3. Wstęp do komunikacji bliskiego zasięgu(NFC)

3.1 Komunikacja bliskiego zasięgu (NFC)

Ten rozdział dokładnie opisuje technologię NFC oraz szczegółowo przedstawia jej aspekty techniczne. NFC, jako jedna z kluczowych technologii bezprzewodowej komunikacji, odgrywa istotną rolę w nowoczesnych aplikacjach mobilnych. Celem rozdziału jest opisanie wykorzystywanych modulacji i kodowań w NFC. Dodatkowo, znajdują się tu informacje na temat bezpieczeńswa tej technologii, przedstawione zostały potencjalne zagrożenia i sposoby ich minimalizacji. W zakończeniu rozdziału technologia NFC została zestawiona i porównana z innymi systemami komunikacji bezprzewodowej, takimi jak Wi-Fi oraz Bluetooth, ukazując ich różnice oraz specyficzne zastosowania.

Komunikacja bliskiego zasięgu (NFC) to protokół komunikacyjny działający na krótkich odległościach- do ok. 10 cm. Pracuje w wysokiej częstotliwości 13,56 MHz. Antena NFC emituje wokół siebie energię rozprowadzaną na niewielkie odległości, co związane jest z jej małymi rozmiarami. Emitowanie energii z wykorzystaniem tej częstotliwości na dalekie odległości wymaga użycia ogromnych anten. Urządzenie NFC musi posiadać co najmniej antenę oraz modulator-demodulator, które są ze sobą połączone. Modem jest odpowiedzialny za konwersje sygnałów eletromagnetycznych na dane cyfrowe. W komunikacji bliskiego zasięgu wyróżnia się dwa podmioty- inicjator oraz cel. Inicjatorem może być czytnik NFC, który jedynie odczytuje dane lub urządzenie czytająco-zapisujące (smartfon), które może zapisywać oraz odczytywać dane do celu. Obiektem docelowym jest urządzenie, odpowiadające na transmisje od inicjatora. Zwykle są nimi smartfony lub podobne do nich, programowalne urządzenia. Pozwala to na duże możliwości m.in. generowanie unikalnej zawartości dla każdej wymiany. Przykładowo można zaprogramować cel w taki sposób, aby w trakcie przekazania danych od inicjatora odesłał potwierdzenie.[2]

Urządzenia zgodne z NFC muszą spełniać surowe standardy, które określa i pilnuje przestrzegania NFC Forum. Jest to stowarzyszenie non-profit założone w 2004 roku przez trzy firmy: Sony, Nokia oraz Phillips, zajmujące się standaryzowaniem i promowaniem tej technologii.

Standard NFC posiada trzy tryby pracy:

1. Odczyt/Zapis - Umożliwia interakcje typu ’dotknij i odczytaj’ lub ’dotknij i zapisz’, co jest przydatne w wielu aplikacjach, od tagów informacyjnych po konfiguracje urządzeń.
2. Peer-to-Peer - W tym trybie, dane są przesyłane w obu kierunkach między dwoma

Rysunek 3.1: Znak "N"

urządzeniami NFC, co pozwala na dwustronną komunikację.

3. Tryb emulacji karty - Tryb emulacji karty to obecnie najpopularniejsze wykorzystanie NFC. Używany m.in. do płatności zbliżeniowych, w których telefon komórkowy z NFC emuluję fizyczną kartę płatniczą.

Znak "N"informuje o zgodności ze standardami NFC forum. Aby móc korzystać z tego znaku należy podpisać umowę z tym stowarzyszeniem. [1]

3.1.1 Format danych NDEF

NDEF (NFC Data Ex-change Format) jest formatem danych, którego używa protokół komunikacyjny NFC. NDEF składa się z takich części jak: nagłówek, posiadający informacje o rekordzie takie jak długość, typ rekordu, itp., oraz ładunku, który zawiera treść wiadomości.
Nagłówek NDEF składa się z flag

MB (message begin) - flaga ustawiona na 1 oznacza, że rekord NDEF jest pierwszym.
ME (message end) - flaga ustawiona na 1 oznacza, że rekord NDEF jest ostatnim.
CF (chunked flag) - flaga ustawiona na 1 oznacza, że rekord NDEF składa się z połączonych ze sobą rekordów.
SR (short record) - flaga ustwiona na 1 oznacza, że rekord NDEF jest krótki i składa się tylko z 7 bajtów zamiast standardowych 10.
IL (ID length) - flaga ustawiona na 1 oznacza, że należy odczytać pola Długość ID oraz ID ładunku.
TNF (type name format) - jest to 3 bitowa flaga, która określa format nazwy typu. Poniżej zostało przedstawione co oznaczają poszczególne wartości.

0 Pusty typ: oznacza, że rekord nie zawiera typu oraz ładunku. Jest używany w sytuacjach, gdy potrzebny jest pusty rekord, przykładowo do zakończenia wiadomości NDEF, jeśli nie ma zdefiniowanego ładunku przez aplikację

użytkownika.

1 Dobrze znane typ: to typ zdefiniowane przez RFC 2141[5], przykładowo "urn:nfc:wkt:T"zapis jest skracany do "T", gdzie TYPE "T"oznacza tekst, urn:nfc jest identyfikatorem dla przestrzeni nazw NFC, a wkt jest skrótem od Well Known Type.
2 MIME media-type: typ określa typ zawartości, np. text/html określa typ html, a typ image/jpeg określa typ JPEG
3 URI(Uniform Resource Identifier): ten typ pozwala na określenie lokalizacji w internecie, na urządzeniu.
4 NFC FORUM zewętrzne typy: to typy zdefiniowane przez zewnętrzne podmioty zgodnie z obowiązującymi standardami.
5 Nieznane typy: przykładem jest typ MIME "aplication/octet-stream", używany do oznaczania danych binarnych.
6 Bez zmian: typ używany w przypadku połączonych ze soba rekordów, gdy flaga CF jest ustawiona na 1, pierwszy rekord w tym łańcuchu ma swój typ, a następne, które wchodzą w skład tej wiadomości mają typ bez zmian.
7 Zarezerwowany: typ zarezerwowany, do przyszłego wykorzystania.

Długość typu : długość pola typ
Długość ID : długość pola ID
Długość ładunku : długość pola ładunku
Typ : typ ładunku
ID : ID ładunku
Ładunek : dane przechowywane formacie NDEF
[6]

3.1.2 Rodzaje modulacji oraz kodowania w NFC

Standard NFC obejmuje 3 podstawowe rodzaje kodowania i modulacji. Każdy z tych rodzajów stosuje unikalne metody modulacji amplitudy i fazy, co pozwala na różnorodność w sposobie przesyłania danych.[1]

NFC-A : W tym typie stosuje się kodowanie Millera dla nadajnika i kodowanie Manchester dla odbiornika. Wykorzystuje ono modulację amplitudową z 100% przesunięciem amplitudy (ASK), co oznacza, że sygnał jest całkowicie wyłączany podczas przerw, co ułatwia demodulację sygnału. NFC-A umożliwia transmisję z prędkością 106 kbps.

NFC-B : W NFC-B zastosowano kodowanie non-return-to-zero (NRZ), które również korzysta z modulacji amplitudowej na poziomie 10% ASK. Tutaj również nie ma sygnału podczas przerw w wysyłaniu danych. Przy odbiorze danych wykorzystuje się modulację BPSK (Binary Phase-Shift Keying), czyli binarne przesunięcie fazowe. Prędkość transmisji, podobnie jak w NFC-A, wynosi 106 kbps.

NFC-F : Odpowiada to technice FeliCa, szeroko stosowanej w Japonii. W tym standardzie używa się kodowania Manchester z modulacją amplitudową ASK, z prędkościami transmisji wynoszącymi 212 lub 424 kbps.

3.2 Bezpieczeństwo w NFC

Bezpieczeństwo jest nieodłącznym elementem każdej technologii komunikacyjnej, a w przypadku NFC jego znaczenie jest szczególnie istotne z uwagi na charakter i zastosowania tej technologii. NFC, będąc technologią umożliwiającą bezprzewodową komunikację na krótkich dystansach, niesie ze sobą szereg potencjalnych zagrożeń. Do najbardziej znaczących należą podsłuchiwanie, ataki DoS (Denial of Service), ataki typu Man-in-the-Middle oraz modyfikacja danych. Poniżej zostały dokładnie opisane te zagrożenia oraz sposoby ochrony przed nimi.[4]

3.2.1 Zagrożenia oraz sposoby ochrony

Podsłuchiwanie : atakujący, który chce podsłuchać komunikację NFC, może w łatwy sposób tego dokonać i zdobyć niezbędna wiedzę oraz sprzęt. Gdy dochodzi do komunikacji przez NFC wysyłane są fale radiowe, a przechwycenie sygnału NFC nie wymaga trudno dostępnego sprzętu. Komunikacja NFC odbywa się na zasięgu do 10cm, jednak posiądając specjalną antenę można przechwycić tą komunkację na większych odległościach. Odległości te są zależne od wielu czynników, np.: parametrów anteny nadawcy, parametrów anteny atakującego, miejsca (wolna przestrzeń lub ściany i inne przeszkody). Ważnym aspektem jest to, w jakim trybie pracuje wysyłające urządzenie. Przykładowo podsłuch dla urządzenia wysyłającego działającego w trybie pasywnym, można wykonać na odległości około 1m, natomiast w trybie aktywnym jest to już aż 10m.

DoS : atakujący, zamiast podsłuchiwania komunikacji może ją zakłócać. Jest to stosunkowo prosty atak, który polega na transmisji odpowiednich częstotliwości widma w danym czasie. Częstotliwości i czas można obliczyć, gdy atakujący ma wiedzę jaka modulacja oraz kodowanie zostały użyte do transmisji.

Modyfikacja danych : atakujący, chcąc zmodyfikować dane musi posiadać wiedzę dotyczącą sposobu kodowania i modulacji, które zostały użyte. W zależności od użytego sposobu modulacji i kodowania osoba atakująca ma różne możliwości modyfikacji danych. Przykładowo dla typu NFC-A modyfikacja danych wymaga od atakującego precyzyjnego manipulowania sygnałem radiowym, co jest zadaniem wymagającym szczegółowej wiedzy technicznej. Możliwa jest jednak zmiana wartości bitu 1 na 0, odwrotnie jest to już niemożliwe. co wynika z charakterystyki modulacji sygnału w tej technologii. Z kolei dla typu NFC-B osoba atakująca ma możliwość zmiany wszystkich bitów.

3.2.2 Sposoby ochrony

Podsłuchiwanie : NFC nie posiada żadnych specjalistycznych zabezpieczeń, które mogłoby chronić się przed tym atakiem, dlatego tak istotne jest ustanowienie bezpiecznego kanału opisanego na końcu tego podrozdziału.

DoS : Aby zapobiec atakowi, urządzenia komunikujące się przez NFC powinny być w stanie go wykryć i ostrzec atakowane podmioty, Związane jest to z mocą sygnału, która do zakłócenia musi być znacznie większa niż ma to miejsce w przypadku normalnej komunikacji NFC.

Modyfikacja danych : zastosowanie trybu aktywnego dla obu urządzeń może skutecznie zabezpieczyć komunikację przed modyfikacją danych, jednak wtedy komunikacja jest bardziej podatna na podsłuchiwanie. Można zapobiegać modyfikacji danych poprzez monitorowanie parametrów transmisji, w razie wykrycia jakichkolwiek nieprawidłowości urządzania mogą natychmiast przerwać komunikację. Najlepszym rozwiązaniem dla tego problemu będzie ustanowienie bezpiecznego kanału komunikacyjnego.

Bezpieczny kanał komunikacyjny pomiędzy urządzeniami to zdecydowanie najlepsze rozwiązanie dla zapewnienia bezpiecznej komunikacji NFC. Inicializacja takiego kanału jest stosunkowo prosta, gdyż można użyć standardowych protokołów do uzgadniania kluczy (np. protokół Diffiego-Helmana). Uzgodniony klucz może być następnie wykorzystany do stworzenia symetrycznego klucza np. 3DES. Finalnie kanał komunikacyjny jest szyfrowany co zapewnia poufność, integralność oraz autentyczność danych.

3.2.3 Wnioski

Komunikacja NFC jest technologią, która posiada wiele zalet. Bezpieczeństwo i szybkość inicializacji komunikacji doskonale sprawdzą się w sytuacji odbioru paragonu ze sklepu na swoje urządzenie. NFC pozwala zidentyfikować użytkownika posiadającego telefon. Przedstawiono również sposoby na zapobiegnięcie atakom takim jak: modyfikacja danych, podsłuchiwanie czy uszkadzanie danych. Wyjaśniono dlaczego ważne w komunikacji bezprzewodowej jest stosowanie bezpiecznego kanału komunikacyjnego. Kolejny rozdział pracy koncentruje się na przetwarzaniu danych w chmurze, które w połączeniu z NFC może zostać wykorzystane do stworzenia innowacyjnego i bezpiecznego systemu do przesyłania danych. Przykładowo, podczas zakupów stojąc w sklepie przy kasie, zamiast otrzymywać fizyczny paragon, konsumenci mogliby zbliżyć swoje urządzenia do terminala NFC, aby w ten sposób otrzymać cyfrową kopię paragonu. Takie rozwiązanie nie tylko przyspiesza proces zakupów, ale także przyczynia się do redukcji zużycia papieru. Przetwarzanie w chmurze oferuje dodatkową warstwę bezpieczeństwa i elastyczności, umożliwiając szybkie i bezpieczne przetwarzanie dużych plików. Na przykład paragony zapisane za pomocą NFC mogą być przechowywane i zarządzane w chmurze, co umożliwia użytkownikom łatwy dostęp do swojej historii zakupów, zarządzanie gwarancjami, czy też śledzenie wydatków.