Internet rzeczy latających

Systemy bezzałogowych statków powietrznych cieszą się ostatnio dużym zainteresowaniem, zwłaszcza ze względu na ich elastyczność i niższe koszty pozyskania. Jednak w wielu regionach pojawiły się problemy prawne, które ograniczają ich działanie w krytycznych środowiskach. W odpowiedzi na dobrze zgłoszone przypadki, wydaje się prawdopodobne, że w wielu krajach wokół krytycznych obszarów, takich jak lotniska (gdzie przypadkowe „uderzenia dronów" mogą stanowić zagrożenie dla samolotów odrzutowych podobnych do „ptasich"), zostaną ustanowione strefy zakazu lotów. - strajki"), więzienia (gdzie zgłaszano przypadki użycia dronów do transportu przemytu towarów do więźniów) oraz obszary wojskowe/poufne (gdzie rząd zwalcza drony z tresowanymi orłami). Zagrożenia bezpieczeństwa ze strony grup terrorystycznych stanowią również zagrożenie dla kluczowej infrastruktury. Wydaje się prawdopodobne, że w przyszłości może dojść do konsensusu międzynarodowego wokół pewnych obszarów (np. lotnisk komercyjnych), ale obraz prawdopodobnie pozostanie płynny przez jakiś czas. W międzyczasie, znaczące wysiłki badawcze badają obecne możliwości UAV i ich potencjał do autonomicznego działania poza polem widzenia dedykowanego operatora, co prawdopodobnie będzie podsycać dalszą debatę i prawodawstwo. Stosunkowo nowa koncepcja Internetu Rzeczy (IoT), polegająca na nowej formie łączenia i współdzielenia zasobów między urządzeniami, została uznana za kandydata do potencjalnej integracji z bezzałogowymi statkami powietrznymi. Taka współpraca może zapewnić nowy stopień swobody dla starych aplikacji i zupełnie nowe spektrum zastosowań. W tym rozdziale omówiono główne cechy Internetu Rzeczy Latających oraz związek tego terminu z systemami bezzałogowych statków powietrznych i Internetem Rzeczy. W rozdziale opisano, w jaki sposób ta nowa koncepcja rozwiązuje znane problemy, ale także wprowadza różne wyzwania do projektowania systemów.

Latające Rzeczy

Popularność i elastyczność systemów wbudowanych wprowadziła w ostatnich dziesięcioleciach nowe zastosowania w segmentach pojazdów, takich jak samochody, drony oraz morskie pojazdy podwodne lub naziemne. Ta sekcja przedstawia główne koncepcje segmentu powietrznego pod nową nazwą, latającą rzecz, obejmującą nie tylko ograniczoną gamę dronów, ale dowolny typ i/lub klasyfikację bezzałogowych systemów powietrznych.

Systemy bezzałogowych statków powietrznych

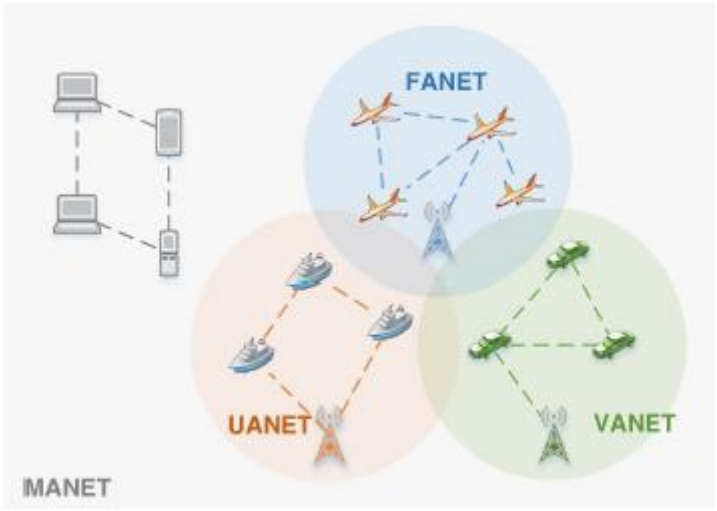
Bezzałogowe statki powietrzne (UAV), popularnie zwane dronami, są uważane za umożliwiające zupełnie nowy sposób wykonywania zadań, które wcześniej były albo nieosiągalne, albo kosztowne, wypełniając luki w wielu nowoczesnych zastosowaniach. Jak pokazano na rysunku, samoloty te mogą mieć wiele różnych rozmiarów i kształtów, a misje mogą być wykonywane przez jeden lub wiele UAV.

To bogactwo formy pozwala na ich wykorzystanie w różnorodnych zastosowaniach, takich jak poszukiwanie i ratownictwo, misje obserwacyjne i dostarczanie towarów. UAV są zwykle uważane za część większego systemu bezzałogowego statku powietrznego (UAS), który zawiera wszystkie elementy potrzebne do wykonania misji). Komponenty UAS mogą się różnić w zależności od typu, rozmiaru i misji UAV, ale zazwyczaj obejmują naziemną stację kontroli (GCS), podsystem komunikacyjny oraz mechanizmy bezpieczeństwa i odzyskiwania. Stworzenie UAS z wieloma współpracującymi UAV wiąże się z dodatkowymi, bardzo wysokimi wymaganiami w zakresie łączności, a aby je spełnić, pojawiło się nowe podejście sieciowe, Flying Ad Hoc Network.

Latające sieci ad hoc

Komunikacja jest kluczowym aspektem i jednym z największych wyzwań w projektowaniu systemów wielu pojazdów. W UAS istnieją trzy główne rodzaje komunikacji: (a) wewnętrzna komunikacja maszynowa (IMC), która obejmuje wszelką komunikację między wewnętrznymi modułami lub urządzeniami UAV, takimi jak automatyczny pilot lub kamery; (b) komunikacja maszyna-maszyna (M2M), która obejmuje komunikację między bezzałogowymi statkami powietrznymi; oraz (c) komunikacja maszyna-infrastruktura (M2I), która obejmuje komunikację między UAV a infrastrukturą sieciową (którą może być np. naziemna stacja kontroli lub satelita, a nawet połączenie obu). W najprostszym scenariuszu wszystkie pojazdy są bezpośrednio połączone ze wspólną infrastrukturą, która może działać jako pośrednik we wszelkiej komunikacji między nimi. Jednak ta strategia ma kilka problemów. Po pierwsze, każdy pojazd musi być wyposażony w drogi i skomplikowany sprzęt, aby nawiązać łączność na duże odległości ze stacją kontroli lub satelitą. Po drugie, na niezawodność komunikacji może wpływać wiele czynników, takich jak zmieniające się warunki środowiskowe, duża mobilność pojazdów, różne topologie terenu czy przeszkody. Wreszcie, typowe użycie naziemnej stacji kontroli (GCS) w celu zapewnienia infrastruktury komunikacyjnej ogranicza lokalizacje docelowe misji do obszaru zasięgu GCS, ponieważ poza tym pojazdy odłączają się od sieci i stają się nieosiągalne.

Wdrożenie sieci ad hoc łączącej wszystkie pojazdy jest jedną z najbardziej realnych alternatyw dla komunikacji opartej na infrastrukturze. Sieć ad hoc składa się z węzłów, które działają również jako routery, tworząc tymczasową sieć bez stałej topologii lub scentralizowanej administracji. Takie podejście zwiększa obszar docelowy misji, ponieważ komunikacja między pojazdami a GCS może być kierowana przez inne pojazdy w serii przeskoków. Ponadto, nawet jeśli nie ma połączenia z GCS, węzły mogą tworzyć sieć ad hoc w celu udostępniania informacji lub współpracy. Sieci ad hoc są klasyfikowane według ich implementacji, wykorzystania, komunikacji i celów misji. Jeżeli węzły tworzące sieć ad hoc są mobilne, sieć jest klasyfikowana jako MANET (Mobile Ad hoc NETwork). W przypadku zastosowań specyficznych dla pojazdów, MANET są podzielone na UANET (Underwater Ad hoc NETwork) dla pojazdów wodnych, VANET (Vehicular Ad hoc NETwork) dla pojazdów naziemnych lub FANET (Flying Ad hoc NETwork) dla statków powietrznych, jak pokazano na rysunku.



Każdy rodzaj sieci samochodowej stoi przed różnymi, unikalnymi wyzwaniami: na przykład UANET musi radzić sobie z podwodnym medium transmisyjnym, a VANET często napotykają nieoczekiwane przeszkody drogowe. Uznano jednak, że sieci FANET muszą rozwiązywać trudniejsze problemy niż inne sieci ad hoc, ze względu na następujące specyficzne cechy:

* Wyższa mobilność węzłów. Węzły FANET zazwyczaj mają większą mobilność niż w innych typach MANET. W rezultacie topologia sieci FANET może zmieniać się częściej, co zwiększa obciążenie spowodowane operacjami łączenia i routingu.

* Wiele połączeń. W wielu aplikacjach węzły w sieciach FANET zbierają dane środowiskowe, a następnie retransmitują je do stacji kontrolnej, podobnie jak w bezprzewodowych sieciach czujnikowych (WSN) . Dlatego systemy FANET muszą zarządzać wielokrotną komunikacją między UAV a stacjami monitorującymi, a także zapewniać obsługę połączeń peer-to-peer między UAV.

* Bardzo niska gęstość węzłów. Typowe odległości między węzłami w sieciach FANET są zwykle dłuższe niż w sieciach MANET i VANET; w związku z tym zasięg komunikacji w sieciach FANET musi być również większy niż w innych sieciach. Nakłada to większe wymagania na łącza radiowe i inne elementy sprzętowe.

* Niejednorodność. Systemy UAV mogą zawierać heterogeniczne czujniki, a każdy z nich może wymagać innych strategii dystrybucji danych.

*Przeszkody. Ze względu na większą mobilność węzłów przeszkody mogą losowo blokować łącza między UAV, które należy zaadresować w celu zapewnienia różnych tymczasowych ścieżek komunikacyjnych, unikając odłączania węzłów.

Latające rzeczy: bezzałogowe statki powietrzne i nie tylko

Wspólną cechą wielu różnych wizji Internetu Rzeczy jest wszechobecność przedmiotów codziennego użytku wyposażonych w identyfikowanie, wykrywanie, tworzenie sieci i możliwości przetwarzania, które komunikują się ze sobą, aby osiągnąć wspólny cel. W kontekście powstających modeli sieciowych, takich jak IoT, zaczyna obowiązywać nowa nazwa dla UAV. Jako Latająca Rzecz, UAV (i wszelkie inne elementy zdolne do latania, takie jak autonomiczne lub nieautonomiczne pojazdy powietrzne) można zintegrować z siecią fizycznych interaktywnych obiektów, które są w stanie komunikować się z innymi urządzeniami i systemami z dostępem do Internetu. Ta integracja została nazwana Internetem Rzeczy Latających i może rozwiązać niektóre problemy w systemach bezzałogowych, a także wprowadzić nowe, wydajne aplikacje.

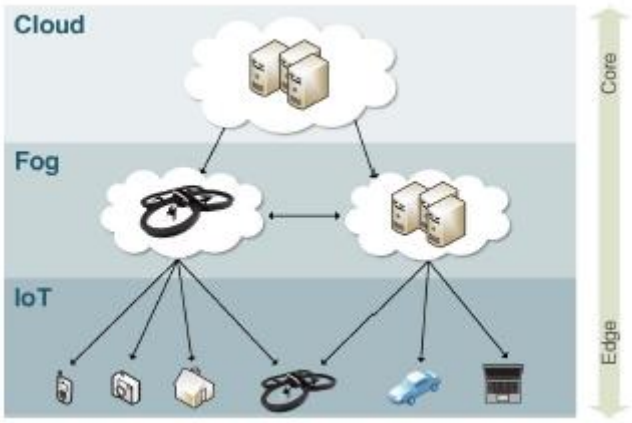
Internet rzeczy latających

Zgodnie z tendencją naszego coraz bardziej połączonego świata, UAV prawdopodobnie będą zintegrowane z innymi elementami i systemami, aby wykonywać misje o większej złożoności. Nowy Internet Rzeczy Latających (IoFT) daje nowy poziom swobody bezzałogowym systemom powietrznym, poszerzając granice ich misji i umożliwiając nowe zastosowania, zwiększając ich łączność, poprawiając współpracę i współpracę między systemami, a także umożliwiając aktualizowanie danych zaopatrzenie. Chociaż nowy Internet rzeczy latających ma zastosowanie w kilku różnych segmentach, szczególną atrakcją jest afordancja, jaką oferuje w środowiskach, które są obecnie źle obsługiwane przez istniejącą (przewodową) infrastrukturę, taką jak obszary wiejskie lub biedne społeczności. Te przykłady są dużymi motywatorami do tworzenia rozwiązań łączących elastyczny adaptacyjny IoT z szybkimi, tanimi UAV, które razem prawdopodobnie zapewnią wysoką jakość usług użytkownikom końcowym w odległych obszarach. Jednak przy rozważaniu obszarów trudno dostępnych pojawia się ważna koncepcja - przetwarzanie mgły. Bliskie relacje można nawiązać między obliczeniami mgły, przetwarzaniem w chmurze i modelami internetowymi, takimi jak Internet rzeczy latających.

Mgła i przetwarzanie w chmurze

Obecnie istnieją dwa główne trendy kształtujące naszą sieć: przetwarzanie w chmurze i rozpowszechnianie komputerów przenośnych. Około 90% globalnych użytkowników Internetu polega obecnie na usługach opartych na chmurze, a wynika to głównie z faktu, że w 2011 r. światowa sprzedaż smartfonów wyprzedziła sprzedaż komputerów PC. Pojawiająca się fala wdrożeń internetowych, takich jak IoT, wymaga nie tylko wsparcia mobilności i geodystrybucji, ale także świadomości lokalizacji i małych opóźnień. Przetwarzanie w chmurze jest kluczową koncepcją dostarczania IoFT. Chmura to model obliczeniowy na żądanie składający się z autonomicznych, sieciowych zasobów informatycznych (sprzętowych i/lub programowych). Ponieważ większość komunikacji zarządzanej przez IoFT jest przesyłana za pośrednictwem infrastruktury IoT, ważnym aspektem staje się jakość usług (QoS), która spełnia te same wymagania co cloud computing. Dostawcy usług oferują usługi w chmurze z predefiniowanymi warunkami QoS w oparciu o Internet jako zestaw zarządzanych, skalowalnych, łatwych w użyciu i niedrogich usług do gromadzenia klientów na zasadzie subskrypcji. Dlatego ważne jest, aby infrastruktura IoFT spełniała wymagania QoS w zakresie świadczenia usług od i do latającego obiektu, ponieważ krytyczność jego operacji może być wyższa niż zwykłych stałych elementów IoT. Co więcej, niektóre aplikacje IoFT wymagają odpowiedzi w czasie rzeczywistym, co odbywa się poprzez delegowanie zadań obliczeniowych do chmury, ze względu na ograniczoną pojemność urządzeń mobilnych. Fakt ten potęguje konieczność świadczenia asertywnych usług. Z drugiej strony, w

przypadku odległych obszarów o ograniczonej lub braku łączności z Internetem, nie zawsze byłby możliwy arbitralny dostęp do usług w chmurze z akceptowalnymi czasami reakcji QoS i wymaganiami czasu rzeczywistego. Jednak niektóre aplikacje mogą nadal korzystać z IoFT, tymczasowo pracując z lokalnymi kopiami danych i usług, imitując strukturę chmury obliczeniowej, a następnie umożliwiając świadczenie usług, które nie opierają się na częstych aktualizacjach. Jest to przypadek, w którym obliczanie mgły jest kluczowym elementem sieci IoFT. Przetwarzanie mgły składa się z wysoce zwirtualizowanej platformy do obliczania, przechowywania i świadczenia usług sieciowych między urządzeniami końcowymi a tradycyjnymi centrami przetwarzania danych w chmurze, które są zazwyczaj, ale nie wyłącznie, zlokalizowane na obrzeżach sieci. Na przykład z perspektywy IoFT, inteligentna farma z ograniczonym dostępem do Internetu mogłaby skorzystać na infrastrukturze mgły przetwarzającej większość danych i usług potrzebnych do zwykłych zadań, przesyłając i pobierając do chmury tylko istotne i/lub niezbędne informacje. Charakterystyka przetwarzania w chmurze/mgle ma ważne przecięcia ze scenariuszami IoT. Główne wymagania IoFT są spełniane przez mgłę obliczeniową ze względu na następujące cechy: (a) małe opóźnienia i świadomość lokalizacji, umożliwiające sieci IoFT działanie przynajmniej w ograniczonym zakresie i czasie, świadczenie usług oraz wykonywanie zadań i misji; (b) mobilność, główna konieczność w aplikacjach IoFT; (c) bardzo duża liczba węzłów, która spełnia wymagania zarówno sieci IoT, jak i IoFT; d) dominująca rola dostępu bezprzewodowego; f) silna obecność aplikacji do transmisji strumieniowej i czasu rzeczywistego; oraz (g) heterogeniczność . Latająca rzecz może odgrywać dwie różne role w scenariuszu IoFT wspieranym przez obliczenia mgły, jak widać na rysunku.



Pierwszy to jednostki przetwarzające w warstwie mgły, służące jako dostawcy Internetu rzeczy latających. Aby podać dwa przykłady, na obszarach oddalonych lub dotkniętych katastrofą, gdzie trudno jest uzyskać łączność, elastyczna struktura mobilna, która mogłaby zapewnić lub rozszerzyć usługi mgły, byłaby ważnym czynnikiem. Podobnie, UAV mogą pełnić rolę dostawców mgły w wysoce połączonych środowiskach, w których niektóre aplikacje mogą dobrze działać w trybie offline przez krótkie lub nawet długie okresy czasu, zmniejszając zużycie danych i tworząc partie informacji do przesłania do chmury w całości -raz. W innej roli bezzałogowe statki powietrzne mogą działać jako węzły brzegowe (użytkownicy końcowi), korzystając z infrastruktury mgły.

Charakterystyka Internetu Rzeczy Latających

IoFT jest rzeczywiście elastyczny. Ta cecha jest ważna dla zapewnienia prawie każdej funkcji w takim modelu. Pomaga zwiększyć ogólną współpracę i współpracę, jest gotowy do operacji w czasie rzeczywistym, jest zwykle aktualny dzięki wysoce połączonemu środowisku i łatwemu dostępowi do Internetu oraz jest wspomagany przez potężną zdalną chmurę i/lub lokalną strukturę mgły . Pod względem kosztów, ponieważ IoFT łączy zalety dwóch dobrze znanych paradygmatów, a mianowicie

IoT i UAV, które mogą różnić się od tanich do drogich komercyjnych produktów z półki, będzie dostępne niedrogie i adaptacyjne rozwiązanie dla większości potrzeb . Współpraca i współdziałanie są pożądanymi cechami większości nowoczesnych systemów komputerowych. Wiele nowoczesnych aplikacji dystrybuuje zadania i udostępnia informacje w czasie rzeczywistym, szybko zapewniając lepsze wyniki. W szczególności środowisko gotowe na IoT jest zwykle zaprojektowane tak, aby było wyposażone w więcej niż jeden sposób pozyskiwania danych, interakcji i automatyzacji określonych zadań. Chociaż IoT jest modelem skalowalnym, jego ekspansja może oznaczać wysokie koszty przy stosunkowo niewielkich zyskach. Jeśli środowisko nie rozwija się łatwo, jego elastyczność może być zagrożona, co skutkuje ograniczoną współpracą i współpracą. IoFT rozwiązuje to napięcie na różne sposoby – na przykład poprzez ustawienie UAV w strategicznych obszarach służących jako bramy, mgła lub dostawcy łączy danych w chmurze, a także poprzez możliwość wymiany czujników i urządzeń wykonawczych w bardziej aktywny i tańszy sposób (na przykład, jeśli psuje się sygnalizacja świetlna, latająca rzecz może być użyta do tymczasowego zastąpienia jej zadania). Co więcej, operacje w czasie rzeczywistym są również priorytetem modelu, ponieważ można go rekonfigurować w celu spełnienia wymagań i zapewnić najlepsze połączenie z serwerami i usługami dostępnymi lokalnie lub przez Internet. Integracja IoFT z infrastrukturami IoT osiągnięta dzięki strategicznemu pozycjonowaniu UAV pomaga modelowi spełnić kilka kluczowych funkcji. Łączenie z internetowym przetwarzaniem informacji może w czasie rzeczywistym zestawiać usługi z całego świata, dostarczając cennych, aktualnych i dokładnych informacji. To z kolei może ułatwić interaktywne podejmowanie decyzji w odpowiedzi na dynamiczne sytuacje. Decyzje te mogą być przetwarzane w potężnych centrach danych dostępnych jako dostawcy chmury. Rezultatem netto jest umożliwienie bardziej niezawodnego i misje bardziej adaptacyjne, maksymalizujące ich potencjalne korzyści lub poszerzające ich zastosowanie. Segmenty IoT i UAS są ograniczone przez ich nieodłączną charakterystykę infrastruktury. Chociaż można je rozszerzyć, na przykład koszt instalacji jest oszustwem, które należy wziąć pod uwagę, zwłaszcza jeśli taka infrastruktura może być niewystarczająco wykorzystana. W takim przypadku zaletą jest zastosowanie elastycznych elementów latających do wykrywania i uruchamiania.

Ogólne nowoczesne zastosowania Internetu rzeczy latających

UAV i IoT to popularne tematy, które przyciągnęły uwagę dzięki swojej elastyczności i tanim osiągnięciom. Korzyści płynące z Internetu rzeczy latających wykraczają poza tradycyjne aplikacje, które ostatnio można zobaczyć w prasie medialnej. Poniższe akapity przedstawią kilka przykładów, jak aplikacje mogą zostać przeniesione na nowy poziom dzięki wykorzystaniu elastyczności IoFT.

Zastosowania w sytuacjach awaryjnych

* Szukać i ratować. W sytuacji awaryjnej z ofiarami latające rzeczy mogą wykrywać i zgłaszać położenie ofiar w czasie rzeczywistym. Informacje te można skoordynować z informacjami z czujników pogody/ruchu, zapewniając skuteczną akcję ratunkową.

* Pierwsza pomoc i materiały eksploatacyjne. Po zidentyfikowaniu pozycji ofiar, latające rzeczy, które przewożą pierwszą pomoc i zaopatrzenie, mogą zostać przeniesione na określone stanowiska, aby pomóc ofiarom, a to może być skoordynowane z wykorzystaniem informacji o dostępności przydatnych zasobów/zapasów w pobliżu lokalizacje. Co więcej, jeśli ofiary poruszały się z jakiegokolwiek powodu, informacje o lokalizacji mogą być aktualizowane w czasie rzeczywistym. Ta aktualizacja może być wykonana przez latające urządzenie, które wykrywa pozycję i wysyła te informacje do dostawcy pierwszej pomocy latającej rzeczy

Aplikacje w inteligentnych miastach

* Nadzór. Latające rzeczy można wykorzystać do zwiększenia pojemności istniejących systemów monitorowania tłumów lub reagowania na sygnały alarmowe. Na przykład w inteligentnym mieście ludzie mogą być połączeni z usługami miejskimi za pomocą technologii do noszenia; w niebezpiecznej sytuacji osoba może powiadomić infrastrukturę na kilka różnych sposobów i wywołać odpowiednie działanie, takie jak przydzielenie nadzorującego obiektu latającego do monitorowania obszaru.

* Monitorowanie ruchu. Chociaż inteligentne miasta mają urządzenia i czujniki do monitorowania ruchu, urządzenia te są kosztowne i mogą być zawodne, więc zasięg nie zawsze jest pełny. Latające rzeczy można wykorzystać na dwa sposoby podczas planowania infrastruktury inteligentnego miasta: w celu zapewnienia elastycznego dodatkowego pokrycia, które można zaplanować (na przykład w celu monitorowania okazjonalnego, ale przewidywalnego dużego natężenia ruchu wokół hali sportowej) lub nieplanowanego (na przykład po zdarzeniu drogowym w obszarze, który nie jest lub słabo jest objęty stałymi czujnikami). W ten sposób latające rzeczy mogą być wykorzystywane do monitorowania tych obszarów i wspomagania zarządzania ruchem samochodowym.

* Dostawa paczek handlowych. Latające rzeczy zapewniają elastyczne źródło usług dostawczych. Mogłyby być wykorzystywane zarówno do zwiększania liczby pojazdów w celu zaspokojenia istniejących rodzajów popytu, jak i do generowania nowych strumieni przychodów z szybkich dostaw w trudno dostępnych lub zatłoczonych obszarach.

Zastosowania w inteligentnych gospodarstwach

* Nadzór. Biorąc pod uwagę, że gospodarstwa są terenami prywatnymi, mogą być narażone na inwazje. Wykorzystanie latających rzeczy do monitorowania granicy farm może pomóc w inwigilacji poprzez zgłaszanie potencjalnych problemów w czasie rzeczywistym za pomocą infrastruktury IoT inteligentnej farmy. Co więcej, IoFT służy jako infrastruktura zaplecza dla aplikacji opartych na IoT.

* Integracja usług. W inteligentnych farmach wymagane są różne zadania, co jest kosztowne, jeśli każde z nich jest wdrażane oddzielnie. Elastyczne urządzenie latające może monitorować uprawy, zwierzęta, rozprowadzać produkty, ładować zapasy i inne zadania. W szczególności może być również podłączony do innych latających rzeczy przez Internet, nawet bez linii wzroku. Ta funkcja może poprawić usługi w inteligentnej farmie poprzez przezwyciężenie ograniczeń tradycyjnych mediów komunikacyjnych.

* Identyfikacja pożaru lub innych problemów. Uprawa może zostać uszkodzona przez kilka czynników, takich jak dzikie zwierzęta, ogień i mróz. Latające istoty mogą wykrywać problemy w uprawach za pomocą własnych czujników lub danych zebranych z czujników stałych.

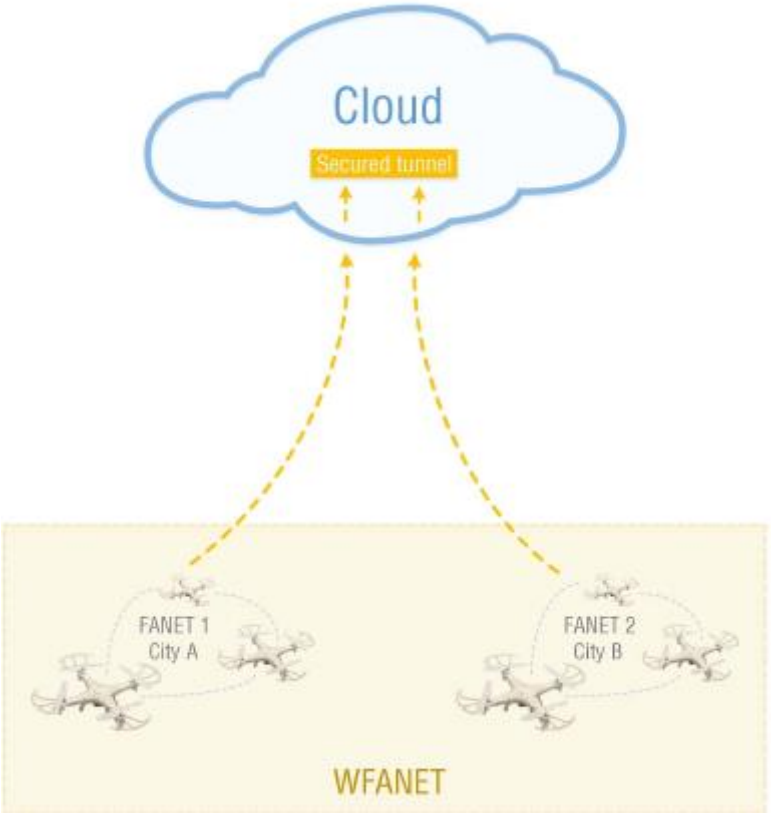
Misje urzędników państwowych

* Nadzór graniczny. Biorąc pod uwagę postępującą globalizację, kraje mają tendencję do ochrony swoich granic na różne sposoby. Koncentrując się na ulepszeniu zautomatyzowanego nadzoru, latające rzeczy mogą identyfikować przejścia graniczne i śledzić nielegalnych imigrantów, jednocześnie przesyłając informacje o lokalizacji w czasie rzeczywistym przez Internet. Takie informacje związane z czujnikami rozłożonymi na ziemi powinny zapewniać dokładniejsze wyniki.

* Wykrywanie pożarów lasów i nielegalne pozyskiwanie drewna. Obawy o globalne ocieplenie narastają z każdym dniem. Jedną z przyczyn jest zmniejszenie obszarów leśnych na całej planecie z powodu pożarów i nielegalnego pozyskiwania drewna. Samoloty załogowe są często używane, ale drogie. Latające przedmioty mogą stać się rozwiązaniem zwiększającym zasięg, a tym samym możliwością identyfikowania problemów w czasie rzeczywistym, co może zapobiec poważnym pożarom lub pomóc w zatrzymaniu nielegalnych drwali.

Nowatorskie zastosowania Internetu rzeczy latających

FANETy umożliwiają łączność między UAV, co upraszcza współpracę i współpracę między latającymi przedmiotami. Niekoniecznie są one jednak połączone z Internetem, ponieważ działają nad rojami UAV, które współpracują ze sobą udostępniając zasoby i dane w lokalnej sieci offline. Przeniesienie latających rzeczy do nowego paradygmatu, takiego jak IoFT, zapewnia „skrzydła" koncepcji FANET i czyni je potężniejszymi. Wyobraź sobie, że latają rzeczy geograficznie odległe bez widocznej linii widzenia (LoS), ale nadal dzielą się danymi, zasobami sieciowymi i usługami, tak jakby wszystkie znajdowały się w tej samej sieci lokalnej. Staje się to możliwe dzięki wprowadzeniu sieci zorientowanych na IoFT. Wide FANETs (WFANETs) łączą koncepcję FANETs z IoT i czerpią inspirację z sieci rozległych (WAN) do czerpania korzyści ze wszystkich paradygmatów. Wizualna reprezentacja jest widoczna na rysunku, który ilustruje rzeczywisty scenariusz z sieciami WFANET.



Główną cechą sieci ad hoc jest istnienie co najmniej jednej ścieżki do każdego węzła w sieci. Zwykle jest to możliwe, jeśli węzły znajdują się w ograniczonym zasięgu i jeśli istnieją strategiczne łącza LoS, gwarantujące, że główne łącza nie zostaną przerwane. Nowa koncepcja sieci WFANET korzysta z połączenia z infrastrukturą IoT już dostępną dzięki pobliskim inteligentnym środowiskom (np. inteligentne miasta, inteligentne drogi, inteligentne domy, inteligentne farmy, a nawet inteligentne samochody). Po podłączeniu do infrastruktury, która może zapewnić szerokopasmowy dostęp do Internetu do lokalnej sieci FANET, można utworzyć tunel do wymiany informacji i współpracy ze zdalnymi sieciami FANET. Łączenie latających obiektów z różnych lokalizacji geograficznych poprzez przezroczyste tunelowanie w chmurze, zapewniające te same funkcje, co lokalny FANET, tworzy WFANET. Sieci WFANET pozwalają na różne podejścia i zastosowania. Dobrym przykładem są duże wydarzenia, na przykład mecze piłki nożnej, igrzyska olimpijskie i koncerty, które wymagają wysokiego poziomu bezpieczeństwa w celu zarządzania dużymi tłumami, monitorowania podejrzanych działań, zarządzania bieżącymi wydarzeniami i tak dalej. Innym przykładem aplikacji udoskonalonej przez sieci

WFANET jest skanowanie nawierzchni pod kątem niebezpieczeństwa, pomagające w zapewnieniu lepszej jakości dróg. Latająca istota skanująca drogi może być pomocna w rozpowszechnianiu ostrzeżeń do inteligentnych systemów transportowych, zmniejszaniu liczby wypadków samochodowych, ulepszaniu usług ochrony i bezpieczeństwa, a także dostarczaniu informacji o możliwych opóźnieniach podróży i/lub powiadomieniach dotyczących osobistych planów. W scenariuszu można by również uwzględnić dodatkowe informacje, takie jak na przykład warunki pogodowe, poprawiając świadczenie usług. Logicznie rzecz biorąc, można sobie wyobrazić, że czujniki przenoszone na bezzałogowych statkach powietrznych można również uznać za samoistne obiekty latające, które akurat znajdują się w kolokacji z innymi osobami na pokładzie. Jeśli te usługi zostaną ogłoszone za pośrednictwem automatycznego brokera, wiele innych agencji może zdecydować się zapłacić za dostęp do nich. Na przykład sprzedawca żywności może wybrać strumienie wideo z dowolnych kamer zamontowanych na UAV, które akurat znajdowały się w tym obszarze, jeśli można je wykorzystać do przewidywania przepływów klientów i reagowania na nie. Co więcej, integracja obiektów latających z inteligentnymi środowiskami pozwala usprawnić działanie UAV. Na przykład lokalizacja GPS (globalnego systemu pozycjonowania) jest krytyczną informacją, która jest niezbędna dla latającego przedmiotu. Dzięki istnieniu infrastruktury, do której podłączona jest latająca rzecz, dostępne mogą być bardzo dokładne informacje o lokalizacji, pomagające UAV działać bardziej precyzyjnie. Inne czujniki, takie jak stacje pogodowe zamontowane na budynkach, mogą dostarczać w czasie rzeczywistym dane o warunkach lotu na trasie lotu. Niektóre problemy z bezpieczeństwem można również rozwiązać za pomocą samego IoFT, takich jak fałszowanie GPS.

Wyzwania

Przedstawiliśmy już niektóre korzyści dla systemów UAV z połączenia z siecią czujników IoT, a jeszcze więcej korzyści, które mogą wyniknąć z dodania elastycznego wykrywania w powietrzu i sieci do aplikacji IoT. Jednak pewne obawy związane z bezpieczeństwem i bezpieczeństwem wynikają z otwarcia „zamkniętego świata" systemu aUAV, o którym tutaj mowa. W tej sekcji podkreślono również, w jaki sposób Internet rzeczy latających może pomóc również w rozwiązywaniu starych problemów.

Zagadnienia ogólne

Nowy model Internetu Rzeczy Latających łączy to, co najlepsze w IoT i UAV w jedno rozwiązanie, które dziedziczy cechy, ale wprowadza też nowe wyzwania, którym trzeba sprostać. Krótko mówiąc, dzielą się one na trzy kategorie. Pierwszy zestaw kwestii dotyczy bezpieczeństwa publicznego oraz obaw etycznych związanych z gromadzeniem i dystrybucją danych. Inne oczywiste obawy dotyczyłyby podsłuchiwania – albo przez fizyczne przechwytywanie obrazów, albo przez zbliżanie się do lokalnych bezpiecznych sieci bezprzewodowych. Wydaje się prawdopodobne, że wiele krajów wprowadzi przepisy wymagające certyfikacji i autoryzacji do latania UAV i skorzysta z możliwości IoFT.

Drugi zestaw problemów wynika z chęci uniknięcia błędów z przeszłości branży komputerowej i obniżenia progów zaangażowania kluczowych interesariuszy, tak aby cała populacja mogła czerpać korzyści z tej technologii. Kwestie te są związane z normalizacją i muszą dotyczyć zarówno przemysłu, jak i rządów. Z technicznego punktu widzenia normalizacja to konieczne, aby wszystkie rzeczy rzeczywiście mogły „rozmawiać" ze sobą, zamiast tworzyć „efekt wieży Babel", w którym urządzenia dzielą się na rozłączne podzbiory (na przykład wszystkie urządzenia tego samego producenta), które mogą rozmawiać tylko z innymi ten sam podzbiór. Projekt sprzętu i oprogramowania musi uwzględniać ograniczenia pamięci, przechowywania, możliwości przetwarzania i źródła zasilania. Prawdopodobnie doprowadzi to do opracowania różnych rozwiązań dla obiektów latających przez różnych producentów, przy użyciu różnych architektur sprzętowych, platformy i protokoły komunikacyjne. W związku z tym istnieje pilna potrzeba, aby powstające standardy komunikacji i przesyłania danych

między urządzeniami były możliwe do wdrożenia w wysoce zasobooszczędnych algorytmach. Ze społecznego i ekonomicznego punktu widzenia normalizacja będzie sprzyjać wejściu na rynek małych i średnich firm, stymulując przedsiębiorczość i konkurencję, z korzyścią dla klienta końcowego oraz upowszechniając wykorzystanie technologii. Trzecia grupa pojawiających się problemów dotyczy głównie bezpieczeństwa i Big Data. Heterogeniczność obejmie również gromadzone dane, ponieważ oczekuje się, że IoT - a w konsekwencji IoFT - przyniesie dużą ilość nowych, najprawdopodobniej nieustrukturyzowanych danych. Jak i gdzie (lokalnie lub zdalnie) te dane będą przechowywane i odzyskane zgodnie z wymaganiami dotyczącymi czasu rzeczywistego i bezpieczeństwa, będą wiązały się z wykorzystaniem technik i technologii Big Data. Te uwagi dotyczą pojedynczego urządzenia IoFT, ale w wielu scenariuszach można wdrożyć więcej niż jedno urządzenie. Wraz ze wzrostem liczby podłączonych urządzeń adresowanie i zarządzanie nimi wszystkimi bez uszczerbku dla jakości usług staje się kwestią krytyczną. Sytuację pogarsza fakt, że nowe urządzenia oferujące lub żądające nowych usług mogą w każdej chwili dołączyć do sieci ad hoc. Dlatego aplikacje muszą być projektowane od podstaw, aby umożliwić rozszerzalne usługi i operacje. Co więcej, IoFT i WFANET mają do czynienia z częstym problemem, którym jest możliwa niedostępność usług związanych z połączeniem internetowym. Rodzi to pytania, np. jakie środki należy podjąć, jeśli LTE/3G/4G połączenie zostanie utracone bez uszczerbku dla misji i prywatności danych?

Problemy bezpieczeństwa w różnych warstwach koncepcyjnych Internetu rzeczy latających

Ogólnie rzecz biorąc, wyzwania związane z bezpieczeństwem są dużym problemem systemów komputerowych. Istnieje kilka problemów związanych z bezpieczeństwem, które mogą występować w aplikacjach opartych na IoFT, które są w większości dziedziczone z podstawowych sieci i technologii (np. UAS, IoT). Poniżej wymieniono główne problemy bezpieczeństwa, które mogą być nałożone przez różne warstwy sieci:

* Warstwa fizyczna. Zarówno ataki zagłuszania, jak i manipulacji są znanymi problemami dla tej warstwy. Zagłuszanie to dobrze znany atak, który powoduje zakłócenia częstotliwości radiowych, z których korzystają węzły sieci. Może przerywać sieć, jeśli w całej sieci używana jest jedna częstotliwość: w najgorszym przypadku przerywanie komunikacji z latającymi przedmiotami; a w najlepszym przypadku powodując nadmierne zużycie energii. Z drugiej strony, jeśli atakujący może fizycznie manipulować węzłami, ma miejsce atak manipulacji, który uszkadza, zastępuje i elektronicznie „przesłuchuje" węzły w celu uzyskania informacji. Ataki spoofingu GPS, które zdarzają się w tej warstwie, polegają na wykorzystaniu sygnału, który jest silniejszy i naśladuje atrybuty prawdziwego sygnału GPS do przejęcia odbiornika GPS. Takie ataki mogą spowodować całkowitą utratę kontroli nad samolotem, co jest bardzo krytycznym problemem.

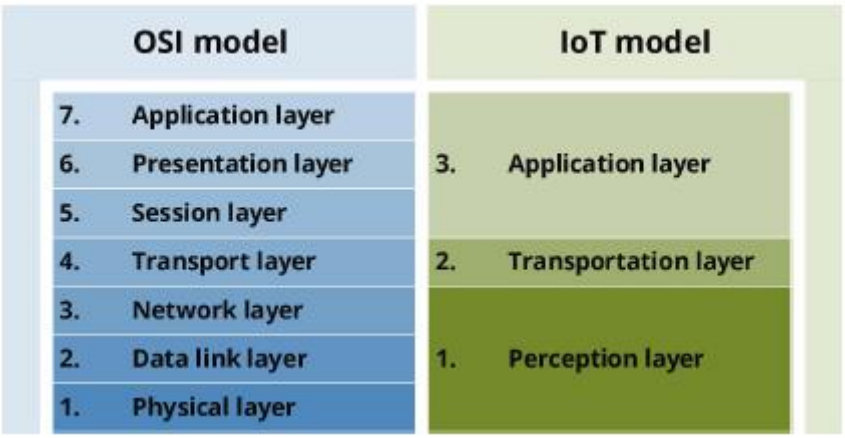
* Warstwa łącza danych. Kolizja, wyczerpanie i niesprawiedliwość to najbardziej prawdopodobne ataki na tym poziomie. Kolizja ma miejsce, gdy dwa węzły jednocześnie próbują transmitować na tej samej częstotliwości, co powoduje częściowe lub całkowite zakłócenie pakietu, co spowoduje błędną transmisję danych przez kanał komunikacyjny. W IoFT jest to duży problem, ponieważ możliwość wystąpienia nieciągłego stanu sieci może spowodować chaos w sieci FANET. Dlatego każda latająca rzecz może zostać naruszona i może zderzyć się ze sobą z powodu utraty informacji w locie. Jeśli dochodzi do powtarzających się kolizji, system może cierpieć z powodu wyczerpania zasobów, czyli ataku wyczerpania. Wreszcie, zamiast wprost blokować dostęp do usługi, atakujący może ją zdegradować, aby uzyskać przewagę, taką jak spowodowanie, że inne węzły w protokole MAC czasu rzeczywistego nie dotrzymają terminu transmisji, co charakteryzuje atak nieuczciwości.

* Warstwa sieci. Na tej warstwie znajduje się kilka ataków. W ataku selektywnego przekazywania złośliwe węzły próbują zatrzymać pakiety w sieci, odmawiając przesyłania dalej lub odrzucania

przechodzących przez nie wiadomości, co może zagrozić sieci FANET, która opiera się na strategicznie rozmieszczonych obiektach latających, aby dotrzeć do wszystkich miejsca docelowe w sieci. Jeśli atakujący sprawi, że skompromitowana latająca rzecz będzie wyglądać bardziej atrakcyjnie dla otaczających, co jest znacznie łatwym zadaniem, ponieważ aplikacje IoFT zwykle odbywają się w otwartych środowiskach, atak selektywnego przekazywania staje się bardzo prosty. Następnie, poprzez dotkniętą istotę latającą, może rozpocząć się sytuacja przesyłania danych, prowadząca do ataku dziury w zalewie. Innym atakiem na warstwę sieciową jest atak Sybil, w którym latający obiekt wykazuje wiele tożsamości w stosunku do innych latających obiektów w sieci. Z drugiej strony tunel czasoprzestrzenny to połączenie pozapasmowe między dwoma węzłami za pomocą łączy przewodowych lub bezprzewodowych, co może ułatwić przekazywanie pakietów szybciej niż normalnymi ścieżkami. Według Wallgrena , atak powodziowy HELLO odnosi się do nadpisania wiadomości „HELLO" poprzez nadawanie silniejszego sygnału, umożliwiając atakującemu przedstawienie się jako sąsiada wielu węzłów, prawdopodobnie całej sieci, co jest bardzo prawdopodobne w scenariuszach z lataniem rzeczy. Podczas pracy systemy komunikacyjne muszą równoważyć chęć maksymalizacji przepustowości (ilość danych przesyłanych w jednostce czasu – co sugeruje duże pakiety) i minimalizacji opóźnienia (maksymalne opóźnienie akceptowane dla przesyłanych i odbieranych danych – co sugeruje małe pakiety). Ostatnim problemem w przypadku wdrażania wielu urządzeń jest to, że węzły w sieciach FANET mogą być stałe lub nie, a odległość między węzłami może się zmieniać podczas ruchu. Aby zapewnić trasę między węzłami, sieci FANET opierają się na technikach rozgłoszeniowych, co staje się problemem, który można interpretować jako atak na system komunikacyjny: rosnący ruch danych między obiektami latającymi a elementami infrastruktury IoFT; rosnąca liczba załogowych statków powietrznych korzystających z tej samej przestrzeni powietrznej; oraz postępujące nadejście latających obiektów w celu zakwestionowania niesegregowanej przestrzeni powietrznej. Aby rozwiązać problem pakietów rozgłoszeniowych do wszystkich węzłów i uniknąć nadmiarowości pakietów i związanych z nią problemów (tj. Broadcast Storm Problem - BSP), należy wziąć pod uwagę techniki łagodzenia BSP

* Warstwa transportowa. Atak typu Flooding powoduje ogromny ruch bezużytecznych wiadomości w sieci. Może to skutkować przeciążeniem i ostatecznie doprowadzić do wyczerpania węzłów . Atak desynchronizacji jest wykonywany, gdy przeciwnik powtarza komunikaty, które przekazują numery sekwencyjne do jednego lub obu punktów końcowych. Spoofing GPS może pomóc atakującym w porwaniu latających rzeczy, co jest kolejnym problemem silnie związanym z sytuacjami, w których atakujący potajemnie przekazuje i prawdopodobnie zmienia komunikację między dwiema stronami, co jest również znane jako ataki typu man-in-the-middle. Ten rodzaj ataku umożliwia atakującemu wylądowanie latającego obiektu w nieautoryzowanym miejscu i wykorzystanie jego legalnego dostępu do sieci. Jednak taki problem może zostać zneutralizowany przez wysoką łączność w środowiskach IoFT: W większości przypadków rozwiązaniem są techniki sprawdzające dokładność sygnałów GPS poprzez porównanie z tymi dostarczanymi przez punkty dostępowe i inne znane stałe infrastruktury.

Z innego punktu widzenia niektórzy badacze zorganizowali IoT w nowej architekturze bezpieczeństwa, która ma również zastosowanie do IoFT. Taka architektura dzieli się głównie na trzy warstwy: percepcję, transport i zastosowanie. Ta organizacja z trzema warstwami implementuje tylko większość cech modelu Open Systems Interconnection (model OSI), mimo że nie jest tak dobrze rozdzielona. Rysunek przedstawia porównanie modelu IoT zaproponowanego przez Jinga i model OSI.



Każda warstwa modelu IoT stoi przed konkretnymi wyzwaniami, które zostaną omówione dalej.

* Warstwa percepcji. Ta warstwa dotyczy głównie gromadzenia informacji, postrzegania obiektów i kontroli obiektów. W warstwie percepcyjnej w ramach Internetu Rzeczy Latających będą wykonywane zadania związane z bezpieczeństwem RFID (identyfikacja radiowa), WSN, RSN (RFID Sensor Network), technologią GPS itp. Niejednorodność obiektów latających i zwykłych urządzeń obsługujących IoT/IoFT jest jednym z głównych problemów, które mogą pojawić się w tej warstwie, co może prowadzić do problemów z kompatybilnością. Inną kwestią jest ograniczenie mocy, zdolności obliczeniowych i pojemności pamięci, zwłaszcza w przypadku rzeczy latających, co czyni je bardziej podatnymi na ataki, co pozwala na fizyczną kradzież informacji, a także modyfikację funkcjonowania

* Warstwa transportowa. Nazywana również warstwą sieciową, główną funkcją warstwy transportowej jest przesyłanie informacji uzyskanych z warstwy percepcyjnej . Ta warstwa obejmuje Wi-Fi, tworzenie i utrzymywanie sieci MANET/FANET i 3G/4G/5G, co prowadzi do problemu heterogeniczności wymiany informacji między różnymi sieciami, co jest jeszcze większym wyzwaniem, jeśli chodzi o IoFT i jego nieodłączną cechę. integracja między różnymi sieciami (IoT, FANET).Ponadto prowadzi to również do nowych luk w odpowiednich segmentach dla implementacji sieci IoFT. Na przykład główne problemy związane z Wi-Fi to ataki typu phishing, złośliwe punkty dostępu, ataki DDoS/DoS i tak dalej. Po stronie MANET/FANET problemy związane z bezpieczeństwem, które można napotkać, to bezpieczeństwo danych, routing sieciowy i problemy z atakami DDos/DoS. Wreszcie, w odniesieniu do sieci 3G/4G/5G głównym problemem jest bezpieczeństwo danych i bezprawne ataki.

* Warstwa aplikacji. Warstwa ta obsługuje wszelkiego rodzaju usługi biznesowe i realizuje inteligentne obliczenia oraz alokację zasobów podczas przeszukiwania, wybierania, wytwarzania i przetwarzania danych. Problemów bezpieczeństwa, z jakimi się boryka, nie da się rozwiązać w innych warstwach modelu IoT, takich jak kwestia ochrony prywatności, która może stać się prawdziwym wyzwaniem w pewnych szczególnych kontekstach. Dlatego w działaniu warstwa wsparcia aplikacji musi być w stanie rozpoznawać niezaufane dane (np. dane spamowe i złośliwe dane) i filtrować je w czasie rzeczywistym. Warstwa aplikacji może być zorganizowana na różne sposoby w zależności od różnych usług i zwykle obejmuje oprogramowanie pośrednie, M2M, platformę przetwarzania w chmurze i platformę wsparcia usług. Kwestie prywatności w latających przedmiotach zostały ostatnio omówione jako duże zagrożenie, ponieważ systemy pamięci masowej stają się coraz bardziej wyrafinowane. Istnieje tendencja do przechowywania jak największej ilości rzeczy w pamięci latającej rzeczy, co gwarantuje, że potrzebne informacje są zawsze dostępne. Jednak takie podejście okazuje się być bardzo krytycznym zagrożeniem bezpieczeństwa. Ponieważ latająca rzecz jest umieszczona w wysoce połączonym środowisku, może zostać fizycznie skradziona lub może przejąć kontrolę. W ten sposób atakujący może nadal używać go jako bramy do uzyskania informacji z sieci, ponieważ latający obiekt jest autoryzowany

i będzie mógł uzyskać dostęp do prywatnych i poufnych informacji. Jest to konsekwencja wysokiej łączności rzeczy i zwiększonej powierzchni kontaktu, która generuje więcej możliwych zagrożeń, które mogą zostać zbadane przez złośliwe podmioty.

Kwestie bezpieczeństwa Internetu rzeczy latających

Rosnąca popularyzacja UAV zwiększyła badania w tej dziedzinie i sprzyja wykorzystywaniu takiej technologii w wielu zastosowaniach. Istnieją mapy drogowe publikowane okresowo przez organizacje wojskowe i cywilne – na przykład Armię Stanów Zjednoczonych (Armia Stanów Zjednoczonych), Amerykański Departament Obrony (DoD), Europejską Grupę Sterującą RPAS (ERSG) oraz Federalną Administrację Lotnictwa (FAA) – które określają oczekiwane zaliczki na bezzałogowe statki powietrzne (US Army, 2010; Yearbook, 2011; UK Civil Aviation Authority, 2012; DoD, 2013). Nie ma jednak wystarczającej liczby badań dotyczących bezpieczeństwa dla konkretnej integracji UAV i IoT, co jest jednym z najważniejszych tematów do dyskusji i otwartą szansą dla badań nad systemami krytycznymi dla bezpieczeństwa. Istnieje pięć wyzwań związanych z integracją UAS, jak stwierdził dr Wilson Felder, dyrektor Centrum Technicznego FAA Williama J. Hughesa, zgłoszony przez Starka: proceduralne, techniczne, bezpieczeństwo statku powietrznego, referencje załogi i akceptacja społeczna. Systemy wykrywania i unikania pozostają jedną z największych przeszkód w bezpiecznej integracji UAS z przestrzenią powietrzną. Każda osoba lub system komputerowy, który spełnia trzy obowiązkowe czynności związane z obsługą statku powietrznego (lot, nawigacja i łączność), powinien przejąć dowodzenie nad statkiem powietrznym, zarówno załogowym, jak i bezzałogowym). Przepisy dotyczące wykrywania i rozwiązywania kolizji muszą być spełnione przez każdy bezzałogowy statek powietrzny zaprojektowany dla niesegregowanej przestrzeni powietrznej. Krótko mówiąc, wymagania FAA wymagają, aby bezzałogowe systemy powietrzne spełniały poziomy bezpieczeństwa równoważne z załogowymi statkami powietrznymi. Obejmuje częstotliwość kolizji UAS eksploatowanego w przestrzeni powietrznej kontrolowanej przez FAA, która obecnie wynosi 1×10^{-7} zdarzeń na godzinę operacji załogowych statków powietrznych Jeśli chodzi o zastosowania IoFT, pojawią się podejścia łączone, które mogą obejmować zarówno załogowe, jak i bezzałogowe statki powietrzne jednocześnie, prowadząc do konieczności korzystania z niesegregowanej przestrzeni powietrznej. Fakt ten zwiększa potrzebę spełnienia wymagań bezpieczeństwa, a pierwszym krokiem jest ich wskazanie i omówienie możliwych rozwiązań.

Pomimo zabezpieczenia zastosowanego do każdej warstwy, istnieje również potrzeba znalezienia wspólnych podejść, które zapewnią bezpieczeństwo indywidualnie i zbiorowo. Ograniczenie naruszeń we wszystkich warstwach w konsekwencji zmniejszy ogólne szanse ataków na sieć. Takie cechy dotyczące bezpieczeństwa i bezpieczeństwa utrudniają zapewnienie bezpieczeństwa systemu, stanowiąc jedno z głównych zagrożeń w tym obszarze, jakim jest znalezienie podejść zajmujących się obydwoma koncepcjami jednocześnie. Pojęcie bezpieczeństwa ma długą tradycję dla pojazdów (ISO, 2011). Jest to dojrzały obszar i istnieje kilka standardów tworzenia bezpiecznych systemów, takich jak RTCA/DO-178C dla oprogramowania UAV (RTCA Inc., 2011) i RTCA/DO-254 dla sprzętu UAV (RTCA Inc., 2000). Bezpieczeństwo dotyczy minimalizacji częstotliwości wypadków lub awarii w systemie, głównie związanych z utratą życia, o dużej wartości aktywa i wiąże się z nieostrożnymi działaniami lub zdarzeniami. Zapewnienie bezpiecznej komunikacji bezprzewodowej oznacza zapewnienie, że przesyłane informacje są odbierane bez błędów transmisji i utraty informacji. Z powodu szumów, zakłóceń i efektów zanikania sieć bezprzewodowa nie może mieć zerowego błędu transmisji, ponieważ nie ma systemu o zerowym ryzyku. W przypadku sieci bezprzewodowej nie da się uniknąć błędów transmisji i utraty informacji, ale można je przezwyciężyć, zmniejszając je lub wykrywając. W celu zagwarantowania komunikacji z bezpieczeństwem, Pendli wymienił szereg wymagań, które muszą być spełnione. Łącza komunikacyjne powinny być niezawodne i odporne na zakłócenia, zagłuszanie,

zakłócenia i efekty zaniku, aby zapewnić łącze bez błędów i strat. Ponieważ latające rzeczy są systemami krytycznymi dla bezpieczeństwa, kanały komunikacji muszą być stale dostępne i bezawaryjnie dostarczać informacje na czas. Zapewnienie wydajności w czasie rzeczywistym oznacza, że stosowana technologia musi uwzględniać opóźnienia podczas transmisji i retransmisji informacji oraz być w stanie poradzić sobie z błędami serii. Mobilność urządzeń i zmieniające się środowisko zewnętrzne wymagają, aby łącza komunikacyjne były niezawodne nawet w niesprzyjających warunkach przeciwko zanikowi kanału, niskim SNR (stosunek sygnału do szumu) i stratom w kanale. Ogólnie rzecz biorąc, w przypadku pojazdów latających istnieją wymagania prawne i prawne, które wymagają uwzględnienia wszelkich czynników wpływających na bezpieczeństwo i włączenia ich do modelu ryzyka spełniającego określone minimalne standardy przed przyznaniem certyfikacji. W przypadku urządzeń IoFT należy uwzględnić możliwe współczynniki awaryjności rozwiązań wszystkich podsumowanych problemów komunikacyjnych. Rzeczywiście, w niektórych zastosowaniach, w których latające urządzenie działa nad miastami lub farmami, które są dziedzinami krytycznymi, potrzeba certyfikacji jest jeszcze wyższa. Chociaż jest jeszcze do zrobienia, mamy nadzieję, że solidność infrastruktury IoT może pomóc w osiągnięciu wymaganych niskich współczynników awaryjności. Krótko mówiąc, twórcy i użytkownicy systemów IoFT muszą traktować bezpieczeństwo jako jeden z głównych problemów. Jednak połączenie wysokiej mobilności i komunikacji bezprzewodowej znacznie zwiększa narażenie tych systemów na złośliwe zagrożenia i błędy wynikające z niepewnej łączności lub terminowości komunikacji. Wymagania niefunkcjonalne, takie jak bezpieczeństwo, stały się tym samym trudniejsze do spełnienia, tworząc nowe wyzwania dla takich systemów wbudowanych o krytycznym znaczeniu dla bezpieczeństwa. W rzeczywistości należy przeprowadzić dalsze badania nad rozwojem i zapewnieniem bezpieczeństwa i ochrony, zajmując się potrzebami multidyscyplinarnych podejść, takich jak zintegrowane systemy sterowania, komunikacja, mechanizmy bezpieczeństwa, sztuczna inteligencja, sieci neuronowe, zasoby bezpieczeństwa i inne problemy technologiczne. Kluczowym wyzwaniem jest to, że rozwiązania architektoniczne zapewniające bezpieczeństwo mogą otwierać kolejne słabości z punktu widzenia bezpieczeństwa. Z drugiej strony, słabości zabezpieczeń mogą prowadzić, jeśli zostaną wykorzystane przez atakujących, do naruszeń bezpieczeństwa, a wdrożenie danego mechanizmu bezpieczeństwa może wpłynąć na bezpieczeństwo. W nielicznych przypadkach, w których brane jest pod uwagę bezpieczeństwo, jedynym problemem, który jest rozwiązywany, jest komunikacja w otwartej sieci, np. systemy bezprzewodowe. Bezpieczeństwo w ogóle nie jest obsługiwane (lub obsługiwane w bardzo ogólny sposób) bez pełnego wsparcia w identyfikacji i łagodzeniu zagrożeń bezpieczeństwa. Dlatego związek między bezpieczeństwem a ochroną wydaje się być nadal otwartą kwestią w społeczności.

Studium przypadku

W tej sekcji zostaną przeprowadzone trzy studia przypadków ilustrujące rzeczywiste zastosowania Internetu rzeczy latających. Pierwszy dotyczy inteligentnych farm, podkreślających zastosowanie WFANET. Drugi dotyczy zapewnienia dostępu do Internetu i usług opartych na IoT na odległych obszarach, zwłaszcza na obszarach wiejskich i peryferiach inteligentnych miast. Wreszcie trzecie studium przypadku dotyczy zarządzania dużymi wydarzeniami i świadczenia ukierunkowanych usług.

Studium przypadku 1: Sieci WFANET do zadań nadzoru w inteligentnych gospodarstwach. Farmy o powierzchni setek hektarów o zróżnicowanej topologii mogą być tworzone i poddawane różnym warunkom klimatycznym na swoim obszarze. Mogą wykonywać wiele różnych zadań w rolnictwie, takich jak hodowla zwierząt, stając się wyspecjalizowanymi jednostkami (np. Gospodarstwo warzywne lub sadownicze, nabiał, ferma trzody chlewnej i drobiu, a nawet wykorzystywane do produkcji włókien naturalnych, biopaliw i innych towarów). Wszystkie z nich mają również dużą infrastrukturę, która może obejmować plantacje, pastwiska, pastwiska, sady, szklarnie, silosy, stodoły i inne budynki oraz

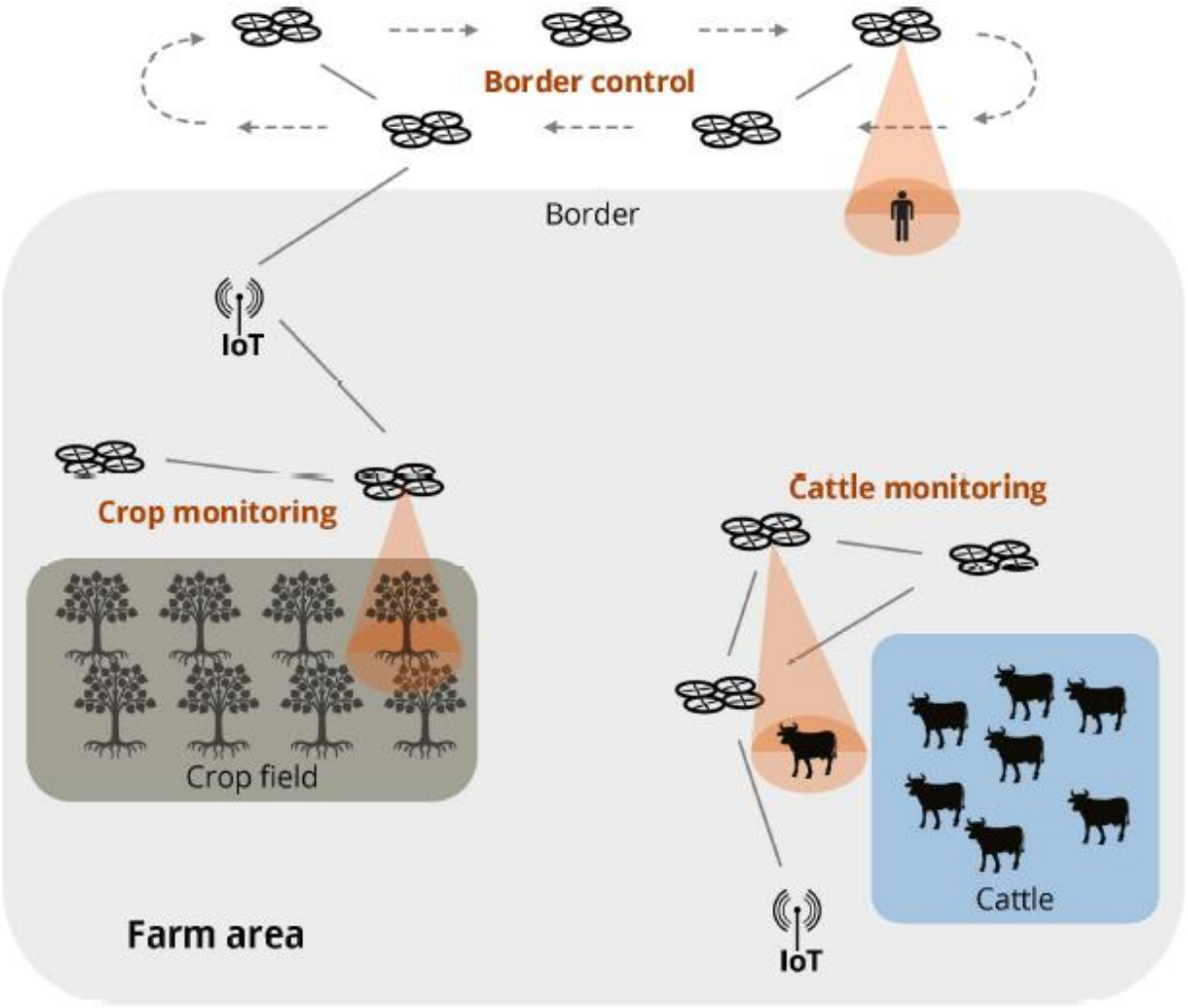
gospodarstwo rolne. W dzisiejszych czasach termin ten został rozszerzony o działalność przemysłową, taką jak farmy wiatrowe i farmy rybne, które mogą działać zarówno na lądzie, jak i na morzu. Aby uzyskać więcej informacji na temat różnych zastosowań IoT w rolnictwie, zapoznaj się z rozdziałem 18. Pojęcie inteligentnych farm jest używane do określenia wszechobecnego środowiska farmy gotowego do IoT w celu zwiększenia ogólnej produktywności i optymalizacji codziennych zadań. Łączność z Internetem można uzyskać w takich środowiskach głównie w strategicznych budynkach administracyjnych, ale także w niektórych dedykowanych dziedzinach, w których znajdują się wyspecjalizowane technologie wykrywania i monitorowania. Niniejsze studium przypadku analizuje scenariusz z perspektywy IoFT poprzez zastosowanie sieci Wide-FANET. Koncepcja Wide-FANET to sieć ad hoc, która korzysta z połączenia z infrastrukturą IoT już dostępną dzięki pobliskim inteligentnym środowiskom. Takie połączenie może zapewnić szerokopasmowy dostęp do Internetu lokalnym sieciom FANET, a następnie można utworzyć tunel do wymiany informacji i współpracy między zdalnymi sieciami FANET. Więcej niż jedna latająca sieć ad hoc z różnych lokalizacji geograficznych połączona przez przezroczyste tunelowanie w chmurze składa się z sieci WFANET.

Problem

Chociaż inteligentne farmy już czerpią korzyści z IoT, nadal mają ograniczoną łączność z Internetem, co zwykle prowadzi do dużych obszarów bez łączności i bez nadzoru. Tak więc struktury sieciowe, które nie zależą od połączeń internetowych, zostały zastosowane jako tymczasowa alternatywa do monitorowania zwierząt, pól uprawnych, lasów, ławic ryb i tak dalej. Często spotyka się WSN i bezprzewodowe sieci ciała (WBAN) rozproszone na wielu polach. Jednak informacje zwrotne z tych sieci i czujników są często ograniczone, opóźnione i słabo aktualizowane, co prowadzi do mniej dynamicznych operacji i ograniczonego ogólnego zarządzania gospodarstwem. Problem poruszany w niniejszym studium przypadku związany jest z ogólnym nadzorem inteligentnego gospodarstwa, w tym granice gospodarstwa, kontrolowane bydło lub podejrzane działania na polu gospodarstwa. Takie problemy stają się coraz większe i bardziej złożone w zależności od wielkości gospodarstwa, a także ze względu na liczbę różnych zadań wymagających monitorowania ze względów bezpieczeństwa. Można je również uznać za krytyczne, ponieważ zagrożone są aktywa o wysokiej wartości.

Proponowane rozwiązania

Poniższe tematy omówią hipotetyczne zastosowanie FANET i WFANET w trzech scenariuszach gospodarstw: kontrola graniczna, monitorowanie bydła i monitorowanie upraw. Rysunek 19.9 ilustruje scenariusze omówione w dalszej części.



Jednym z najważniejszych zadań z punktu widzenia bezpieczeństwa jest nadzorowanie granic farmy w celu zidentyfikowania potencjalnych zagrożeń, takich jak intruzi (ludzie lub nie) i uruchomienie odpowiednich procedur. W typowym scenariuszu zadanie będzie wykonywane przez ludzkie patrole i/lub kamery monitorujące. To rozwiązanie, oprócz kosztownych, prawdopodobnie nie będzie skuteczne, ponieważ ryzyko ludzkiej porażki jest zawsze obecne. WFANET zapewniłby kontrolę granic przy niższych kosztach. UAV zyskałyby dzięki dostępnej infrastrukturze IoT, aby dostarczać obrazy lub dane z monitoringu w czasie rzeczywistym do centrali kontroli (np. dla ochroniarzy, wyspecjalizowanej firmy ochroniarskiej lub komisariatu policji). Zastosowanie bezzałogowych statków powietrznych ograniczyłoby konieczność instalowania kamer monitorujących nad granicami nieruchomości i wymaganą jej infrastrukturę (np. baterie czy ogniwa słoneczne do zasilania), co ponownie obniżyłoby koszt zadania. Korzyści byłyby jeszcze większe w przypadku większych gospodarstw, ponieważ wykorzystanie sieci WFANET umożliwiłoby wymianę istotnych informacji między więcej niż jednym lokalnym systemem FANET, w ramach wspólnego monitorowania granic na żywo. Ponadto dane z oficjalnych rządowych serwisów internetowych mogą być wykorzystywane do identyfikacji zbiegów. Inna sytuacja związana jest z monitoringiem bydła. W dużych gospodarstwach normalne jest wyznaczanie strategicznych powierzchni gruntów przeznaczonych pod hodowlę bydła. Takie obszary muszą być stale monitorowane, aby uniknąć ucieczek lub nieuprawnionej interwencji człowieka. Po raz kolejny, jeśli rozwiązanie opiera się na zasobach ludzkich, zakres monitoringu może być nieskuteczny lub być zbyt powolny, aby podjąć odpowiednie działania z niewielkimi szkodami dla bydła lub innych

pól gospodarskich. Infrastruktura IoT zapewniłaby środki do śledzenia bydła poprzez instalowanie tanich czujników w każdym pojedynczym zwierzęciu. Co więcej, dzięki badaniu terenu za pomocą UAV, akwizycja danych szybko przepłynęłaby z obszaru hodowli bydła do centrów monitoringu, zapewniając środki do podejmowania terminowych działań. Alternatywnie, automatyczne działania mogą również mieć miejsce, gdy tylko zostanie zidentyfikowane niepożądane zachowanie, na przykład zamknięcie bram zapasowych w przypadku ucieczki bydła. W tym celu sieci FANET (na małych obszarach) lub WFANET (na większych obszarach) identyfikują i uruchamiają odpowiednie działania. Nadzór pól uprawnych może być motywowany kilkoma czynnikami, takimi jak wczesna identyfikacja szkodników i plag, sprawdzanie gleby i monitorowanie warunków pogodowych. Po raz kolejny odpowiednie działania lokalne mogą mieć miejsce, gdy tylko zostanie zidentyfikowana nietypowa sytuacja. W takim przypadku dokładniejsze informacje można uzyskać, rozpoczynając specjalistyczne misje z wykorzystaniem FANET i/lub WFANET w oparciu o dodatkowe informacje wymagane do precyzyjnego rozpoznania środka zaradczego2,3. UAV mogą zbierać dane z bezprzewodowych sieci czujników umieszczonych na ziemi na strategicznej częstotliwości, mogąc przesyłać takie dane w czasie rzeczywistym do centrów monitoringu. Co więcej, taka częstotliwość zbierania danych może opierać się na warunkach pogodowych, pochodzących zarówno z lokalnych czujników, jak i usług internetowych.

Studium przypadku 2: Dostęp do Internetu i świadczenie usług IoT w obszarach odległych i peryferyjnych z IoFT jako czynnikiem przeciwmgielnym.

Obszary wiejskie i peryferia miast mogą być najtrudniejszymi obszarami do świadczenia usług opartych na Internecie/IoT, zwłaszcza ze względu na brak odpowiedniej infrastruktury. W większości przypadków nie warto instalować pełnej infrastruktury, która będzie rzadko wykorzystywana na odległych obszarach. Co więcej, ponieważ popyt jest zwykle niski, rząd i firmy nie będą zainteresowane aktualizacją takiej infrastruktury w celu dostosowania do wymagań najnowszych technologii. Z drugiej strony zdarzają się sytuacje, w których wsparcie usług opartych na Internecie/IoT pozytywnie poprawiłoby zadania związane z poszukiwaniami i ratownictwem, poziomami jakości życia, wydarzeniami specjalnymi, śledzeniem osób/obiektów i tak dalej. W niniejszym studium przypadku zbadane zostaną korzyści płynące z wykorzystania Internetu rzeczy latających do zwiększenia zasięgu powszechnych usług inteligentnych miast. W ten sposób istnieje potencjalna możliwość zapewnienia łączności internetowej i usług opartych na IoT w celu tymczasowego usprawnienia zadań specjalnych w niedrogi sposób.

Problem

Śródmieście inteligentnego miasta prawdopodobnie będzie regionem geograficznym, który jako pierwszy doświadczy nowatorskich wysiłków i zaktualizowanych technologii, podczas gdy peryferia będą zwykle ostatnimi, które staną w obliczu pełnej integracji, a także pozyskają odpowiednie inwestycje. Jest to naturalny proces, biorąc pod uwagę model biznesowy pełen potencjalnych możliwości, który skupia się na gęsto zaludnionych obszarach, aby był rentowny. W innym kontekście obszary wiejskie mogą nie potrzebować przez cały czas łączności z Internetem, ale na pewnym etapie muszą aktualizować/synchronizować dane. W tym celu mule danych mogą być stosowane na przykład w pojazdach, które fizycznie przewożą komputery z dedykowanymi serwerami pamięci masowej, pozwalającymi na powolną, ograniczoną synchronizację raz dziennie. Chociaż takie podejście można w wielu sytuacjach uznać za niedrogie i wydajne, jest ono mało elastyczne i nie zapewnia korzyści z w pełni połączonej infrastruktury. Ten sam problem występuje w sytuacjach awaryjnych, na przykład w poszukiwaniach i ratownictwie. Infrastruktura sieci lokalnej nie zapewnia wsparcia w czasie rzeczywistym, którego taka operacja byłaby potrzebna do prawidłowego i wydajnego wykonywania zadań poszukiwawczych, a także ratowniczych. W niektórych przypadkach brak zasięgu sieci

komórkowej jeszcze bardziej ogranicza łączność, co prowadzi do konieczności elastycznego, niedrogiego i łatwego w konfiguracji podejścia. Wobec tych kwestii paradygmat IoFT może być odpowiednią alternatywą czasowej lub trwałej minimalizacji omówionych już problemów. W następnym podrozdziale zostaną omówione proponowane rozwiązania dla powtarzających się przypadków, pokazując, jak ten paradygmat rozwiązałby przypadki praktyczne.

Proponowane rozwiązania

W tym miejscu zostaną przedstawione trzy główne zastosowania tego studium przypadku. Pierwsza dotyczy znaczenia sieci IoFT dla peryferii inteligentnych miast. Drugi dotyczy monitoringu środowiska na obszarach wiejskich, który pomaga policji środowiskowej w identyfikowaniu nielegalnych działań i podejmowaniu odpowiednich środków zaradczych. Na koniec omówiono zjawiska naturalne i wsparcie operacji kryzysowych, biorąc pod uwagę, że w takich sytuacjach łączność staje się problemem ze względu na utratę pobliskiej infrastruktury. Rysunek 19.10 ilustruje scenariusze, które zostaną omówione dalej. Dzięki strategicznemu przenoszeniu dronów na obrzeża inteligentnych miast, potężne połączenie z Internetem będzie dostępne dla obszarów o ograniczonym dostępie, pomagając w zapewnieniu łączności z peryferiami miast. Z tego połączenia, a pełna gama usług IoFT będzie dostępna dla użytkowników końcowych w pobliżu przez określony czas, umożliwiając realizację odpowiednich zadań. Na przykład firma elektroenergetyczna inteligentnego miasta może zautomatyzować proces odczytu zużycia energii w mieszkaniu. Takie zadanie zwykle wykonuje osoba notująca zużycie w każdym mieszkaniu/budynku, co zajmuje więcej czasu i jest podatne na błędne odczytanie. Zastosowanie odpowiednich identyfikatorów do każdego mieszkania (np. tagów RFID), które z kolei będą rozpoznawalne przez infrastrukturę IoFT, umożliwiłoby odczytanie zużycia energii na dużym obszarze w ciągu kilku minut. Jest to możliwe dzięki istnieniu nad terenem latającego FANET/WFANET, świadczącego taką klasę usług i będącego w stanie dostarczyć informacje w czasie rzeczywistym zarówno klientowi (np. ostrzeżenia o złym długu), jak i firmie energetycznej (np. czytelnictwo w konkretnych rezydencjach, które wymagałyby wizyty technicznej). Co więcej, istnienie jednego latającego obiektu lub FANET/WFANET nad dzielnicą, która nie jest jeszcze wyposażona w infrastrukturę inteligentnego miasta, może być wykorzystane jako wsparcie ruchu dla kierowców w tych regionach. Inteligentne samochody skorzystałyby z ostrzeżeń IoFT o ruchu drogowym. Zwykłe samochody mogą również otrzymywać ważne informacje o ruchu drogowym za pośrednictwem smartfonów podłączonych do infrastruktury IoFT. Takie działania przyczyniłyby się do bezpieczniejszego i dokładniejszego korzystania z ulic, nie wspominając o sytuacjach awaryjnych, które mogłyby mieć miejsce, i w pełni skorzystałyby z infrastruktury IoFT. Obszary wiejskie zwykle nie wymagają stałego dostępu do Internetu. W niektórych przypadkach można wykorzystać mule danych, które umożliwiają przesyłanie danych między odległymi lokalizacjami w celu efektywnego tworzenia łącza transmisji danych. Podobnie sieć IoFT może być stworzona do przesyłania danych do pożądanej lokalizacji, ale z przerywanym łączem zapewnianym przez mobilną sieć ad hoc łączącą miasto i odległy obszar. Pojęcie mgły obliczeniowej jest w tej sytuacji jasne, ale sieć IoFT wyłania się jako czynnik umożliwiający model. W sekcji 19.3.1 omówiono zastosowanie UAV jako infrastruktury obliczeniowej mgły przy użyciu elementów IoFT w celu zapewnienia zaktualizowanego, elastycznego rozwiązania. Taka aplikacja dobrze pasuje do obszarów wiejskich, które potrzebują lepszego świadczenia usług do wykonywania bardziej zaawansowanych zadań. Model ten spełnia również wymogi monitoringu środowiska przez oficjalne agencje rządowe, co jest trendem ze względu na zgłaszane ostatnio problemy globalne. Monitorowanie w czasie rzeczywistym za pomocą latających rzeczy może być zdalnie analizowane przez specjalistów w centralach, którzy będą mogli wykorzystać aktualne obrazy do identyfikacji podejrzanych działań. Jeśli ma miejsce nielegalna praktyka środowiskowa, policja środowiskowa może natychmiast przenieść się do regionu, który jest wspierany przez infrastrukturę IoFT przez cały czas, umożliwiając wydajną pracę na gorącym uczynku.

Sytuacja częsta również na obszarach oddalonych jest związana ze zjawiskami naturalnymi i wsparciem operacji kryzysowych. Klęski żywiołowe i sytuacje katastroficzne można przewidzieć, ale zwykle nie da się ich kontrolować. Ich zniszczenie może doprowadzić do niedostępności podstawowych usług infrastruktury lokalnej, takiej jak sieci komórkowe, powodując chaos. Zastosowanie IoFT w celu zapewnienia środków łączności z centrum miasta przez sieć FANET, która dociera do obszaru katastrofy, może być skutecznym tymczasowym działaniem wspierającym ratowników w wykonywaniu ich pracy tak, jak to tylko możliwe. Na przykład, jeśli katastrofa doprowadziła do śmierci, można rozważyć rozpoznawanie ciał w czasie rzeczywistym przez krewnych. Jednak transport ludzi na teren katastrofy nie zawsze jest bezpieczny lub właściwy. Ponadto w niektórych sytuacjach nie jest możliwe natychmiastowe usunięcie wszystkich ciał, co powoduje panikę i ludzi zalewanych telefonami z żądaniem informacji. IoFT w sytuacjach awaryjnych zapewni łączność w celu świadczenia podstawowych usług, centralnych urzędów rządowych i agencji prasowych, które będą aktualizowane o najnowsze odkrycia, a także pełne wsparcie dla karetek pogotowia ratunkowego przewożonych do obszaru docelowego.

Studium przypadku 3: Ukierunkowane świadczenie usług podczas dużych wydarzeń dzięki IoFT

Wielkie imprezy odbywają się przez cały rok w zasadzie wszędzie. Mogą być różnego rodzaju, takie jak lokalne wystawy, duże prezentacje teatralne i setki jednoczesnych koncertów i prezentacji w kilku różnych miejscach festiwalu muzycznego. Te duże wydarzenia mogą być zatłoczone przez ludzi przyjeżdżających z wielu miejsc z różnymi wymaganiami dostępności. Ogólne bezpieczeństwo to kwestia, którą może wspomóc infrastruktura IoFT, zwłaszcza gdy wydarzenie odbywa się w odległej lokalizacji (np. gigantyczne festiwale muzyczne). Jest to podobne do sytuacji opisanej w Studium przypadku 1, kiedy mogą być wymagane zadania nadzoru. Jednak to studium przypadku skupi się na dostarczaniu ukierunkowanych usług na potrzeby dużych wydarzeń zapewnianych przez sieci IoFT.

Problem

W przypadku dużych imprez jednym z najbardziej niepokojących problemów jest utrata ludzi, zwłaszcza dzieci. Czasami sygnał sieci komórkowej nie będzie dostępny, a znalezienie kogoś w zatłoczonym miejscu jest prawie niewykonalną misją dla jednej osoby. Co więcej, ze względu na dużą liczbę osób, ciężko jest przemieszczać się z miejsca na miejsce, aby sprawdzić, czy zaczął grać Twój ulubiony zespół lub czy niedługo skończy się nudna prezentacja. Są to pożądane informacje, które zwykle są niedostępne lub częściowo dostępne w przewodnikach papierowych, które mogą stać się nieaktualne w ciągu kilku minut.

Proponowane rozwiązania

Możliwość zastosowania IoFT w przytoczonych sytuacjach może być prostym i skutecznym rozwiązaniem. Poniższe podrozdziały omówią konkretnie dwa przypadki. Najpierw zostanie omówiona aplikacja znajdowania osób. Po drugie, zostaną omówione informacje w czasie rzeczywistym o wielu miejscach festiwali muzycznych. Rysunek 19.11 przedstawia scenariusz tego studium przypadku. Często zdarza się, że w zatłoczonych miejscach nagle zostajesz oddzielony od przyjaciół lub rodziny. Jeśli sieć komórkowa jest niedostępna z jakiegoś powodu lub w telefonie rozładuje się bateria, możesz mieć problem. Co więcej, sytuacja staje się jeszcze gorsza, jeśli dziecko z jakiegoś powodu ginie, a rodzice desperacko go szukają. Identyfikacja osób za pomocą kamer stacjonarnych połączonych z infrastrukturą obiektów jest w większości przypadków skuteczna. Jednak w zatłoczonych miejscach kąt kamery może być problemem. W przypadku zagubionych dzieci jest to tym bardziej problematyczne, że wysokość wpłynęłaby negatywnie na zasięg kamery. W takich przypadkach rozsądnym rozwiązaniem byłaby latająca rzecz podłączona do FANET/WFANET w celu dokładnego, szybkiego wyszukiwania na miejscu. Transmisja w czasie rzeczywistym może być monitorowana przez

przeszkolone osoby, a także krewnych. Taki wysiłek znacznie zmniejszyłby szanse na zranienie pozostawionego bez opieki dziecka, a także zapewniłby skuteczne środki wspierające rodziny. Innym istotnym tematem w przypadku dużych wydarzeń, szczególnie tych, w których atrakcje odbywają się jednocześnie w wielu miejscach, jest możliwość uzyskania dostępu do informacji w czasie rzeczywistym. Można się zastanawiać, czy koncert przeznaczony na konkretną godzinę rozpoczął się, czy jest opóźniony. Co więcej, dlaczego nie mieć dostępu do transmisji strumieniowej audio lub wideo, aby sprawdzić, jak idzie wydajność lub jak jest zatłoczona? Sieć IoFT wraz z kamerami stacjonarnymi i czujnikami może dostarczać zestaw informacji o wielu obiektach w czasie rzeczywistym do centralnego serwera, który redystrybuowałby takie informacje w całej sieci. Osobiste smartfony lub specjalne stacje mogłyby uzyskać dostęp do takich informacji, usprawniając świadczone usługi w dniach imprezy.

Wnioski

Internet of Flying Things integruje latające rzeczy z paradygmatem Internetu Rzeczy. Ta nowa koncepcja zwiększa współpracę i współpracę między UAV, zwiększając zasięg sieci i stwarzając nowe możliwości zastosowań UAS, takich jak interaktywne podejmowanie decyzji. W kontekście IoT świadomość podstawowych cech latających obiektów, takich jak możliwości, cele i ograniczenia, jest kluczowym czynnikiem określającym, na ile kwalifikują się one do wykonywania skomplikowanych misji i jak prawdopodobne jest ich zintegrowanie z Internetem Rzeczy. Pomimo faktu, że latające rzeczy mogą być traktowane jako ogólne węzły w paradygmacie IoFT, opracowanie konkretnych podejść może pomóc w osiągnięciu bardziej zoptymalizowanych, bezpiecznych i pewnych wyników. Istnieją zrozumiałe obawy dotyczące zagrożenia, jakie sieciowe UAV mogą stanowić dla prywatności i bezpieczeństwa. Prawodawstwo prawdopodobnie będzie dotyczyć projektowania i użytkowania systemów opartych na IoFT, a aby pomóc w budowaniu zaufania publicznego, największym otwartym wyzwaniem stojącym przed tą dziedziną jest opracowanie i przyjęcie solidnych standardów bezpieczeństwa – zarówno urządzeń, jak i danych, które one przenoszą i przekazać. Biorąc pod uwagę wiele fizycznych form, jakie może przybierać UAV, należy opracować polityki bezpieczeństwa i algorytmy, które będą zasoobooszczędne, działają na wielu różnych typach sprzętu (od urządzeń do przechowywania danych po różne podwozia samolotów) i oprogramowania (w różnych warstwach sieci protokoły). Kiedy rozszerzy się rozważania na roje składające się z wielu UAV, a nawet różne grupy połączone za pośrednictwem sieci WFANET, zasady muszą uwzględniać większą „podatną na zagrożenia powierzchnię" sieci ad hoc oraz nadmiarowość informacji (klucze szyfrowania itp.), które pojawi się, gdy urządzenia mobilne będą niedostępne przez pewien czas w miarę ich przemieszczania się. Pomimo wszystkich wyzwań Internet Latającej Rzeczy jest obiecującym paradygmatem z dużymi szansami na zastosowanie. Dla projektantów misji powietrznych podłączenie UAV do inteligentnych środowisk umożliwi pozyskiwanie i dostarczanie aktualnych informacji, zwiększając dokładność wykonywanych przez nich zadań. Połączenie UAV z Internetem oznacza, że mogą zlecać przetwarzanie do serwerów w chmurze, zmniejszając w ten sposób zapotrzebowanie na wyrafinowany sprzęt i czyniąc je bardziej elastycznymi i łatwiejszymi w użyciu w nowych scenariuszach. I odwrotnie, dla projektantów infrastruktury i IoT, Flying Ad Hoc Networks oferują nowy, elastyczny sposób łączenia środowisk, które mogły zostać oddzielone z powodu ich oddalenia lub z powodów czasowych, takich jak klęski żywiołowe lub awarie infrastruktury. Udoskonalenia te są bardzo ważną innowacją w tej dziedzinie, dającą możliwości nowych zastosowań, szczególnie trudnych w czasie rzeczywistym, na przykład poszukiwanie i ratownictwo, krytyczne zadania nadzoru i monitorowanie wrażliwych pól.