В подальшому розвитку мережевих технологій, система IP-геолокації не втратить свою актуальність, і буде використовуватися в такому ж ключі і далі, але при цьому система не позбавиться своїх мінусів. Як варіант вирішення одного з недоліків є блокування проксі-серверів і анонімайзерів, але це призведе до зниження рівня анонімності користувачів.

Список літератури

1. . Коростелёва Н.И. Самоорганизующаяся информационно-поисковая система для предоставления логистических услуг под названием «Cloud Logistics» // II Международная научно-практическая конференция «Инновационные технологии организации и управления наукоемким производством». М.: МГТУ им. Н. Э. Баумана, 2011. С. 70-85.

2. Топ-10 API картографических сервисов. Режим доступа: http://habrahabr.ru/company/what3words/blog/252311/

3. Документация Google API Режим доступа: https://developers.google.com/maps/?hl=ru

Лохвінський В.С., Рябуха. О.М.
ОНАЗ ім. О.С. Попова

ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ ГЛОБАЛЬНОГО ПОЗИЦІОНУВАННЯ GPS ТА GSM З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті розглядаються сучасні системи геолокації. Дається коротка історична пам'ятка про становлення геолокації. Описуються основні принципи праці цих систем. Окремо виділяються переваги і недоліки, які так чи інакше впливають на якість отримання геолокаційних даних за допомогою сучасних технологічних засобів, таких як: супутники та базові станції мобільного оператора. Розглядаються основні алгоритми шифрування для забезпечення захисту інформації, котра передається за допомогою цих систем.

З розвитком космічних і наземних систем зв'язку людям стало доступно глобальне географічне позиціонування – геолокація. Розвиток геолокації почався ще в 50-ті роки минулого століття, але перші результати були отримані тільки на початку 70-х років. Перша назва системи – NAVSTAR. Надалі систему перейменували у Global Positioning System – система глобального позиціонування (GPS).

Сьогодні геолокація – це процес спостереження за цілісністю об'єктів, без якого не може обійтись жодна державна структура або комерційна організація. Основними системами геолокації виступають GPS і Wi-Fi-мережі. На ряду з усталеними системами обчислення позиційних даних все частіше і частіше використовують комерційну систему Global System for Mobile Communications – глобальна система мобільного зв'язку (GSM).

Основою системи GPS є три сегменти: космічний, наземний і призначений для користувача. Космічний сегмент складається з 30-ти автономних супутників, рівномірно розподілених по орбітах з висотою 20 350 км (для повноцінної функціональної роботи системи досить 24 супутника, інші 6 супутників є резервними і використовуються для оповіщення про надзвичайні ситуації, а також при необхідності коригують точність системи, зменшуючи похибку). Перебуваючи на орбіті, супутники випромінюють за двома частотами спеціальний навігаційний сигнал, в якому міститься два види зашифрованих кодів, один із яких доступний тільки військовим і федеральним службам США. Кожен супутник випромінює ще й третій сигнал, який інформує користувача про додаткові параметри: працездатність супутників, їх стан та ін.

Орбіта супутників періодично контролюється мережею наземних станцій спостереження. За допомогою цих станцій обчислюються балістичні характеристики, реєструються відхилення супутників від розрахункових траєкторій руху, визначається їх бортовий час, здійснюється моніторинг навігаційної апаратури та ін. Зібрану інформацію

обробляють суперкомп'ютери і періодично передають на супутники для корекції орбіт і оновлення навігаційних даних.

В GPS одним з найбільших недоліків системи є те, що при певних умовах сигнал, що виходить від супутника, може не доходити до приймача або доходити, але зі значними спотвореннями або затримками. Наприклад, GPS система абсолютно марна в глибині квартири, всередині залізобетонного будівлі, навіть при використанні професійних геодезичних приймачів в підвалі або в тунелі. Так як робоча частота лежить в дециметровому діапазоні радіохвиль, то це призводить до того, що рівень сигналу супутника може серйозно знизитися під щільністю листя дерев або через дуже велику хмарність. Так само на прийом сигналу впливають наземні джерела радіосигналу і, в рідкісних випадках, магнітні бурі.

Ще один важливий недолік: невисокий нахил орбіти супутників – близько 55°, що серйозно погіршує точність в приполярних районах Землі.

Так само важливим є те, що GPS реалізована і експлуатується Міністерством оборони США. Таким чином отримання сигналу користувачем GPS безпосередньо залежить від США.

До переваг даної системи можна зарахувати незначну похибку – близько 15-20 метрів.

Що стосується захисту сигналу, котрий проходить через супутники, то тут все дуже двояко, тому що основні алгоритми шифрування і розшифрування сигналу відомі тільки військовим США. У відкритому доступі існує інформація тільки про те, що у 2000 році для комерційного та побутового користувача був відключений виборчий доступ (S/A), у якому використовується C/A-код, у зв’язку с цим алгоритм модернізували.

Із доступних даних відомо, що передача сигналу здійснюється таким чином: P-код шифрується кодовими даними (A-S) в результаті чого виходить сигнал, що має назву «Y-код», який можуть розшифрувати тільки армійські GPS приймачі.

Перехід на Anti-Spoofing (A-S) був навмисним. Мета цього переходу – перешкоджати доступ до P-кодової частини сигналу GPS цивільним особам і ворогові. При спробі впровадження в захищений канал зв'язку обладнання перейде в режим використання C/A-коду, який використовується тільки в S/A доступі. Ця інформація стосується лиже захищеного каналу зв’язку, де використовується шифрування.

У свою чергу GSM система використовує тільки наземний сегмент стільникового зв'язку – базові станції. Відбувається це таким чином: мобільний пристрій здійснює пошук найближчої базової станції, сканує ефір на наявність вільних сот, причому, кожна сота має свій унікальний номер (CellID). З числа знайдених базових станцій визначаються шість, які задовольняють вимогам енергетичних витрат і якості сигналу, але мобільний пристрій працюватиме в один момент часу тільки з однією стацією.

Для ідентифікації базових станцій їх об'єднують в групи і присвоюють унікальний ідентифікатор (LAC). Як правило, приналежність до групи визначають за місцем положення базових станцій.

При взаємодії цих двох параметрів LAC і CellID, які виступають в ролі унікальних ідентифікаторів базової станції, на якій зареєстровано і працює мобільний пристрій, центром комунікації визначається вірний напрямок для відправки даних. В іншому випадку, пристрій доводилося б шукати серед тисячі базових станцій.

Крім параметрів LAC і CellID використовується ще один параметр – Timing Advance (лімітована затримка сигналу). Він визначає сектор базової станції і фіксує час прийому і передачі сигналу, що дозволяє визначити відстань від базової станції до пристрою.

Дані, що визначають місце розташування мобільного пристрою, оновлюються з певною періодичністю, а в разі переміщення пристрою – при кожному перемиканні між базовими станціями.

Основними критеріями роботи геолокаційних сервісів в системі GSM є: точність визначення координат і частота їх поновлення. Для зменшення похибки визначення координат знаходження потрібного пристрою в системі визначається тріангуляцією, в якій

застосовують симплекс між декількома базовими станціями, що дозволяє не обмежуватися тільки дальністю до них.

В системі GSM основним недоліком є відстань передачі сигналу між базовою станцією і пристроєм. Відстань не перевищує 120 км.

Ще одним недоліком є похибка у визначенні координат. Похибка змінюється в залежності від кількості базових станцій в місці знаходження пристрою. Наприклад, в містах, де щільність покриття мережі максимально допустима, рівень похибки може досягати не більше 100-200 м, але, опинившись за межею міських базових станцій, похибка зростатиме і буде в діапазоні 100-500 м.

До переваг можна віднести досить низький рівень впливу перешкод на дану систему, і можливість проходження сигналу крізь будь-які об'єкти. Також одним з важливих факторів є те, що ця система широко використовується по всьому світі як мобільний зв'язок.

Для шифрування сигналу в GSM використовується алгоритм із сімейства A5, котрий має чотири ітерації:

– A5/0 – алгоритм в якому відсутнє шифрування;

– A5/1 – поточний шифр, котрий найбільш розповсюджений;

– A5/2 – аналог A5/1, але дешевший і порівняно з іншими версіями даного шифру має меншу криптостійкість. Ринок збуту – країни, які не входили ЄС. В даний час не використовується;

– A5/3 – блочний шифр. Розроблений у 2001 році з цілю посунути застарілий алгоритм A5/1 у третьому поколінні мобільних систем. Цей алгоритм має іншу назву – Касуми. За основу при створені був взятий шифр MISTY, котрий є власністю корпорації Mitshubishi. В даний час алгоритм має найвищий рівень криптостійкості, але поки що використовують тільки передові фірми починаючи з в мережі 3GPP.

Стосовно вразливостей алгоритму шифрування A5: його рівень криптостійкості дуже високий, але для спрощення доступу до інформації, котра знаходиться в захищеному каналі, розробники алгоритму шифрування, навмисно послабили алгоритм доступу для спецслужб.

Отже, порівнюючи вище зазначені системи, можна сказати, що система GPS дуже вибаглива до місця знаходження розшукуваного об'єкту і вельми дорога в розгортанні і обслуговуванні, але при цьому покриває величезні площі, а також не має відкритого доступу до алгоритму шифрування і ставить під сумнів цілісність і достовірність інформації, котра передається через систему GPS.

В свою чергу GSM не вимагає великих капіталовкладень в розгортанні і обслуговуванні, але радіус покриття, в основному, залежить від кількості базових станцій. Ця система дає змогу використовувати спеціально розроблений алгоритм шифрування, який має відкритий доступ для ознайомлення з ним.

Сьогодні велика кількість компаній почала проектувати своє обладнання для геолокації під режим Real Time Kinematic – кінематика реального часу (RTK). Цей режим дає змогу зменшити час старту системи опитування геолокаційного обладнання, а також робить похибку незначною, приблизно 1-2 см по широті та 2-3 см по довготі. Виходячи з цього можна припустити, що система GSM має велике майбутнє в геолокації.

Список літератури

1. Яценков В.С. Основы спутниковой навигации. Системы GPS NAVSTAR и Глонасс – М.: Горячая линия-Телеком, 2005. – 272 с.

2. Соловьев Ю.А. Системы спутниковой навигации – М.: Эко-Трендз, 2000. – 270 с

3. Попов В.И. Основы сотовой связи стандарта GSM – М.: Эко-Трендз, 2005. – 296 с

4. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации. – 4-е изд., перераб. и доп. – Санкт-Петербург: Питер, 2011. – 560 с.