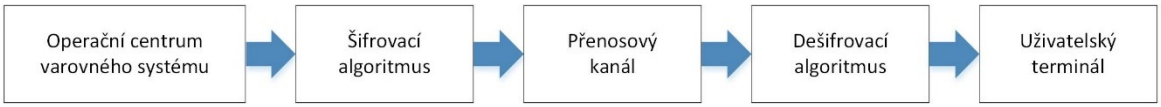
zajištěna exkluzivita zpráv v jednotlivých oblastech. To znamená, že zpráva M1 může být úspěšně dešifrována pouze v oblasti L1, zpráva M2 pouze v oblasti L2, zpráva M3 v oblastech L3 a L4 – stejnou zprávu lze ve stejný časový okamžik odeslat i do oblastí, které spolu přímo nesousedí.

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.

Jeden z prvních algoritmů pozičního šifrování publikovaný v roce 2003 pod názvem Geo-Encryption (Scott & Denning) vychází z hybridního principu kryptografie.

5.2 Aspekty systému pro pozičně šifrované vysílání informací

Systém pro poziční šifrované vysílání je zamýšlen jako rozšíření koncepce systému Radio-Help. 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 3.



Obrázek 3: Základní části systému pro pozičně šifrované vysílání informací
Zdroj: vlastní zpracování

5.2.1 Přenosový kanál

Mezi uvažované přenosové kanály pro systém cílené distribuce informací s funkcí pozičního šifrování patří HD Radio, DAB+, GSM sítě a Internet. 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.

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 1 je uvedeno shrnutí předností a nedostatků platformy DAB+ z pohledu systému pro poziční šifrované vysílání varovných informací.

Tabulka 1: 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

5.2.2 Šifrovací algoritmus

Princip pozičního šifrování navržený Scottem et al. v roce 2003, který využívá principu hybridního šifrování, 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.

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).

Následující tabulka 2 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 2: 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 Návrh konceptuálního řešení

6.1 Vymezení oblasti pro příjem dešifrované varovné zprávy

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

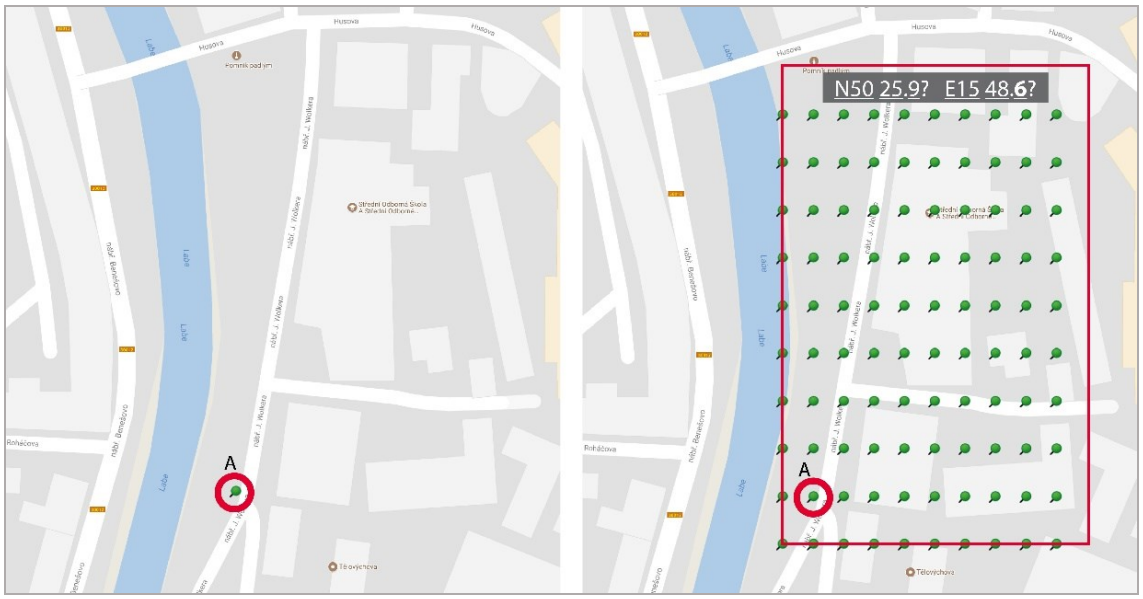
Základem pro vymezení oblasti dále navrhovaným způsobem je generování množiny bodů (matice/síť 10 x 10 bodů), která bude tvarem odpovídat pravoúhlému polygonu. Na tuto množinu je kladen požadavek, aby body, které budou tvořit vymezenou oblast (hraniční i vnitřní), měly nějakou **společnou vlastnost**, 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 3. 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).

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.

Tabulka 3: 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



Obrázek 4: 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.

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 4 je vyznačena červeným obdélníkem. Z obrázku je nyní zřejmá hledaná společná vlastnost bodů, která je důležitá pro vytvoření šifrovacího klíče. Všechny body zobrazené na obrázku 4 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 algoritmu 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?'.

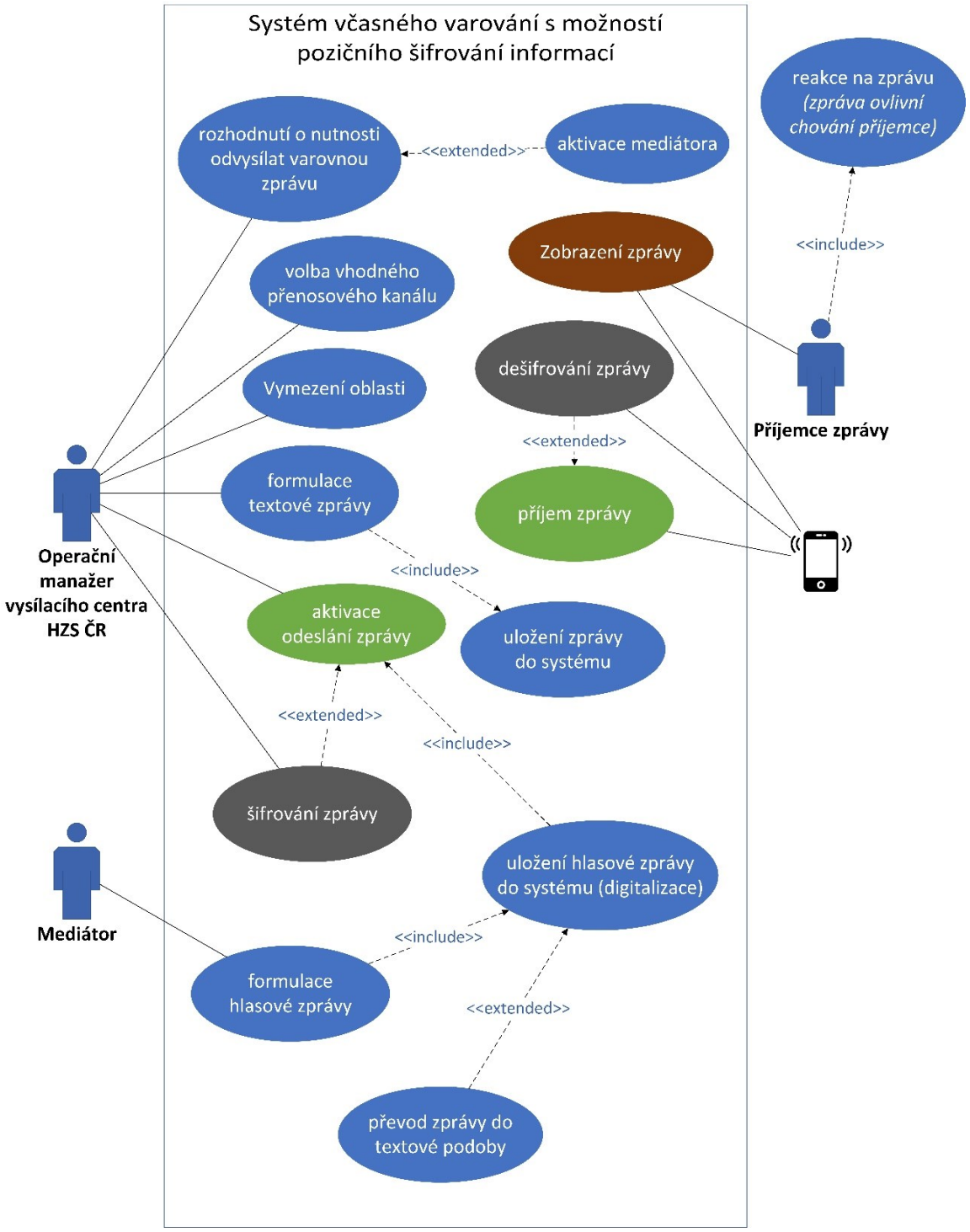
Předpokladem je, že by celý proces fungoval automaticky. To znamená, že operační manažer si na dotykové obrazovce pomocí „mapové“ aplikace vymezí body, které budou tvořit oblast pro příjem varovné zprávy. Následně aplikace na pozadí vytvoří dostatečný počet čtyřúhelníků pro pokrytí vymezené oblasti a 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.

6.2 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.

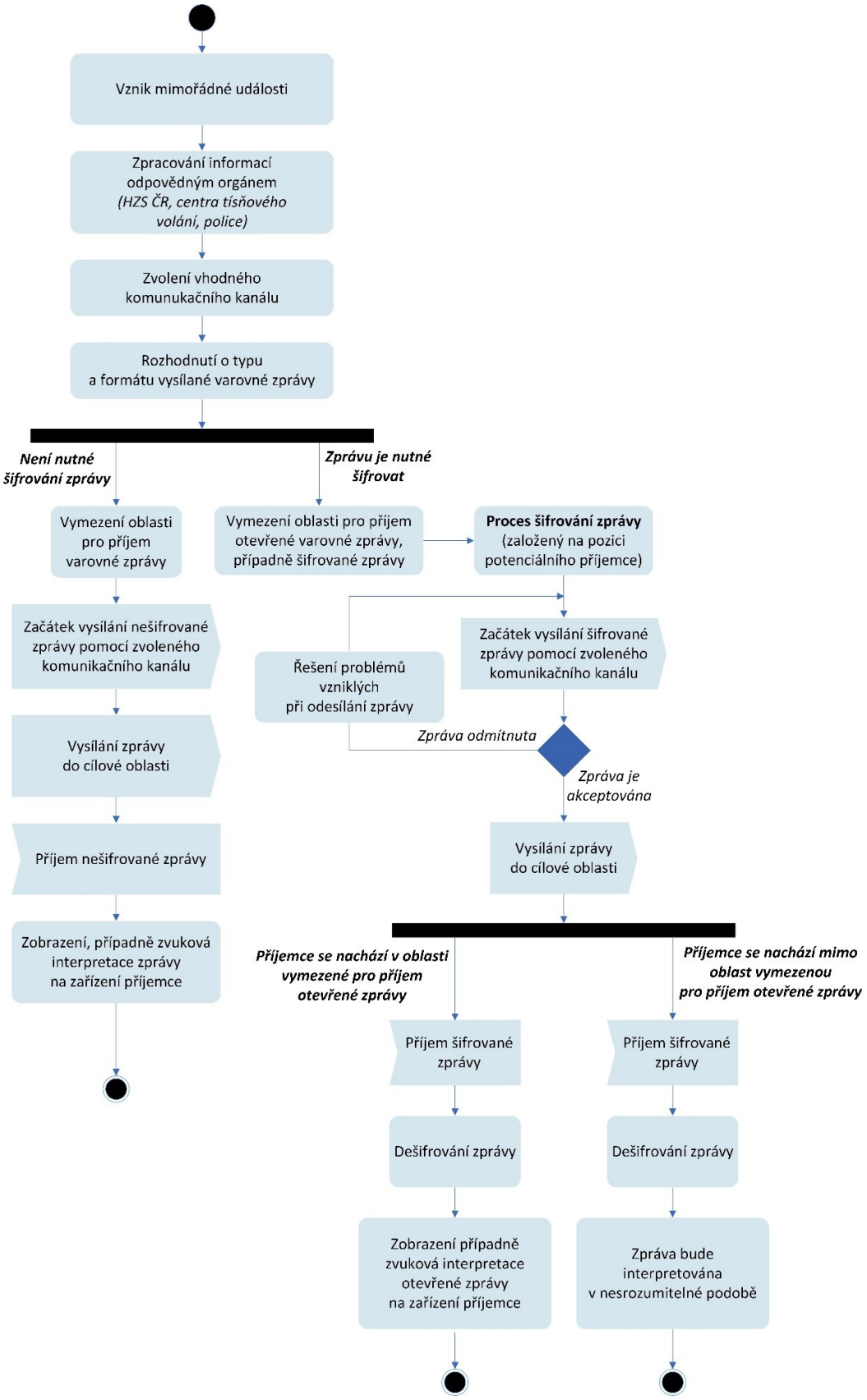
Diagram na obrázku 5 navazuje na harmonické začlenění systému Radio-Help do struktury IZS ČR, jehož garantem a základní součástí je HZS ČR. Hlavní úlohu na straně distributora informace má **operační manažer vysílacího centra HZS ČR** (reálně se bude jednat spíše o tým), který rozhoduje na základě vstupních 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 6.1. Druhým UML diagramem (obrázek 6), který je použit pro znázornění procesní logiky systému včasného varování s funkcí pozičního šifrování, je diagram aktivit (Activity diagram).



Obrázek 5: Use case diagram

Zdroj: Vlastní zpracování



Obrázek 6: UML diagram aktivit – procesní logika systému

Zdroj: vlastní zpracování

7 Ekonomicko-implementační hledisko

7.1 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, 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.

7.2 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. 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 5.2.2.

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 6.1 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. 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

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

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

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

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

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

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

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

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

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.

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

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

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

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.