GeoIoD: Um Protocolo de Disseminação de Informação Geocast para Internet dos Drones

Lailla M. S. Bine[1], Luiz Filipe M. Vieira[1], Linnyer B. Ruiz[2], Antonio A. F. Loureiro[1]

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)
CEP 31270-901 – Belo Horizonte – MG – Brasil

[2]Departamento de Informática
Universidade Estadual de Maringá (UEM)
CEP 87020-900 – Maringá – PR – Brasil

{laillabine, lfvieira, loureiro}@dcc.ufmg.br, lbruiz@uem.br

Abstract. *In recent years, applications that use drones have become promising to perform the monitoring, search, rescue, and on-demand delivery. For multiple applications to work together, coordinated airspace access must be provided, forming an Internet of Drones (IoD). In UAV networks, location-based information dissemination may be required. Thus, this work proposes GeoIoD, a geocast information dissemination protocol for IoD focused on the emergency scenarios context. The performance evaluation on the OMNeT++ simulator showed that GeoIoD decreased the number of generated messages and increased the delivery rate when compared to the Flooding protocol.*

Resumo. *Nos últimos anos, aplicações que utilizam drones se tornaram promissoras para fazer o monitoramento, busca, resgate e entrega sob demanda. Para que várias aplicações possam funcionar em conjunto, é necessário haver um acesso coordenado no espaço aéreo, formando a Internet of Drones (IoD). Em redes de UAVs, pode ser necessária a disseminação de informações baseadas em uma localização. Assim, este trabalho propõe o GeoIoD, um protocolo geocast de disseminação de informações para IoD com foco no contexto de situações emergenciais. A avaliação de desempenho, realizada no simulador OMNeT++, mostrou que o GeoIoD diminuiu as mensagens geradas e aumentou a taxa de entrega quando comparado ao protocolo Flooding.*

1. Introdução

As aplicações que utilizam veículos aéreos não tripulados, ou UAVs (*Unmanned Aerial Vehicles*), também conhecidos como drones, vêm atraindo grande atenção do público nos últimos anos [Hall 2016]. Aplicações que realizam algum tipo de monitoramento [Wu et al. 2016, Tosato et al. 2019] (e.g., trânsito, poluição e desastres naturais) comumente utilizam mais de um drone que trabalham em conjunto formando um enxame de drones.

Em um cenário futuro, é possível que existam várias companhias fornecendo serviços que utilizam drones. Uma das aplicações mais promissoras é a entrega sob demanda. Essa área possui vários projetos em desenvolvimento como o *Amazon Prime*

Air[1] e o *Google Wing*[2]. Com inúmeras possibilidades de aplicações funcionando ao mesmo tempo é necessário o acesso controlado ao espaço aéreo. Gharibi et al. [Gharibi et al. 2016] propuseram uma arquitetura para prover o acesso controlado dos drones no espaço aéreo denominada *Internet of Drones*.

Nas redes UAVs, da mesma forma que em VANETs (*Vehicular Ad Hoc Networks*), pode ser necessária a disseminação de informações baseadas em uma localização. Um possível exemplo desse cenário é uma aplicação que realiza o monitoramento de grandes desastres naturais. A identificação de uma vítima deve ser informada rapidamente às autoridades mais próximas que, neste caso, podem possuir uma base de operações com localização estática. Também, pode ser necessário informar outros drones na região para que eles se aproximem do local identificado com objetivo de apoiar o resgate (e.g., fornecer imagens do local por diferentes ângulos). Esse processo pode ser realizado utilizando um protocolo *geocast*.

Existem várias formas de transmitir informações entre drones. Arafat e Moh [Arafat and Moh 2019] abordaram diferentes protocolos de roteamento utilizados em redes UAVs. A transmissão de informação entre os drones possui particularidades diferentes quando comparada a outras redes como as VANETs. Ainda de acordo com Arafat e Moh [Arafat and Moh 2019], alguns exemplos dos desafios existentes em IoD são: alta mobilidade dos nós na rede e uma topologia dinâmica considerando que os enlaces entre UAVs podem ser frequentemente desconectados.

Esses mesmos conceitos devem ser considerados no desenvolvimento de protocolos de disseminação de informações. Na literatura, existem alguns trabalhos relacionados a disseminação de informações entre drones com foco em segurança [Aggarwal et al. 2019] e também considerando um contexto como *urban sensing* [Wu et al. 2016]. Todavia, ainda não foram projetados protocolos que buscam disseminar informações em um cenário de IoD considerando regiões geográficas.

Dada a motivação descrita acima, o objetivo deste trabalho é desenvolver um protocolo de disseminação *geocast* para *Internet of Drones*, que considera da melhor forma possível a mobilidade e dinamicidade da topologia da rede. O foco será o contexto de situações emergenciais. Nesse caso, é importante que a disseminação das informações ocorra da maneira mais eficiente e rápida possível, pois o cenário tratado está relacionado a vidas humanas.

Assim, a principal contribuição deste trabalho é o projeto do protocolo GeoIoD que é um protocolo de disseminação de informações *geocast* considerando a Internet dos Drones. Também é feita a avaliação de desempenho desse protocolo considerando um cenário de emergência realizada via simulador OMNeT++. Os resultados obtidos mostram a melhora na entrega de mensagens com um número menor de transmissões.

As próximas seções deste trabalho estão organizadas como segue. A Seção 2 apresenta uma visão geral do modelo denominado Internet dos Drones desenvolvido por Gharibi et al. [Gharibi et al. 2016]. A Seção 3 discute a motivação e os trabalhos relacionados à disseminação de dados e informações entre drones e em redes híbridas. A Seção 4 apresenta o protocolo GeoIoD e a Seção 5 discute os resultados obtidos. Ao final, a

[1]https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

[2]https://x.company/projects/wing/

Seção 6 apresenta a conclusão e trabalhos futuros.

2. Internet dos Drones: Uma visão geral

A Internet dos Drones (*Internet of Drones* – IoD) é um modelo proposto por Gharibi et al. [Gharibi et al. 2016] com o intuito de fornecer acesso coordenado ao espaço aéreo para drones. A IoD foi baseada na estrutura de três redes de larga escala, a saber: Rede de Controle de Tráfego Aéreo, Rede Celular e a Internet. O espaço aéreo utilizado pelos drones possui uma estrutura semelhante às estradas. Essa estrutura é composta por:

- Vias áreas: caminho por onde o drone deve voar em uma só direção, semelhante às estradas;
- Interseções: cruzamentos de duas ou mais vias áreas;
- Nós: ponto de interesse dos drones, no qual é possível o modo de voo livre.

Para facilitar o controle do espaço aéreo, ele é particionado em zonas (ver Figura 1). Cada uma das zonas possui suas vias aéreas, interseções e nós. Para o drone passar de uma zona adjacente a outra ele deve utilizar, obrigatoriamente, portões de entrada e saída. Assim, o conjunto de vias aéreas, nós e interseções podem ser representados por um grafo conforme apresenta a Figura 1.

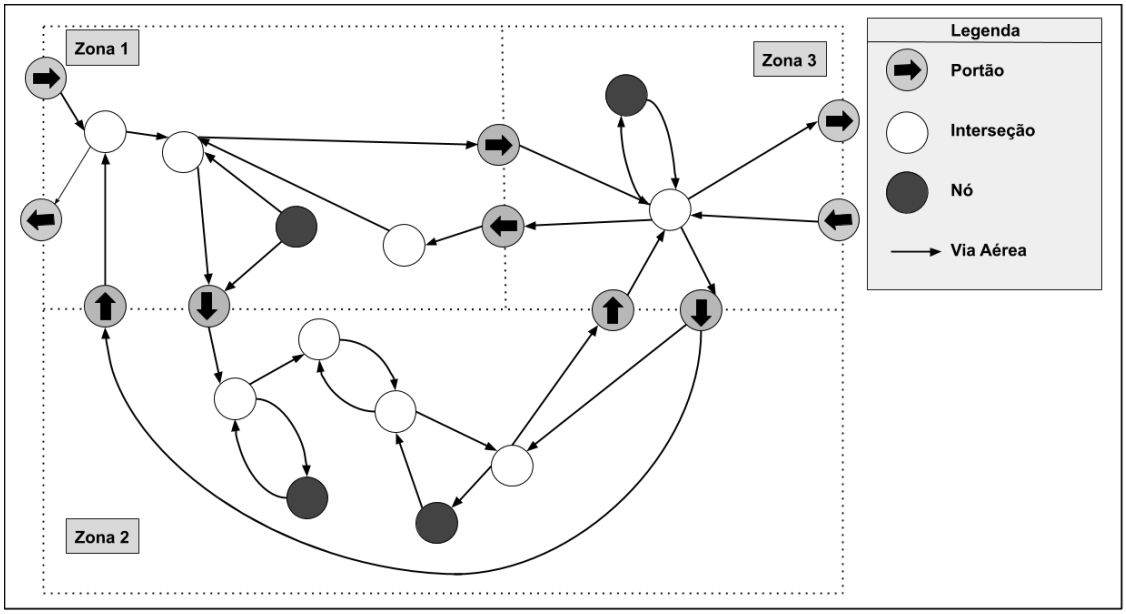

Figura 1. Representação da estrutura da Internet dos Drones (baseada em [Gharibi et al. 2016])

Cada zona possui um ou mais ZSPs (*Zone Service Providers*) que são responsáveis por coordenar os drones que estão na sua região, regulando o caminho que ele deve seguir de um ponto a outro, utilizando as vias áreas e os portões. Quando um drone passa de um zona para outra os ZSPs devem ser capazes também de coordenar o *handoff*. Os ZSPs devem funcionar semelhante a operadoras de telefonia celular, ou seja, em uma mesma região é possível que mais de uma operadora esteja fornecendo um serviço. Porém, no caso da IoD, as operadoras também devem trabalhar em conjunto para que haja harmonia na rede evitando, assim, colisões e congestionamentos. Os componentes dessa arquitetura são os drones e ZSPs (*Zone Service Providers*) detalhados a seguir:

- Drones: veículos aéreos autônomos capazes de navegar sem colisões ao longo de uma rota planejada entre dois pontos;
- ZSPs: coordenam os drones fornecendo informações de navegação entre dois elementos na zona designada para os drones solicitantes.

Os ZSPs também são responsáveis por gerenciar outras propriedades como: a necessidade de recarga energética para locomoção dos drones, fornecendo uma rota até um posto de recarga; o gerenciamento do congestionamento de vias aéreas fornecendo, caminhos alternativos; e pontos onde drones podem pousar em situações de emergência. Além disso, os ZSPs também devem prover informações meteorológicas para que os drones possam ter uma navegação ciente do ambiente e, portanto, mais confiável e segura.

Assim, uma das maiores diferenças entre o desenvolvimento de aplicações que consideram a arquitetura de IoD para as que não consideram é a presença do ZSP na estrutura. O desenvolvimento de um protocolo de disseminações de informações deve considerar que o ZSP também deve estar ciente das mudanças (ou até mesmo controlar essas mudanças) que uma informação recebida por um drone pode causar na rede.

3. Motivação e Trabalhos Relacionados

A comunicação é extremamente importante para a realização de missões que utilizam um enxame de drones, como no caso de situações de emergência em centros urbanos e não-urbanos. Cenários nos quais existem vidas em perigo, como mostram as partes A e B da Figura 2, disseminar a informação de localização pode ser crucial para salvar vidas. Outra aplicação é o uso de drones na segurança pública como mostram as partes C e D da Figura 2.

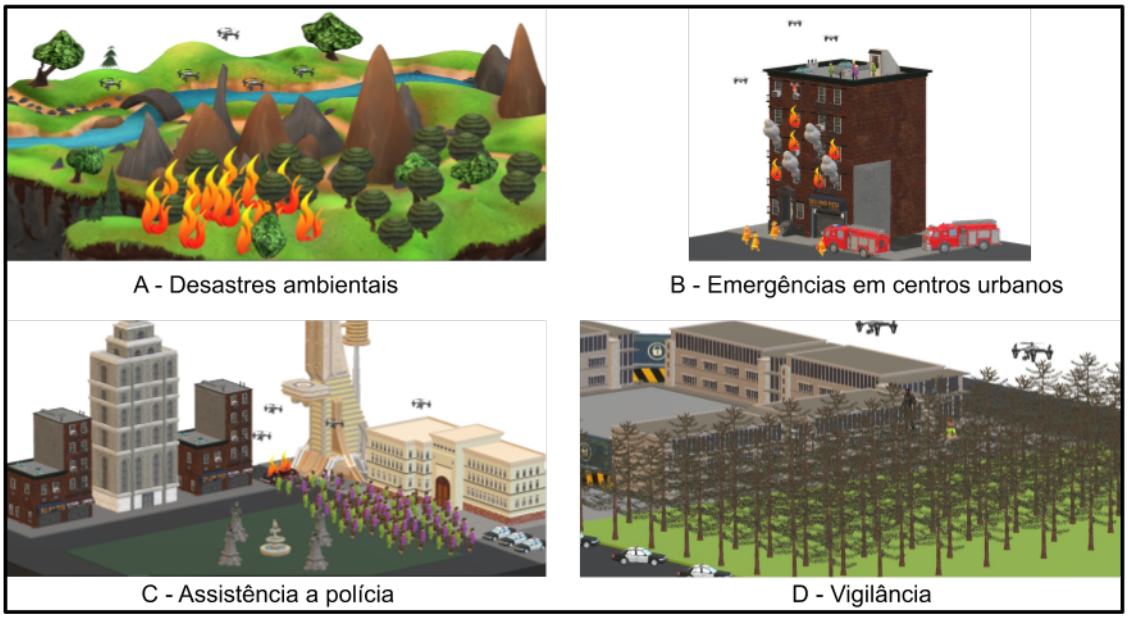

Figura 2. Exemplos de cenários nos quais a disseminação de informação entre drones é crucial

Os protocolos baseados em posição usam informações geográfica, fornecidas por GPS (*Global Positioning System*), para tomar decisões. Isso minimiza a sobrecarga e torna

os protocolos de roteamento mais escaláveis [Arafat and Moh 2019]. Fatores como a alta mobilidade dos nós, topologia dinâmica e distribuições irregulares de UAV contribuem para que o desenvolvimento de um protocolo que garanta a comunicação confiável seja um desafio em redes de UAV [Sahingoz 2013].

Apesar de Arafat and Moh [Arafat and Moh 2019] apresentarem alguns protocolos que utilizem GPS em redes UAV, nenhum deles foi desenvolvido considerando o cenário de rede IoD. Nessa rede, o ZSP é o componente que controla a rede dos drones. Nesse caso, ele tem um papel similar a um controlador em uma rede definida por software (SDN- *Software Defined Networks*). Nessas redes, o gerenciamento do controle e dos dados de rede são separados [He et al. 2016]. Já nas redes IoD, o ZSP é o responsável por gerenciar o controle da rede e, além disso, também pode controlar a rota dos drones ativamente. Este aspecto difere, por exemplo, de uma VANET, na qual a rota dos carros podem ser influenciadas por informações da rede (e.g. mudança de rota por um aviso de acidente de trânsito), porém, as alterações de rota não são mandatórias, já que o condutor do veículo é quem possui o poder de decisão final.

Segundo Bekmezei et al. [Bekmezci et al. 2013], a comunicação é crucial para a cooperação e colaboração entre UAVs. Na literatura são encontrados trabalhos relacionados à disseminação de informações entre UAVs com diferentes focos, como redes urbanas [Wu et al. 2016], baixo custo energético [Khelifi et al. 2018, Aadil et al. 2018], formação de redes auto-organizáveis [Cunha and Vieira 2019] e segurança [Aggarwal et al. 2019]. Nos últimos anos, a comunidade acadêmica vem desenvolvendo trabalhos relacionados a protocolos geocast de disseminação de informações em redes *ad hoc*, principalmente considerando o contexto de VANETs [Allal and Boudjit 2013, Kaiwartya and Kumar 2014, Cunha et al. 2016]. No entanto, o cenário de mobilidade em VANETs não pode ser considerado o mesmo de redes com drones, devido a uma série de fatores, como condições meteorológicas e disposição das vias.

Ainda considerando protocolos geocast, foram encontrados poucos trabalhos que consideram o contexto de UAVs, denominados *Flying Ad hoc Networks* (FANETs), que são apresentados na Tabela 1, indicando quais as principais características de cada trabalho e quais simuladores foram considerados para realização dos experimentos.

Um ponto a ser destacado, é que quando se trata especificamente de drones, na literatura é comum encontrar trabalhos que consideram redes onde os drones são utilizados como apoio para disseminação de informações, como por exemplo, o trabalho de Ghazzai et al. [Ghazzai et al. 2019] que utiliza drones como apoio para disseminação de informação em VANETs. Porém, também são poucos os que consideram um cenário *geocast* nesse contexto.

Outra questão a ser destacada é que nossa proposta, no melhor do nosso conhecimento, é a única que considera o contexto de IoD para um protocolo *geocast*. Mesmo quando considerado protocolos que não são *geocast*, a literatura apresenta um único trabalho ([Aggarwal et al. 2019]) que considera o desenvolvimento de um protocolo de disseminação de informações no cenário de IoD. Porém, seu foco é a segurança das informações utilizando *blockchain*. Assim, este trabalho busca explorar uma lacuna na literatura, ao projetar um protocolo de disseminação de informações que consideram o cenário de IoD.

Trabalho	Contexto	Características	Simulador
[Gankhuyag et al. 2017]	FANET	Abordagem preditiva que utiliza informações da trajetória	C++
[Hussen et al. 2019]	FANET	Abordagem preditiva	OPNET e MATLAB
[Ghazzai et al. 2019]	VANET com apoio de FANET	Abordagem com foco em eficiência energética	–
[Bousbaa et al. 2020]	FANET	Abordagem com foco na mobilidade dos nós e dinamicidade da rede	NS-3
GeoIoD	**IoD**	**Abordagem com foco na mobilidade dos nós e no cenário IoD**	**OMNeT++**

Tabela 1. Trabalhos relacionados ao desenvolvimento de um protocolo geocast para disseminação de dados e informações no contexto de UAVs.

4. GeoIoD: Protocolo Geocast para Internet dos Drones

O protocolo *geocast* GeoIoD possui como foco a disseminação de informações em cenários nos quais o drone precisa enviar informações baseadas em localização. Nesses casos, geralmente, são organizadas missões de drones para realizarem um determinado objetivo, como a localização de pessoas ou objetos. Ao encontrar um possível alvo da missão, o drone deve enviar uma mensagem para a estação base, que nesse caso é um ZSP, e para os drones mais próximos.

Como cada missão possui propriedades diferentes, inicialmente o ZSP deve ser configurado com alguns dados como: área de interesse a ser percorrida pelos drones, quantidade de drones na missão, raio de interesse para o *geocast*, alcance da transmissão de cada drone, entre outros dados necessários que podem variar de acordo com as características das tarefas a serem realizadas. Durante a missão, o ZSP é capaz de estabelecer comunicação direta com os drones (esta comunicação pode ser realizada, por exemplo, por uma rede LTE – *Long Term Evolution* ou por alguma outra rede específica) e recebe periodicamente a posição dos drones que é armazenada em uma *hash table*, conforme a Tabela 2. Essa suposição é bem razoável já que tipicamente no momento do resgate há um mínimo de condições físicas/meteorológicas para que esses procedimentos sejam levados adiante.

Id_drone	Posição	Timestamp
D_7	$(50.002, 30.123, 20.421)$	1573986030
D_10	$(90.102, 300.183, 70.141)$	1573986610
D_9	$(680.156, 670.187, 83.204)$	1573983310

Tabela 2. Exemplo de uma *hash table*.

Um ponto importante no projeto deste protocolo é a questão da quantidade de drones que deverão tomar uma ação ao receber uma mensagem. Considere a seguinte

situação: em uma VANET, quando ocorre um acidente em uma estrada, é interessante avisar todos os carros que estão na região para que eles saibam que é necessário tomar alguma ação como, por exemplo, mudar a rota. Já na IoD, nem todos os drones que estão na região de interesse da mensagem devem tomar alguma ação. Suponha que uma vítima foi localizada; talvez a equipe de resgate precise que apenas um drone na região tome a ação de se aproximar do local onde a vítima está e os outros continuem procurando por outras vítimas.

Assim, outro parâmetro inserido na inicialização do ZSP é a quantidade de drones que devem tomar alguma ação quando uma vítima for localizada. Essa informação pode ser variável em cada missão, sendo decidida pela equipe responsável pela busca de acordo com a necessidade da situação encontrada.

Quando um drone deseja enviar uma mensagem (por exemplo, ao encontrar uma pessoa), ele primeiramente envia uma mensagem ao ZSP que irá responder com o endereço dos drones para os quais a mensagem deve ser enviada. Como o ZSP possui os endereços de todos os drones, ele seleciona os N (quantidade de drones que devem se aproximar do local do drone que enviou a mensagem) drones mais próximos do drone solicitante. Essa seleção leva em consideração o parâmetro N e a localização dos drones em relação ao drone solicitante.

O ZSP realiza o cálculo do envio de acordo com o Algoritmo 1. Esse algoritmo recebe como entrada a Tabela_Drone, que é uma *hash table* com os dados de posicionamento dos drones da rede; o raio que é área que deve ser considerada alcançada pelo drone, sendo que essa informação é baseada na potência de transmissão do drone; e a variável N, que representa a quantidade de drones que devem tomar uma ação quando uma vítima é encontrada. O retorno é uma lista com os N (ou tanto quanto possível) drones mais próximos.

Algoritmo 1: Seleção de drones para receber a mensagem

```
Entrada: Tabela_Drone, Raio, N
Saída: Lista_Prioridade_Drone

para cada drone D na Tabela_Drone faça
    dist ← distanciaEuclediana(D.x, D.y, D.z)
    se dist está dentro do Raio então
        Lista_Prioridade_Drone.push((dist,D.endereco))
    fim
    Lista_Total_Drones.push((dist,D.endereco))
fim
se Lista_Prioridade_Drone.size() > N então
    retorna os N primeiros drones de Lista_Prioridade_Drones
senão
    ZspTransmite(Lista_Total_Drones, N - Lista_Prioridade_Drone.size())
    retorna Lista_Prioridade_Drones
fim
```

Caso seja necessário mais drones do que os encontrados dentro do raio, o próprio ZSP avisa os N drones mais próximos para se aproximarem do drone solicitante (método

ZspTransmite). Assim, nesse caso, o ZSP funciona de forma similar a uma rede definida por software (SDN). A Figura 3 apresenta um cenário onde não existe nenhum drone no alcance do *drone 8*, sendo necessária a intervenção do ZSP, caso esse drone encontre uma vítima nessa situação.

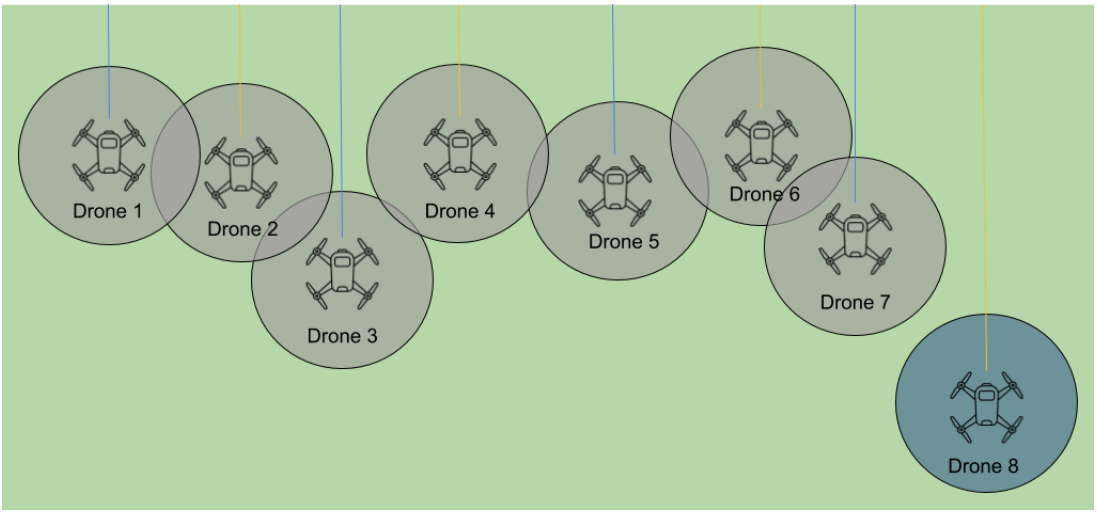

Figura 3. Exemplo, no qual caso o *drone 8* encontrasse uma vítima, não existiria nenhum drone em seu alcance.

Para realizar o controle da rede, os seguinte tipos de mensagens são possíveis para um ZSP:

- POSITION: o ZSP está recebendo uma posição de um drone;
- ASK_DRONE_MSG: um drone está solicitando ao ZSP o envio de uma mensagem;
- SEND_DRONE_MSG: o ZSP envia a um drone solicitante a lista de drones que devem receber a mensagem;
- SEND_DRONE: o ZSP envia a um drone uma mensagem direta. Utilizada no caso de não haver drones próximos a um drone que enviou uma mensagem.

Ao receber a mensagem do ZSP de volta, o drone envia a mensagem apenas para os drones que o ZSP selecionou. No caso dos drones, os seguintes tipos de mensagem são possíveis:

- SEND_POSITION: envia ao ZSP sua posição;
- ZSP_MSG: solicita ao ZSP o envio de uma mensagem;
- MSG_ZSP: recebe do ZSP uma lista com os drones mais próximos;
- SEND_DRONE: envia uma mensagem aos drones.

5. Avaliação de desempenho

Para a avaliação de desempenho do GeoIoD foi utilizado o simulador OMNeT++[3] na versão 5.5.1 com o apoio do *framework* INET[4] (versão 4.1.2), que possui suporte para

[3]https://omnetpp.org/
[4]https://inet.omnetpp.org/

modelagem de redes sem fio móveis. Esta seção descreve o cenário utilizado e os resultados obtidos na simulação. Os resultados do GeoIoD foram comparados com o protocolo *Flooding* adaptado para o contexto de IoD.

O protocolo *Flooding* consiste em transmitir as mensagens para todos os nós vizinhos, sem nenhum controle [Arafat and Moh 2019]. A adaptação realizada consiste em inserir o controle do ZSP. Assim, antes de enviar a mensagem, o drone envia ao ZSP um pedido de permissão para realizar o *Flooding* e, ao receber uma confirmação, o drone solicitante realiza esse procedimento normalmente. Esse protocolo foi escolhido por apresentar uma alta taxa de entrega de mensagens [da Costa et al. 2019].

5.1. Cenário

O cenário utilizado para realização dos experimentos foi uma situação de emergência, na qual um enxame de drones está em uma missão de localização de vítimas. Porém, dois casos foram considerados, o primeiro com 20 drones e uma área de $10^3\text{m}\times10^3\text{m}$ e o segundo com 50 drones e uma área de $10^4\text{m}\times10^4\text{m}$. O modelo de mobilidade utilizado nos dois casos foi o *column*, que consiste no movimento conjunto dos nós em uma linha, sendo útil em situações de busca [Verma 2018]. No OMNeT++, para representar esse modelo foi utilizado o padrão linear, já implementado no simulador.

As simulações foram realizada com duração de 180 s e repetidas 30 vezes. Assim, os gráficos apresentam um nível de 95% de confiança. A comunicação nos dois cenários foi realizada com o padrão IEEE 802.11n. A potência de transmissão entre os drones foi de 3 mW para o primeiro cenário e de 40 mW para o segundo. Como a comunicação entre o drone e o ZSP é direta, foi considerado que a potência de transmissão é de 4000 mW (porém, como já citado essa parte pode ser modela como uma comunicação LTE) e que o drone envia ao ZSP sua posição a cada 3 s. A Tabela 3 apresenta as configurações do cenário utilizadas.

Parâmetro	**Cenário 1**	**Cenário 2**
Mobilidade	Linear	Linear
Número de drones	20	50
Área de simulação	$10^3\text{m}\times10^3\text{m}$	$10^4\text{m}\times10^4\text{m}$
Velocidade	20–30 m/s	20–30 m/s
Potência de Transmissão entre drones	3 mW	40 mW
Tempo de simulação	180 s	180 s
Protocolo da camada de enlace	IEEE 802.11n	IEEE 802.11n
Tamanho do Pacote	512 B	512 B

Tabela 3. Parâmetros utilizados na simulação do GeoIoD.

Para uma comparação mais justa com o protocolo *Flooding*, a variável N foi definida como todos os drones dentro do raio de interesse do drone solicitante. Caso não houvesse nenhum, um drone mais próximo era avisado pelo ZSP. Na simulação, também foi considerado que os drones possuíam altitudes entre 100 e 150 metros. O mais importante nessa simulação não á a altitude dos drones em si, porém a variação de altitude entre

eles que no caso foi considerado 50 metros. Essa variação partiu da suposição de que em um evento de busca e resgate os drones teriam uma altura similar. Outro parâmetro a ser destacado é a variação da velocidade dos drones. Os valores foram escolhidos baseados na referência [Bousbaa et al. 2020].

A Figura 4 apresenta a modelagem de um cenário hipotético de busca em uma situação de emergência. Para simular que um drone encontrou uma vítima foi utilizado um parâmetro de probabilidade. Para cada drone, no início de cada simulação, foi sorteada uma probabilidade entre 0 e 1 e um tempo entre 5 e 170 segundos. Caso a probabilidade sorteada fosse maior do que 0.7, considerava-se que no tempo sorteado o drone havia encontrado uma vítima e, então, ele enviava uma mensagem ao ZSP avisando.

Figura 4. (a) cenário hipotético de busca em uma situação emergencial. (b) modelagem do cenário no OMNeT++.

Um fator importante em cenários de missões de resgate, é que é comum que as autoridades responsáveis criem um centro próximo ao local do evento para apoiar o resgate de vítimas. O ZSP, nesse caso, será uma estação base criada temporariamente, por exemplo, no centro de resgate para que as autoridades possam coordenar e receber as informações de forma mais eficiente. Assim, considerando o cenário IoD, nas quais os drones devem seguir vias definidas, no cenário utilizado por esse trabalho, o ZSP responsável pela missão precisa reservar todo o espaço aéreo de busca apenas para o resgate. Para isso ele deve informar todos os ZSPs da região para que rotas de outros drones sejam desviadas caso necessário. Isso significa que todas as vias aéreas que passam pelo local devem ser desativadas dando prioridade a missão de busca e regaste, além disso toda a região pode ser transformada em um nó temporário no espaço aéreo. O que de acordo com a arquitetura de Gharibi et al. [Gharibi et al. 2016] permite que os drones utilizem o modo de voo livre.

5.2. Resultados

Para avaliação dos resultados, foram utilizadas três métricas: (i) número de mensagens geradas, (ii) taxa de entrega e (iii) atraso na entrega das mensagens. Os resultados para os Cenários 1 e 2 são apresentados de duas formas, tanto para o *Flooding* quanto para o GeoIoD. A primeira não considera as mensagens de informação de posição dos drones e a segunda considera as mensagens de informação de posição dos drones.

A Figura 5 apresenta o gráfico do número de mensagens geradas, após 180 segundos, tanto para o Cenário 1 quanto para o Cenário 2. Como esperado, quando é considerada as mensagens de posição, o número de mensagens é superior de quando elas não são consideradas. Também observa-se que o *Flooding* gera mais mensagens quando comparado com o seu correspondente no protocolo GeoIoD. Um fator a ser destacado é que a quantidade de mensagens geradas pelo GeoIoD nos dois cenários são próximas. Um motivo para isso é que o Cenário 2 possui uma área maior e proporcionalmente menos drones do que o Cenário 1. Assim, os drones estão distribuídos dentro da área de forma mais distante uns dos outros fazendo com que menos mensagens sejam enviadas.

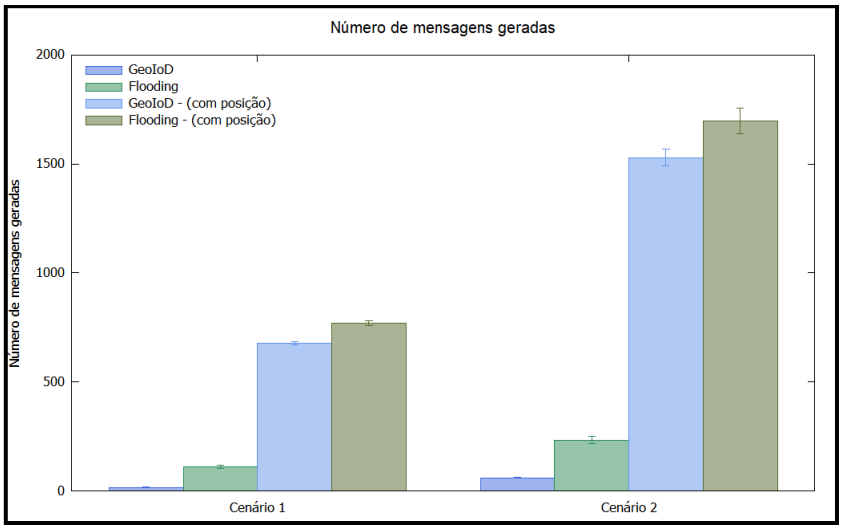

Figura 5. Número de mensagens geradas, após 180 segundos, para os protocolos simulados.

A Figura 6 mostra os resultados da taxa de entrega das mensagens, após 180 segundos de simulação. No decorrer da simulação foi observado que a taxa de entrega do *Flooding* diminuiu. Com o passar do tempo, o número de mensagens aumenta, bem como a colisão de mensagens evitando que mensagens sejam entregues. Esse fator fica visível nos cenários que não consideram as mensagens de posição. Como as mensagens de posição são um número consideravelmente maior e raramente não são entregues, quando elas são consideradas a taxa de entrega de mensagens aumenta. Outro fator interessante é que no Cenário 2 obteve-se uma taxa de entrega maior do que no Cenário 1. Acredita-se que isso se deve ao fato de que no Cenário 1 temos um área de simulação menor com um número de drones proporcionalmente maior do que no Cenário 2.

Como no GeoIoD a quantidade de mensagens geradas é menor, a taxa de colisões também diminui, proporcionando uma maior quantidade de mensagens entregues. Um dos motivos para a geração de colisões foi a forma modelada de simulação de encontro

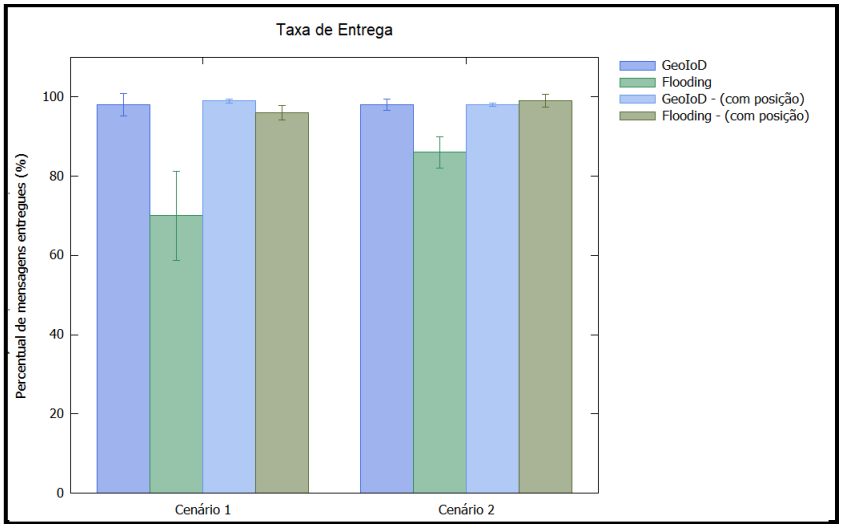

Figura 6. Percentual de mensagens entregues, após 180 segundos, para os protocolos simulados.

de uma vítima. Assim, era possível acontecer de drones próximos acabarem tendo uma probabilidade sorteada que considerava que eles encontrariam uma vítima. Além disso, os tempos sorteados para isso acontecer também eram próximos, fazendo com que colisões ocorressem.

No *Flooding* sem posição fica perceptível esse fator devido ao número de mensagens enviadas ser maior do que no GeoIoD sem posição. Já na parte que considera as mensagens de posição, esse fator não é percebido, pois as mensagens de posição são em número consideravelmente superior as mensagens que não são. Na sequência tem-se a Figura 7 que apresenta o atraso na entrega de mensagens.

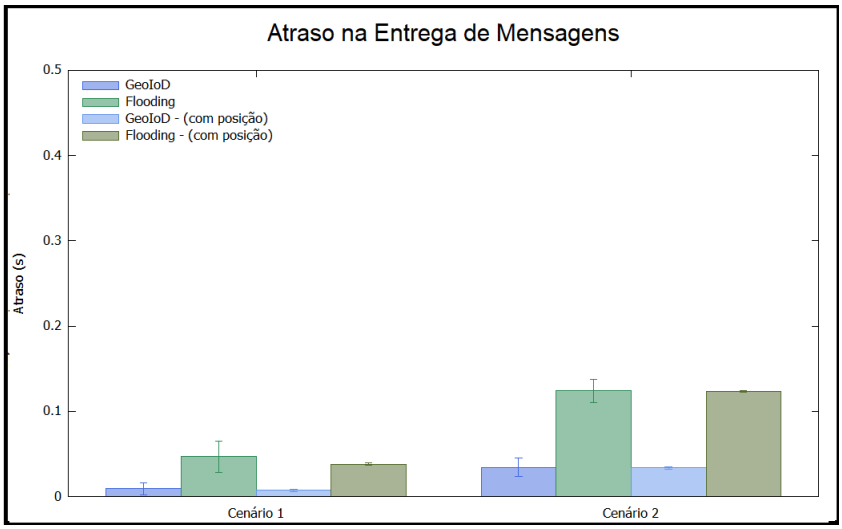

Figura 7. Atraso na entrega das mensagens, após 180 segundos, para os protocolos simulados.

Por fim, a Figura 7 apresenta o atraso na entrega das mensagens, ou seja, o tempo que a mensagem leva para ser transmitida a partir do momento que o drone solicitante

envia uma mensagem ao ZSP até os drones de destino recebê-las. Nesse caso, observa-se uma pequena diferença entre o *Flooding* e o GeoIoD devido ao *Flooding* entregar a nós que estejam mais longe do drone que enviou a mensagem fazendo com que o atraso seja um pouco maior.

Como no GeoIoD apenas drones próximos recebem a mensagem, tanto no Cenário 1 quanto no Cenário 2 o resultado é similar. Um fator a ser observado é que ao considerar as mensagens de posição do drone na rede, a média do atraso apresenta uma leve diminuição em comparação ao que não considera essas mensagens. Como já citado, essas mensagens são entregues de forma direta, portanto a média do atraso acaba diminuindo.

6. Conclusão

Este trabalho apresentou o projeto de um protocolo geocast para Internet dos Drones. Os resultados mostraram que o protocolo proposto gera menos mensagens evitando colisões e, consequentemente, aumentado a sua taxa de entrega. Porém, não houve resultados consideráveis para a métrica atraso na entrega das mensagens. Apesar da avaliação ter sido realizada em um cenário de busca e resgate, essa abordagem pode ser interessante em situações que drones ajudam na vigilância e na segurança e saúde pública.

Por considerar o cenário de IoD, atualmente, é possível realizar apenas simulações de seu desempenho. Assim, como trabalho futuro espera-se melhorar a simulação desenvolvida para que ela seja mais realística e avaliar novos cenários. Também pretende-se estender o GeoIoD para que ele tenha um bom desempenho em cenários urbanos e não urbanos. De toda forma, considera-se que este protocolo é um passo inicial no projeto de protocolos de disseminação de mensagens no contexto de IoD.

7. Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, CNPq e processo nº 15/23064-8, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

Referências

Aadil, F., Raza, A., Khan, M., Maqsood, M., Mehmood, I., and Rho, S. (2018). Energy aware cluster-based routing in flying ad-hoc networks. *Sensors*, 18(5):1413.

Aggarwal, S., Shojafar, M., Kumar, N., and Conti, M. (2019). A new secure data dissemination model in internet of drones. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE.

Allal, S. and Boudjit, S. (2013). Geocast routing protocols for vanets: Survey and geometry-driven scheme proposal. *J. Internet Serv. Inf. Secur.*, 3(1/2):20–36.

Arafat, M. Y. and Moh, S. (2019). Routing protocols for unmanned aerial vehicle networks: A survey. *IEEE Access*.

Bekmezci, I., Sahingoz, O. K., and Temel, Ş. (2013). Flying ad-hoc networks (fanets): A survey. *Ad Hoc Networks*, 11(3):1254–1270.

Bousbaa, F. Z., Kerrache, C. A., Mahi, Z., Tahari, A. E. K., Lagraa, N., and Yagoubi, M. B. (2020). Geouavs: A new geocast routing protocol for fleet of uavs. *Computer Communications*, 149:259–269.

Cunha, A. V. S. and Vieira, L. F. M. (2019). Soan: Self-organizing aerial networks. *Internet Technology Letters*, 2(3):e104.

Cunha, F., Villas, L., Boukerche, A., Maia, G., Viana, A., Mini, R. A., and Loureiro, A. A. (2016). Data communication in vanets: Protocols, applications and challenges. *Ad Hoc Networks*, 44:90–103.

da Costa, F. S., de Sousa, R. S., Soares, A. C., Loureiro, A. A. F., and Vieira, L. F. M. (2019). Geoasdvn: Um protocolo geocast ciente de obstáculos baseado em redes veiculares definidas por software. In *Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 1084–1097. SBC.

Gankhuyag, G., Shrestha, A. P., and Yoo, S.-J. (2017). Robust and reliable predictive routing strategy for flying ad-hoc networks. *IEEE Access*, 5:643–654.

Gharibi, M., Boutaba, R., and Waslander, S. L. (2016). Internet of drones. *IEEE Access*, 4:1148–1162.

Ghazzai, H., Khattab, A., and Massoud, Y. (2019). Mobility and energy aware data routing for uav-assisted vanets. In *2019 IEEE International Conference of Vehicular Electronics and Safety (ICVES)*, pages 1–6. IEEE.

Hall, R. J. (2016). An internet of drones. *IEEE Internet Computing*, 20(3):68–73.

He, Z., Cao, J., and Liu, X. (2016). Sdvn: Enabling rapid network innovation for heterogeneous vehicular communication. *IEEE network*, 30(4):10–15.

Hussen, H. R., Choi, S.-C., Park, J.-H., and Kim, J. (2019). Predictive geographic multicast routing protocol in flying ad hoc networks. *International Journal of Distributed Sensor Networks*, 15(7):1550147719843879.

Kaiwartya, O. and Kumar, S. (2014). Geocast routing: Recent advances and future challenges in vehicular adhoc networks. In *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 291–296. IEEE.

Khelifi, F., Bradai, A., Singh, K., and Atri, M. (2018). Localization and energy-efficient data routing for unmanned aerial vehicles: Fuzzy-logic-based approach. *IEEE Communications Magazine*, 56(4):129–133.

Sahingoz, O. K. (2013). Mobile networking with uavs: Opportunities and challenges. In *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 933–941. IEEE.

Tosato, P., Facinelli, D., Prada, M., Gemma, L., Rossi, M., and Brunelli, D. (2019). An autonomous swarm of drones for industrial gas sensing applications. In *2019 IEEE 20th International Symposium on"A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 1–6. IEEE.

Verma, J. (2018). Taxonomy of mobility models. *Opportunistic Networks: Mobility Models, Protocols, Security, and Privacy*.

Wu, D., Arkhipov, D. I., Kim, M., Talcott, C. L., Regan, A. C., McCann, J. A., and Venkatasubramanian, N. (2016). Addsen: Adaptive data processing and dissemination for drone swarms in urban sensing. *IEEE transactions on computers*, 66(2):183–198.