Exame - 2024

Motivação
Drones desenvolvem sua missão sobre redes móveis ad hoc voadoras (FANET – Flight AdHoc Network), ou seja, usam o conjunto completo de protocolos que estudamos no curso. Sabemos que cada parte do stack de protocolo tem vulnerabilidades e pode ser explorada por um atacante, assim como as aplicações e os sistemas operacionais.

A ideia do projeto final do curso de redes é criar um ambiente (simulado ou real) onde um pelotão de drones está se deslocando para cumprir uma missão. E há um atacante querendo impedir esta missão de se completar.
Pode escolher um dos ataques da disciplina de segurança e repetir neste cenário.

A missão está na camada de aplicação – é de livre escolha do grupo. Exemplos: operações de busca e salvamento, vigilância de plataforma de petróleo, levantamento de problemas urbanos, etc.
O ambiente a desenvolver sua aplicação, pode ser simulado. Imagino processos que tem um componente de localização que varia no tempo (simulando deslocamento) e consequentemente a conectividade pode ser afetada com a variação da localização. A localização deve ser corrigida para manter a conectividade. Identifico dois parametros importantes: localização e qualidade do sinal . Serão o pano de fundo de qualquer aplicação.

Precisa interface gráfica? Não, o foco do curso não é esse.
O ataque pode ser realizado em um drone parado? Não. Se fosse não estariamos explorando a FANET, o dinamismo traz alguns desafios, que embora a gente não vá tratar diretamente (como por exemplo algoritmos de roteamento), vamos ter que considerar. Sugiro que implementem na sua aplicação um cheque periódico de conectividade, o nível de sinal deve ser razoável sempre, senão já aborta a missão.

Então, o drone está em vôo, o ataque entra pela rede. A vulnerabilidade pode estar em qualquer ponto da rede – na app de controle em solo, no código do drone, no stack de protocolo de rede, mas o resultado da exploração desta vulnerabilidade é impedir a realização da missão.

Simultaneamente ao curso de redes, vocês fizeram a disciplina de Fundamentos de Segurança e Sistemas Distribuidos, então, ao chegar no fim do curso, vocês tem uma bagagem incrível para colocar alguns conceitos em ação.

Simuladores disponíveis
Há simuladores Open-Source para pelotão de drones com ênfase nos controles de robôs (que UAVs não deixam de ser!). Alguns simuladores colocam a ênfase na interface gráfica. Ela é útil, mas no nosso caso pode ter um mínimo de representação.

Há algumas opções de simuladores prontos para uso na experiência:
(1) CoppeliaSim
 https://www.coppeliarobotics.com .

(2) OpNet: Links uteis
https://opnetprojects.com/opnet-network-simulator/

https://networksimulationtools.com/fanet-simulator/

(3) Omnet: Links uteis
https://omnetpp.org/
https://www.projectguideline.com/simulating-and-visualizing-3d-flying-ad-hoc-network-fanet-under-omnetpp/

(4) Mininet WiFi
https://mininet-wifi.github.io/

A Tarefa
Os grupos devem conter 3 alunos (pode ser o mesmo grupo do GT)

1. Cada grupo vai definir a aplicação.
2. Cada grupo vai definir o ambiente onde rodar a aplicação
3. Cada grupo vai definir qual será o ataque
4. Realizará simulações testando ambas as situações: (1) sucesso da missão e (2) fracasso da missão com sucesso do ataque.
5. Entregará um relatório sucinto com as devidas explicações e testes.