НЯКОИ АСПЕКТИ НА СИГУРНОСТТА ПРИ МОБИЛНИ AD HOC МРЕЖИ

Желязко Николов, Росен Спиров, Любомир Алексиев

Abstract: *Security has become a major concern in order to provide protected communication between mobile nodes in a hostile environment. In comparison with the traditional wire nets, the characteristics of mobile ad hoc networks pose a number of challenges to the security model, such as shared wireless medium and highly dynamic network topology. In this article some aspects of information security and routing in mobile ad hoc networks are overviewed.*

Keywords: *Mobile ad hoc networks, information security, routing.*

1. Въведение.

Безжичните мобилни мрежи, които работят без централизиран контрол и стационарна инфраструктура са известни като ad hoc мрежи. Първоначално те са използвани единствено за военни цели, но днес се развиват и осигуряват както държавни структури и служби, така и широк кръг комерсиални приложения. Това развитие служи като катализатор за намиране на похвати за компрометиране на сигурността на мрежовия информационен обмен, особено във военната сфера.

Известно е, че мобилните ad hoc мрежи се отличават със сравнително висока устойчивост на преднамерени смущения, която се дължи основно на използваните широколентови сигнали. В съвременните условия при налагането на мрежовоцентричен модел за водене на военни операции, разглежданите мрежи имат водеща роля при комуникационно-информационната поддръжка на тактически действия. В тези случаи противодействието на мобилните ad hoc мрежи се извършва не само чрез използване на предаватели на преднамерени смущения, но и чрез създаване на условия за нарушаване на информационната сигурност. В настоящия доклад са разгледани някои аспекти на сигурността по отношение на информациония обмен и маршрутизиращите протоколи.

2. Основни компоненти на информационната сигурност при мобилни ad hoc мрежи.

Осигуряването на информационната сигурност при съвременните комуникационно-информационни системи, и в частност при мобилните ad hoc мрежи, може да бъде разглеждано като изпълнение на комплекс от мероприятия насочени към удовлетворяване на изискванията за: **достъпност, цялостност, автентификация, конфиденциалност и невъзможност за отказ** [1, 4, 5, 6].

Достъпността на една комуникационно-информационна мрежа гарантира нейната наличност и факта, че тя може да бъде използвана при поискване от оторизиран потребител. Достъпността се осигурява чрез контрол на потребителите, резервиране на записи и архивиране на информация.

Цялостността гарантира, че информацията не е била променена или унищожена по неоторизиран начин. Тя се постига чрез недопускане на изменение на информацията както по злонамерен начин, така и при използване на информация от ненадежден източник. Рискът от недостатъчна цялостност се минимизира чрез използване на надеждни източници на информация и цифрови подписи.

Чрез **автентификацията** се установява валидността на съобщение или източник, както и правото на потребителя за получаване на специфични категории информация. Автентификацията се гарантира чрез използване на персонални атрибути за сигурност, асиметрично криптиране и цифрови подписи. Тя гарантира, че източниците на информация се проверяват за валидност при получаване на информацията или при първоначален достъп до нея.

Афтентификацията е от особена важност за установяването на източника на нова или променена маршрутизираща информация при ad hoc мрежите. Ако този компонент на сигурността не е гарантиран, е възможно да се допусне нарушаване на маршрутизацията или отклоняване на трафика в произволни направления. Това би довело до невъзможност за комуникация. Афтентификацията и цялостността обикновено се осигуряват паралелно, тъй-като цифровите подписи се прилагат както за потвърждаване на произхода на информацията, така и за недопускане на изменение по неоторизиран начин. При неадекватна защита на цялостността е възможно да се допусне злонамерено унищожаване на съобщения или да се генерира лъжлив трафик, като тези действия може да бъдат приети за грешки при обмена.

Конфиденциалността гарантира, че информацията е защитена по начин, който позволява достъп до нея само на оторизирани потребители. Конфиденциалността се постига чрез прилагане на процедури за сигурност и криптиране.

Нарушаването на конфиденциалността на маршрутизиращата информация при разглежданите комуникационни структури може да даде възможност на неоторизиран потребител да установи местоположението на устройствата и да ги разпознава. Подобен пробив повишава уязвимостта на мрежата, като създава условия и за други действия за нарушаване на сигурността.

Невъзможността за отказ гарантира, че подателят на информацията разполага с доказателство за доставката ѝ, а получателят е уверен в идентичността на подателя. По този начин и двете страни не могат да отрекат, че са обработвали данните. При обмен на съобщения в системата се генерират съответните записи.

3. Действия за компрометиране на сигурността на мобилни ad hoc мрежи и механизми за защита.

Съществуват две основни направления за защитата от действия за компрометиране на информационната сигурност [5]:

- превантивна дейност - прилагане на механизми за защита от компрометиращо действие;
- установяване на компрометиращото действие и предприемане на мерки за неговото неутрализиране.

От своя страна действията за компрометиране на сигурността на мобилни ad hoc мрежи могат да бъдат разделени в две категории: пасивни и активни [2].

При пасивните действия извлечената информация се употребява, без да бъде променяна и въвеждана отново в мрежовия трафик. В този случай се нарушава конфиденциалността. Поради факта, че тези действия не водят до прекъсване на комуникацията, те се установяват сравнително трудно. Противодействието се осигурява посредством подходящо криптиране и контрол на достъпа.

Активните действия водят до нарушаване на нормалната работа на ad hoc мрежата. При тях се извършва злонамерено модифициране на информацията или въвеждане на грешни данни. Резултатът може да бъде нарушаване на маршрутизиращите процедури и понижаване на производителността на мрежата. Активните действия за компрометиране на информационната сигурност могат да бъдат разделени на външни и вътрешни.

Външните активни действия се извършват с помощта на устройства, които не са легитимна част от ad hoc мрежата. Адекватно противодействие може да бъде осигурено при използването на процедури за автентификация.

Вътрешните активни действия за компрометиране на сигурността се

осъществяват чрез вече оторизирани устройства, част от мрежата. По тази причина тези действия са сравнително трудни за откриване.

Два от ключовите механизми за защита на мобилните ad hoc мрежи от действия за компрометиране на сигурността са криптиране на съобщенията и използване на специални кодове за удостоверяване на идентичността на подателя. Те осигуряват цялостност на информацията и автентификация.

При мобилните ad hoc мрежи се използват основно два начина за криптиране на данни – симетрично и асиметрично. Системите със симетрично криптиране използват един ключ за криптиране и декриптиране на съобщенията, докато асиметричните – по един за всяко действие. Във втория случай рискът от компрометиране на сигурността на информацията е по-нисък и по тази причина асиметричното криптиране намира приложение при мобилните ad hoc мрежи с военно предназначение.

По отношение на кодовете за удостоверяване на идентичността на подателя, при мобилните ad hoc мрежи се използва специален код за автентификация на съобщението. Той представлява хеширано представяне на съобщението и е криптографска чексума, която се определя от ключа за криптиране и декриптиране. При обратното преобразуване и евентуално съвпадение на кода в приемната страна се потвърждава фактът на недопускане на промяна на съобщението и се гарантира цялостността на информацията.

Използваните протоколи при мобилните ad hoc мрежи са уязвими от гледна точка на сигурност на информацията [2]. Една от основните причини за този недостатък е факта, че топологията на разглежданите структури се променя динамично. Това създава трудности при определянето на причината за промяна на маршрутизиращата информация, която може да е резултат както от изменение на броя или метоположението на устройствата, така и от въвеждане на лъжлив трафик [3].

4. Маршрутизиращи протоколи за осигуряване на информационната сигурност.

Особеностите на мобилните ad hoc структури, в сравнение с традиционните проводни мрежи, налагат необходимостта от използването на специфични маршрутизиращи протоколи. Те могат да бъдат разделени на две основни групи: проактивни и реактивни. На фиг. 1 са посочени най-често използваните маршрутизиращи протоколи, които предлагат съвременни решения за осигуряване на сигурността [3].

Фиг. 1. Маршрутизиращи протоколи, предназначени за осигуряване на информационната сигурност на мобилни ad hoc мрежи.

Характерно при проактивните протоколи е, че те поддържат информация за маршрута между кои да е две устройства в мрежата. Поради факта, че данните за използваните пътища обикновено се съхраняват в таблици те се наричат още table-driven протоколи. Друга тяхна особеност е, че позволяват на всяко устройство непрекъснато да актуализира информацията си за топологията на мрежата.

При реактивните маршрутизиращи протоколи се изграждат път между две устройства само при необходимост. След първоначалното му определяне, маршрута се пази докато е наличен и докато се използва.

Предимство на проактивните маршрутизиращи протоколи е времето за използване на маршрута, тъй като той е наличен и може да се използва веднага.

Всеки от посочените на фиг. 1 маршрутизиращи протоколи притежава предимства и недостатъци, които го правят подходящ за определени условия на работа. Те притежават и определени възможности за адаптиране към динамично променящата се топология на мрежата, но в същото време несъвършенствата им, от гледна точка на сигурността, могат да бъдат използвани за компрометиращи действия [3].

5. Заключение.

Въпреки използваните механизми за защита мобилните ad hoc мрежи са уязвими по отношение на сигурността на информацията. Една от причините за това е динамично променящата се топология, която е предизвикателство при адаптирането и подбора на маршрутизиращи протоколи.

Широкият кръг от приложения и условия за работа на мобилните ad hoc мрежи не позволява да се посочи универсален подход при създаването и усъвършенстването на протоколи, които са в състояние да удовлетворят съвременните изисквания за сигурност на информацията. Предвид факта, че хибридните маршрутизиращи протоколи съчетават предимствата на проактивния и реактивния подход, би могло да се търси компромисно решение в тази посока.

Използвана литература:

1. Доктрина на въоръжените сили на Република България – НП 01. Министерство на отбраната на Република България, София, 2011.

2. Mohapatra, P., S. Krishnamurthy. Ad Hoc Networks Technologies and Protocols. Springer, 2005. ISBN 0-387-22690-7.

3. Singh, K., R. S. Yadav, Ranvijay. A Review Paper on Ad Hoc Network Security. International Journal of Computer Science and Security. Volume 1, Issue 1, pp 52-69, 2007.

4. Wang, X. Mobile Ad-Hoc Networks: Protocol Design. InTech Chapters, 2011. ISBN 978-953-307-402-3.

5. http://seminarprojects.com/Thread-security-in-ad-hoc-wireless-networks-full-report 20.09.2013.

6.https://www.cs.tcd.ie/hitesh.tewari/papers/netsec00_manet_sec.pdf 20.09.2013.

За контакти:

Желязко Николов
ВВМУ „Н. Й. Вапцаров”, кат. „Електроника”
9026, Варна, ул. Васил Друмев №73
e-mail: zhelyazko_nikolov@abv.bg

Росен Спиров
ТУ-Варна, “ОУЛ по Електроника”,
9010, Варна, Ул. Студентска № 1, 606Е
e-mail: rosexel@abv.bg

Любомир Алексиев
ТУ-Варна, „ОУЛ по Мехатроника”,
9010, Варна, Ул. Студентска № 1, 523НУК
e-mail: aleksiev.l.i@abv.bg