UNISINOS

Programa de Pós-Graduação em

Computação Aplicada

Mestrado/Doutorado Acadêmico

Júnior André Marostega

MSIS – Modelo de Defesa Cibernético utilizado Técnicas de Ataques em Paralelo a Redes Sem Fio em Território Suspeito com Veículo Aéreo Não Tripulado

São Leopoldo, 2020

Júnior André Marostega

MSIS - MODELO DE DEFESA CIBERNÉTICO UTILIZANDO TÉCNICAS DE ATAQUES EM PARALELO A REDES SEM FIO EM TERRITÓRIO SUSPEITO COM VEÍCULO AÉREO NÃO TRIPULADO

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre pelo Programa de Pós-Graduação em Computação Aplicada da Universidade do Vale do Rio dos Sinos — UNISINOS

Orientador:
Prof. Dr. Rodrigo da Rosa Righi

São Leopoldo
2020

M354m Marostega, Júnior André.
MSIS: modelo de defesa cibernético utilizando técnicas de ataques em paralelo a redes sem fio em território suspeito com veículo aéreo não tripulado / por Júnior André Marostega. – São Leopoldo, 2020.

80 f. : il. color. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Computação Aplicada, São Leopoldo, RS, 2020.
Orientação: Prof. Dr. Rodrigo da Rosa Righi, Escola Politécnica.

1.Computadores – Medidas de segurança. 2.Internet – Medidas de segurança. 3.Teste de invasão (Medidas de segurança para computadores). 4.Internet das coisas. 5.Redes locais sem fio – Medidas de segurança. 6.Protocolo de aplicação sem fio (Protocolo de rede de computador). 7.Drone. I.Righi, Rodrigo da Rosa. II.Título.

CDU 004.056
004.056.53

Catalogação na publicação:
Bibliotecária Carla Maria Goulart de Moraes – CRB 10/1252

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela oportunidade de poder lutar e realizar mais este sonho.

Agradeço a minha esposa pelo apoio, dedicação e paciência prestados ao longo deste percurso.

Agradeço aos meus pais, que me ensinaram o valor da educação e a lutar pelos meus sonhos.

Agradeço aos meus irmãos Paulo Marostega, Marlon Marostega e minhas cunhadas Arlete Marostega e Joseane Marostega, que financiaram este sonho para que eu pudesse dedicar o meu amor aos estudos e realizar este sonho.

Agradeço de forma imensa ao Prof. Dr. Rodrigo da Rosa Righi, meu orientador, que foi um exemplo que busquei seguir, também sua atenção e dicas valiosas as quais empreguei em meus esforços.

Agradeço também a empresa Ricohpel Soluções Corporativas LTDA, em especial, aos proprietários Josiane Schneider e ao Marcos Schneider, pelo apoio, compreensão do tempo que me foi dado para dedicação aos meus estudos.

Não poderia deixar passar o agradecimento aos que foram meus colegas de pós-graduação, Ms. Hugo Vaz Sampaio, André Mayer, Mateus Schmitz da Silveira, Igor Fontana de Nardin e Thiago Roberto Lima Lopes, pela ajuda, discussões e auxílio nos momentos de maiores dificuldades.

RESUMO

O estudo realizado nesta dissertação teve como resultado a elaboração de um sistema de segurança para intrusão móvel, denominado Msis *(Mobile Security Intrusion System)*. Um protótipo foi desenvolvido para auxiliar autoridades, na execução de ataques cibernéticos para fins investigativos e, assim, colaborar em assuntos que envolvem cenários que podem ser considerados críticos, como: investigação policial, sequestros e outros tipos de situações de riscos a sociedade. O sistema Msis atua na varredura de redes sem fio (Wi-Fi) e, também, na captura de pacotes de dados para a senha de autenticação durante o processo de *handshake* entre dispositivos e roteadores. Entre os assuntos que são abordados se destaca: *Internet of Things*, protocolos de comunicação, *pentest* e segurança da informação. Vários trabalhos descrevem sobre ataques específicos, usando dispositivos de IoT, porém usando técnicas e métodos individuais. As diversas técnicas que estes trabalhos apontam variam quanto ao objetivo final, ou seja, não exatamente a captura de *hash*. Em relação aos trabalhos que descrevem sobre protocolos, as características que são tratadas são direcionadas ao processamento de dados, desempenho em relação ao consumo de energia e até mesmo ao consumo de banda, ainda há um número limitado de trabalhos com o foco em segurança, sendo essa uma lacuna a ser preenchida na literatura em segurança. O Msis visa contribuir para literatura de duas formas, primeiro, na ação de duas técnicas de ataque, sendo executadas de forma paralela usando *Threads*. Segundo, no desenvolvimento de um protocolo projetado para ser executado em um dispositivo de IoT, que realiza a comunicação de dados priorizando a segurança dos dados. O Msis é dividido em três módulos, Msis-A, Msis-P e o Msis-C. O Msis-A é executado em um dispositivo com recursos limitados e tem como objetivo a realização de varreduras de redes sem fio (Wi-Fi) e execução de ataques às mesmas. A projeção dos ataques é realizada com duas técnicas, conhecidas como *Brute Force* e *Evil-Twin*. O sistema Msis se diferencia por possibilitar a realização de ambas técnicas de ataque, em paralelo e de forma simultânea, com a utilização de *Threads*. Já o Msis-P fica encarregado de realizar a comparação e quebra de senha, processo que é realizado após o Msis-A ter realizado a captura da *hash* de determinada rede. Com a finalidade de comunicação entre o módulo Msis-A e o Msis-P é que foi desenvolvido o protocolo de comunicação Msis-C, protocolo localizado na camada de aplicação e a sua função é garantir a comunicação de forma segura, aplicando criptografia nos dados e, assim, realizando a comunicação entre os módulos A e P. Um componente não menos importante deste estudo foi a utilização de um VANT (Veículo Aéreo não Tripulável) usado como mecanismo de deslocamento entre determinadas áreas para assim realizar os ataques. Os resultados apresentados pelo protótipo validam a efetividade e ganho de tempo em ataques usando as técnicas do Msis-A em um ambiente real, bem como também o sucesso no funcionamento da segurança e comunicação que o Msis-C apresentou nos testes executados.

Palavras-chave: Internet das Coisas. Protocolos. Segurança da Informação. Ataque em rede sem fio. VANT.

ABSTRACT

The study carried out in this dissertation proposes a security system for mobile intrusion, called Msis (Mobile Security Intrusion System). A prototype was developed to assist authorities in carrying out cyberattacks for investigative purposes, thus collaborating on matters involving scenarios that can be considered critical, such as police investigation, kidnappings and other types of risk situations to society. The Msis system acts scanning wireless networks (Wi-Fi), and capturing authentication password data packets during the handshake process between devices and routers. Among the subjects that are addressed, we highlight, Internet of Things, communication protocols, pentest, and information security. Several papers describe specific attacks, with IoT devices, using individual techniques and methods. Msis system differs by focusing on hash capture. Papers that describe protocols focus on data processing, performance, energy consumption, and bandwidth consumption, but there is a limited number of papers that focus on security, being this is a gap to be filled in the security literature. Msis aims to contribute to the literature in two ways. First, performing two attack techniques in parallel using Threads. Second, the development of a protocol, designed to be executed in an IoT device, that performs data communication prioritizing data security. Msis is divided into three modules, Msis-A, Msis-P, and Msis-C. Msis-A runs on a device with limited resources and aims to scan wireless networks (Wi-Fi) and execute attacks on them. The attacks are projected using two techniques, known as Brute Force and Evil-Twin. The Msis system is different in that it allows both attack techniques to be carried out, in parallel and simultaneously, with the use of Threads. Msis-P is in charge of comparing and breaking a password, a process that is performed after Msis-A has captured the hash of a given network. Msis-C is a communication protocol, developed to ensure safe communication between modules Msis-A and Msis-P. Msis-C is located in the application layer, applying encryption to data, and thus carrying out the communication between modules A and P. Another important component of this dissertation, is the use of a UAV (unmanned aerial vehicles) as a movement mechanism between certain areas to carry out the attacks. The results presented by the prototype validate the effectiveness and time savings in attacks using the techniques of Msis-A in a real environment. As well as the success in the operation of security and communication that Msis-C presented in the tests performed.

Keywords: IoT. Protocol. Security Information. Pentest. UAV.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

VANT	Veículo Aéreo Não Tripulável
VARP	Veículo Aéreo Remotamente Pilotado
UAV	*Unmanned Aerial Vehicle*
RPV	*Remote Piloted Vehicle*
WEP	*Wired Equivalent Privacy*
WAP	Wi-Fi *Protected Access*
WPA2	Wi-Fi *Protected Access* 802.11i
LAN	*Local Area Network*
WAN	*Wide Area network*
MAN	*Metropolitan Area Network*
IoT	*Internet of Things*
GB	*Giga Byte*
RAM	*Random Access Memory*
ETF	*Evil-Twin-Framework*
ETFITM	*Evil-Twin-Framework-in-the-middle*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
MITM	*Man in the Middle*
RSA	*Rivest-Shamir-Adleman*
RC4	*Rivest Cipher 4*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
TKIP	*Temporal Key Integrity Protocol*
MAC	*Media Access Control*
AES	*Advanced Encryption Algorithm*
FTP	*File Transfer Protocol*
LTE	*Long Term Evolution*

SUMÁRIO

1 INTRODUÇÃO

O acesso à rede mundial de computadores, internet, ao longo dos anos vem crescendo (VILLAGE, 2019). A sociedade desenvolveu uma dependência com o uso da internet, negócios são realizados a todo o momento, a comunicação entre as pessoas se tornou algo mais objetivo e rápido, os serviços, em geral são mais dinâmicos, objetos são conectados à rede e geram dados de forma ininterrupta. Assim, diante do avanço da tecnologia se aumenta de forma automática a tendência de uso irregular da internet, com finalidade de a prática de crimes de diversos tipos ou até arquitetá-los.

Diante desse cenário, a pesquisa relacionada à segurança da informação, que tem por objetivo atuar na proteção do usuário final, é de extrema importância, uma vez que ação de ataques que se verificam nos dias atuais ocorrem de várias maneiras, seja por e-mail, arquivos oriundos de *downloads*, *softwares* e outros mecanismos que evoluem a cada dia (MING; CHEN; GUO, 2019). Dessa forma, um conceito que ganha cada vez mais força em projetar oportunidades de desenvolver novas soluções é IoT.

A nomenclatura IoT, que é conhecida como Internet das Coisas, foi usada por Kevin Ashton, pela primeira vez, no ano de 1998, em sua apresentação (WEBER, 2009). Conceito que é considerado um paradigma de conexão, ou seja, comunicação entre um ou mais dispositivos que se localizam em sua volta (GUBBI et al., 2013). Uma rede que possui diversos dispositivos conectados entre si tem como objetivo a comunicação e transferência de dados. Essa ligação de dispositivos insere *hardwares* e *softwares*, ambos se comunicando por uma rede de comunicação e, assim, trocando informações, dados de maneira automática (MIORANDI et al., 2012).

Como o objetivo desses dispositivos é coletar, processar e comunicar um volume significativo de dados, um ponto que é vulnerável a ser explorado é a segurança. Como consequência de possíveis falhas, cibercriminosos se aproveitam em conseguirem vantagens em diferentes pontos que podem ser significativos para determinados contextos de aplicação (Dorri; Kanhere; Jurdak, 2017). O limite para usabilidade desse novo conceito é totalmente ilimitado e isso pode determinar com pontualidade suas aplicações e, também, os cuidados sobre o uso de aspetos de segurança, levando-se em conta cada aplicação e arquitetura (Leo et al., 2014) (MOKHTARI; ANVARI-MOGHADDAM; ZHANG, 2019).

Na arquitetura de Internet das Coisas (IoT) existem vários tipos de protocolos de comunicação. Cada protocolo possui características diferentes umas das outras, isso faz com que cada necessidade acabe adotando um protocolo em decorrência de sua necessidade ou opte pelos protocolos mais populares, que são o COAP e o MQTT. Uma lacuna referente aos protocolos é a segurança, quanto mais pontos de segurança um protocolo possuir, a robustez e pontos como processamento, memória serão mais exigidos pelos dispositivos que os executarão (DIZDAREVIĆ et al., 2019).

Como as aplicações de usabilidade de IoT são amplas. A importância de conhecer que existem pontos vulneráveis em relação à segurança e esses devem ser trabalhados para que a ar-

quitetura não seja comprometida como um todo, e se torna um grande diferencial para o sucesso de projetos que visam trabalhar com este conceito IoT. O trabalho de manter um ambiente, um projeto ou um dispositivo em constante melhoria só agrega valor e baixa o ponto de insegurança para situações que podem ser desagradáveis, uma vez que a segurança dos dispositivos esteja em risco (Alladi et al., 2020; AMIN et al., 2020).

1.1 Motivação

Diante de novos conceitos e necessidades bem específicas é que Internet das Coisas (IoT) se torna, a cada dia, uma realidade da sociedade, mas existe ainda uma lacuna quando analisados os pontos em relação aos protocolos para uso dessas tecnologias, a falta de padrões e a vasta oportunidade que todos os dias se torna disponível, acaba tornando este processo de padronização dos protocolos cada vez mais complexo. Uma grande lacuna que várias pesquisas descrevem como oportunidade se encontra na segurança e criptografia que diversos protocolos apresentam (KUMKAR et al., 2012), (MAHMOUD et al., 2016), (SHARON et al., 2017), (ISCTE-IUL et al., 2018) e (DIZDAREVIĆ et al., 2019).

Quando o enfoque se volta a VANT, percebe-se como este dispositivo pode ser importante na área de segurança da informação. Atualmente, há vários estudos voltados para a comunicação e segurança dos próprios VANT. As lacunas desses trabalhos se encontram na segurança e controle das mesmas (BASTOSN; ALMEIDAE, 2009), (ALTAWY; YOUSSEF, 2016) e (PRIYA; SWETHA, 2019).

Já (WANG; LEE; AHN, 2016), (MOHAMMED et al., 2016), (STEINMANN; BABICEANU; SEKER, 2016), (Emmanouil Vasilomanolakis et al., 2018) e (PI, 2018) abordam suas preocupações em relação aos links de comunicação entre VANT e a base de controle. Cada estudo apresenta um mecanismo para tratar este problema de maneiras diferentes com o objetivo de garantir um nível mais elevado de segurança. Percebe-se que ainda não existem parâmetros e padrões para garantir uma segurança global desses dispositivos.

Em estudos que focam abordagens de *pentest* são identificadas várias maneiras de se praticar a técnica entre diferentes modos. Se observa que ainda o número de sistemas que possuem tipos de falhas, seja de gravidades mais simples a mais complexas, é grande. Uma lacuna que se observou nos trabalhos estudados e outros pesquisados foi a não abordagem de vários tipos de ataque de forma simultânea a um determinado alvo (MILLER, 2011), (PATTON et al., 2014), (De Jimenez, 2017) e (SHWARTZ et al., 2018).

Depois de observados os vários trabalhos e identificadas as lacunas entre IoT, técnicas de invasão e VANT se concentra forças em desenvolver um sistema que visa unificação entre técnicas de ataque com processamento paralelo em dispositivos de IoT e a garantia de comunicação segura entre partes do sistema. Assim, unificando esses em um VANT para realizar um mecanismo de ataque personalizado com finalidade de auxiliar projetos que visam beneficiar as autoridades para contribuir para a sociedade.

1.2 Questão de Pesquisa

A questão de pesquisa, que o modelo busca responder, é a seguinte: *como seria um modelo que poderia ser usado para ações de ataque a uma determinada rede sem fio (Wi-Fi). Levando em consideração momentos críticos para as autoridades. Situações que envolvem locais de difícil acesso ou na tentativa de ser discreto para realizar um tipo de ação, uma vez que o objetivo possa envolver contextos mais simples ou até situações mais delicadas, como sequestros ou até investigações sigilosas*.

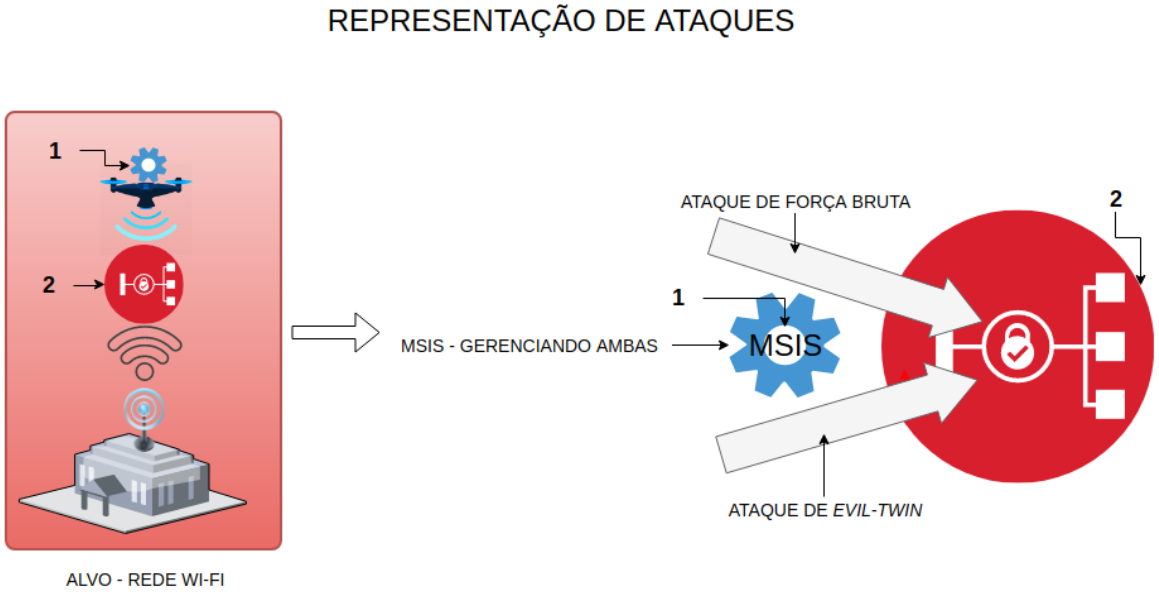
Dessa forma, é proposto o desenvolvimento de um sistema que possa ser executado em dispositivos de Internet das Coisas (IoT), ou seja, dispositivos com recursos como energia, memória e processamento limitados, mas com maiores possibilidades de usabilidade. O modelo será projetado para executar duas técnicas de invasão de forma paralela, assim diminuir o tempo neste processo de ataque a determinada rede sem fio (Wi-Fi). O modelo também vai propor um protocolo de comunicação seguro entre o dispositivo de IoT e a comunicação em nuvem, que será alocado em um servidor usado para realizar o processamento mais robusto e a quebra das senhas.

1.3 Objetivos

O objetivo desta pesquisa é desenvolver um sistema para auxiliar as autoridades como polícia, corpo de bombeiros ou equipes de investigações para agirem em combate de ações que envolvem investigação policial, resgates, sequestros ou situações que se relacionam com a coleta de informações para determinados casos. Essas necessidades se enquadram em realizar determinada ação de ataque a uma rede sem fio (Wi-Fi). Assim, para que posteriormente seja possível a descoberta da senha e, como consequência, o acesso à determinada rede, tornando todo este processo simplificado e preciso, tendo como resultado a oportunidade de uma ação preventiva diante da criminalidade ou ações que podem prejudicar a sociedade. Estratégia que evita a exposição de vidas humanas aos confrontos diretos, perante um cenário de risco.

O Msis tem como objetivo a unificação de técnicas para a realização de invasão a redes sem fio (Wi-Fi), ambas conhecidas como técnicas de *Brute Force* e *Evil-Twin*. O modelo busca a execução dessas técnicas de forma individual e também de forma paralela, abrindo assim possibilidades de ganho quanto à questão relacionada ao tempo de identificação da senha de acesso à determinada rede sem fio. Outro objetivo será o desenvolvimento de um protocolo de segurança próprio do Msis para que esse possa se comunicar entre seus módulos e as informações transmitidas sejam totalmente criptografadas. Para o desenvolvimento do modelo será preciso a utilização de técnicas de segurança da informação, assim como dispositivos de IoT.

Figura 1 – Tem o objetivo de representar a ação de um VANT sobre uma zona de ataque, ou seja, um local considerado seu alvo. O número 1 aponta para o Msis, que fica alocado junto ao VANT. Já o número 2 apresenta o momento em que é realizado o ataque, que na figura está sendo exibido ao lado direito. Pode-se observar, do lado direito, na imagem, que o ataque de *Brute Force* e o ataque de *Evil-Twin* estão apontados para um mesmo local e entre esses existe o Msis, representado pela engrenagem, que se encontra no meio para fins de gerenciamento dessas duas técnicas



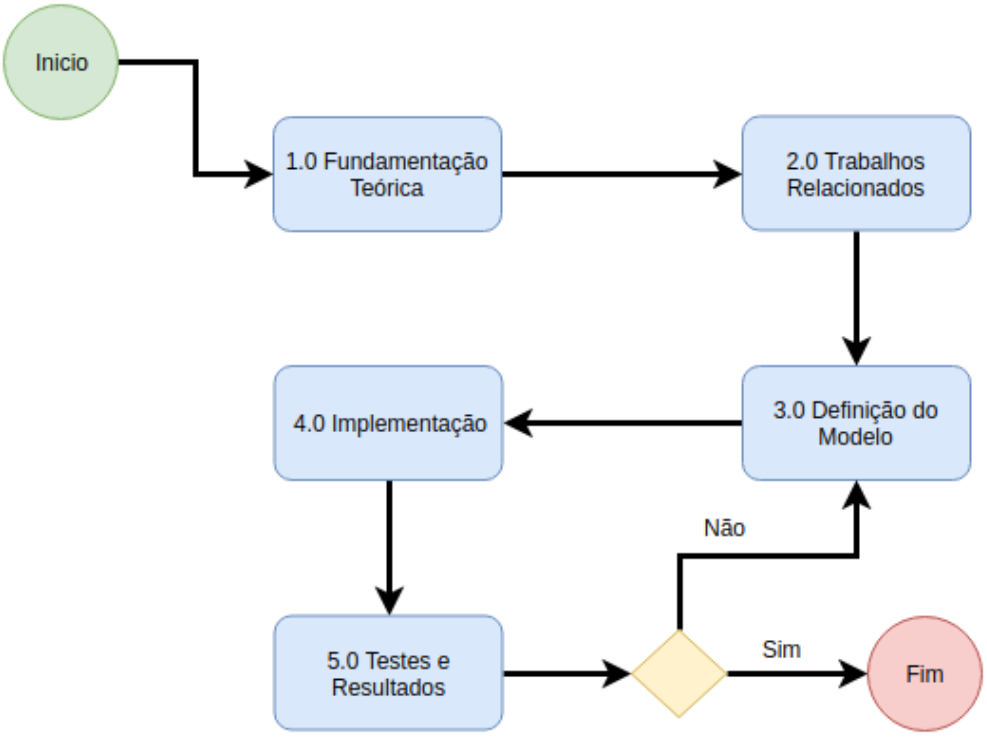
Fonte: Elaborado pelo autor.

1.4 Etapas de Desenvolvimento da Pesquisa

O desenvolvimento da pesquisa ocorreu de acordo com o fluxograma apresentado na Figura 2. As etapas no fluxograma estão divididas em cinco etapas: 1.0 Fundamentação teórica; 2.0 Trabalhos relacionados; 3.0 Definição do modelo; 4.0 Implementação; 5.0 Testes e análise dos resultados.

Primeiro, a realização de um estudo das teorias envolvidas com o tema principal, como resultado se formou o referencial teórico. Na segunda etapa se apresenta a pesquisa dos trabalhos relacionados, uma vez que o objetivo foi pesquisar e buscar trabalhos com o tema relacionado a esse. Assim foram identificadas algumas lacunas sobre o assunto. Na terceira etapa, a estratégia foi elaborada em propor um modelo sobre as lacunas encontradas na etapa anterior, unificando ao objetivo deste trabalho. Já na quarta etapa o objetivo está na exposição da implementação do modelo. Finalizando com a quinta etapa na qual se realiza a coleta dos dados de testes com finalidade de validar e concluir o trabalho.

Figura 2 – Representa o fluxograma das etapas



Fonte: Elaborado pelo autor.

1.5 Organização do Texto

A proposta está organizada em sete capítulos. Capítulo um se encontra a introdução do assunto, na sequência são apresentados os objetivos e as etapas programadas para o desenvolvimento desta pesquisa. O capítulo dois exibe a fundamentação teórica, que trata de conceitos sobre o modelo. Já o capítulo três aborda e exibe alguns trabalhos relacionados ao tema aqui proposto. No capítulo quatro se encontra descrito o modelo proposto e a evolução desta pesquisa. O capítulo cinco apresenta a metodologia de avaliação. No capítulo seis são apresentados os resultados, também se faz uma análise sobre os resultados encontrados. Finalizando, o capítulo sete apresenta a conclusão do trabalho, descrevendo sobre os resultados encontrados e os trabalhos futuros que podem ser realizados.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão abordados alguns conceitos básicos e fundamentais para a elaboração desta pesquisa. Para facilitar a compreensão e interpretação, este capítulo se divide em três seções. Todas com exibição dos fundamentos e conceitos, uma vez que as seções estão divididas da seguinte maneira: primeira: abordagens sobre segurança da informação; segunda: protocolos de comunicação e Internet das Coisas (IoT); e terceira: veículo aéreo não tripulado também conhecidos como drones.

2.1 Segurança da Informação

A segurança da informação é uma área concentrada dentro da computação e seus esforços estão em tratar de assuntos vinculados à proteção, à prevenção, ao monitoramento de dados e informações digitais. Essa área é bastante extensa e ganha muita atenção por parte da sociedade em geral, sejam universidades, empresas, governos entre outros. Nos últimos anos, a evolução digital está crescendo em uma dinâmica elevada, assim como nascem novas tendências e tecnologias diariamente. A geração de novos dados não fica para trás, e isso demanda muito esforço para garantir a total integridade e segurança da informação. Hoje, os dados que são gerados possuem valores específicos para os novos negócios que surgem e se desenvolvem.

Conforme (De Jimenez, 2017), a base da segurança da informação é dividida em quatro pilares:

- Autenticação: significa que o software ou serviço precisa identificar quem é você. Exemplo: usuário e senha.
- Autorização: após existir a validação e identificação do usuário, de quem é você, é preciso saber onde você pode acessar. Exemplo: permissões de acesso a determinado local, diretório ou arquivo.
- Integridade: a garantia de que os dados que estão armazenados em determinado local estão protegidos contra acesso indevido, alterações ou exclusões por usuários que não possuem as permissões.
- Disponibilidade: a segurança de que os sistemas estejam sempre disponíveis aos usuários legítimos.

Profissionais que atuam na prevenção e segurança de sistemas são conhecidos como *Hackers*. Aqueles que atuam de forma oposta, aplicam seu conhecimento e esforços para acessar sistemas, coletar dados variados e até danificar esses são conhecidos como *Crackers* (De Jimenez, 2017). Na computação, conforme as novas tendências que estão surgindo, novas áreas nascem e ganham profissionais focados em determinados assuntos. A especialidade de segurança da informação não é diferente, dessa forma, não será descrito todas as subáreas.

Esta pesquisa vai atuar sobre situações de ataques, usando técnicas de *Pentesters*, que abaixo serão mais aprofundadas de forma mais clara.

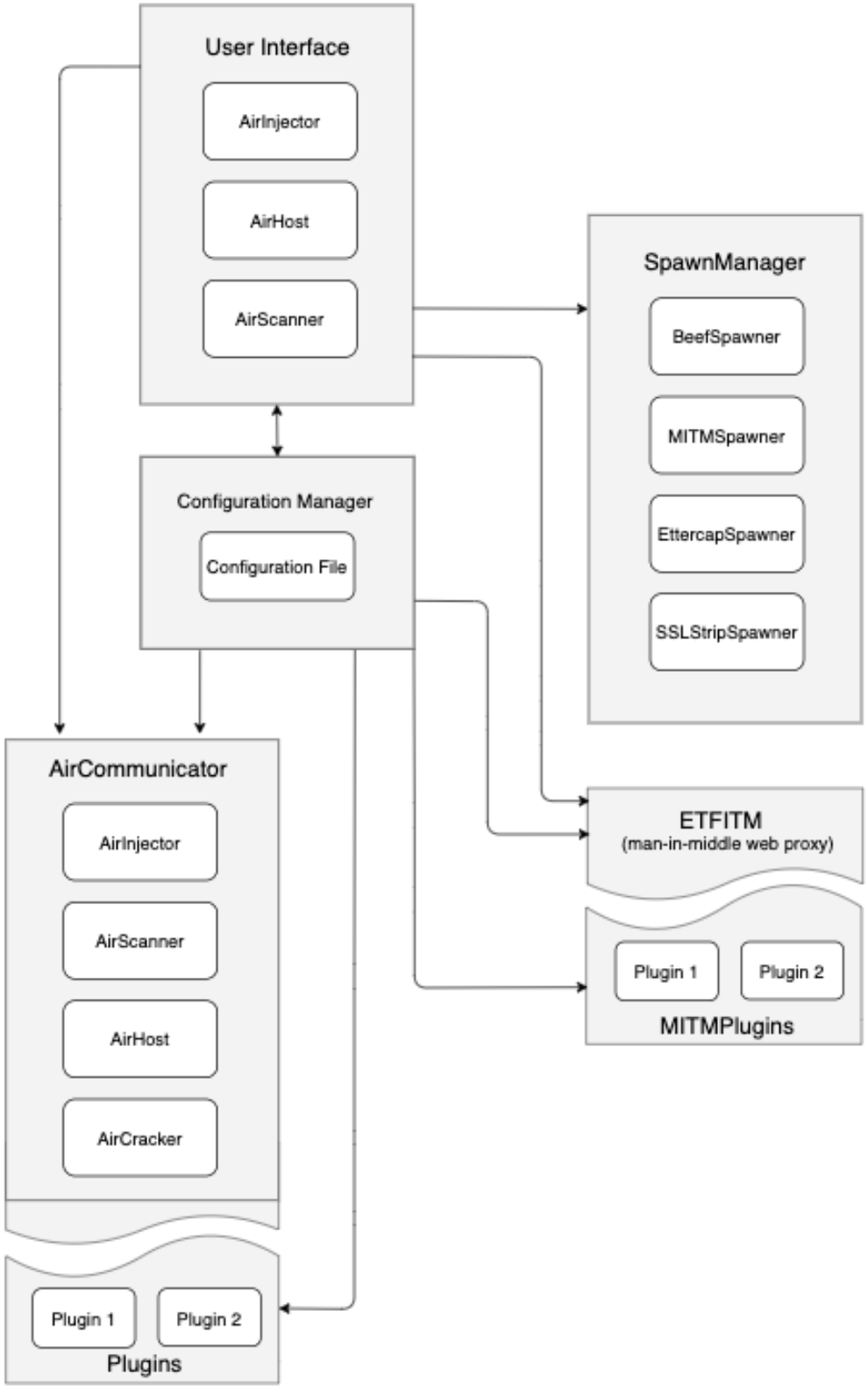
2.1.1 Descrição

1. *Evil-Twin:*

   Iscte-iul (ISCTE-IUL et al., 2018) e (SETHURAMAN; DHAMODARAN; VIJAYAKUMAR, 2019) demonstram a técnica que é usada para exploração de vulnerabilidades em redes sem fio (Wi-Fi). A característica deste tipo de ataque é o invasor se passar por um ponto de acesso idêntico aos confiáveis. O grande ponto de uso dessa técnica é o reflexo do comportamento de dispositivos clientes sem fio (Wi-Fi), ou seja, aqueles dispositivos que conectam na rede sem fio (Wi-Fi) de forma automática. Também descrevem sobre um *framework*, desenvolvido na linguagem de programação Python, que se chama *Evil-Twin-Framework* (ETF) - seu foco é atuar principalmente na comunicação, lado cliente. Profissionais de *Pentest* acabam usando muito para exploração de vulnerabilidades. A arquitetura desse *framework* (ETF) é composta de vários módulos que se comunicam entre si. Conforme ilustrado na Figura 3.

   - *AirCommunicator* - Módulo sem fio (Wi-Fi) - Seu objetivo é suportar uma alta gama de recursos sem fio (Wi-Fi) e ataques. Sendo assim, na figura são identificados três pilares de comunicação sem fio (Wi-Fi). Todos são pacotes de *sniffing* - injeção de pacotes personalizados e criação de pontos de acesso. Este módulo principal realiza a leitura do arquivo de configuração antes de iniciar os serviços. Qualquer tipo de ataque que seja sem fio (Wi-Fi) pode ser construído usando estes recursos (ISCTE-IUL et al., 2018).
     - *AirScanner*: objetivo é *sniffing* de pacote.
     - *AirInjector*: objetivo é realizar a injeção de pacotes.
     - *AirHost*: objetivo é a criação de pontos de acesso.
   - ETFITM (*Evil-Twin-Framework-in-the-middle*) - é um módulo MITM (*Man-In-The-Middle*) que é usado pelo *pentest* ou auditor de segurança para criar um *proxy* da web que pode interceptar tráfego de origem HTTP e HTTPS (ISCTE-IUL et al., 2018).
   - *Plug-ins* existe a possibilidade de extensão do *framework* através de *plug-ins* - com ênfase em duas características (ISCTE-IUL et al., 2018).
     - *Plug-ins* MITM: são *scripts* que são executados no momento em que o MITM *proxy* se encontra ativo. Isso porque o *proxy* passa todas as solicitações, HTTP ou HTTPS e as respostas podem ser via os *plug-ins*.

Figura 3 – Arquitetura do *Framework - Evil-Twin*



Fonte: (ISCTE-IUL et al., 2018)

  - *Plug-ins* (Wi-Fi) - objetivo de seguir um fluxo com uma complexidade de execução maior, deixando aberto para que cada usuário possa desenvolver de acordo com dado cenário.

- *Configuration Manager* no qual é realizada a configuração geral e os outros módulos possam buscar informações neste (ISCTE-IUL et al., 2018).

2. *Brute Force:*

   É quando se consegue acesso a algum serviço ou *software* realizando todas as possíveis tentativas de usuário e senhas possíveis. Segundo (SHWARTZ et al., 2018) e (GILLELA; PRENOSIL; Venkat Reddy, 2019) é um método usado para tentar todas as possíveis chaves para decodificar os dados até encontrar os dados corretos. Na criptografia é citado como uma busca por força bruta ou chave exaustiva *search*. Esta técnica é conhecida como criptoanálise.

2.1.2 Comunicação: segurança e exploração em redes sem fio (Wi-Fi)

Com o passar dos anos, a rede mundial de computadores apresenta evoluções, em todas as suas lacunas, assim cada vez mais fazendo parte da rotina das pessoas, seja nas indústrias, universidades, escolas, cafés e até mesmo dentro das residências. Um facilitador de várias operações é a rede sem fio (KUMKAR et al., 2012), também conhecida como WLAN, que proporciona liberdade aos seus usuários para que possam realizar as suas atividades de forma mais dinâmica. Estas redes se tornaram bastante comuns em redes privadas e públicas. Vale a ressalva da sua importância, que cabe o destaque da mobilidade e liberdade.

Segundo (KUMKAR et al., 2012) escreve que essas conexões acabam carregando um ponto bastante crítico, sendo dada muito pouca atenção e se está falando de segurança ao contrário da rede, que é classificada por LAN, que seria a rede via conexão de cabo, também conhecida como rede cabeada, ou seja, menos liberdade e mobilidade, mas mais segura. Quando é realizada uma conexão utilizando a tecnologia IEEE 802.11 (Wi-Fi), é preciso realizar a autenticação, ou seja, inserir uma senha para poder ter permissão a esta rede, no momento em que é inserida a senha pelo dispositivo do usuário, a mesma é validada via um protocolo de segurança, cujo objetivo é assegurar os dados validados no ato da inserção da senha, estes protocolos são chamados de WEP *Wired Equivalent Privacy*, WPA rede sem fio (Wi-Fi) *Protected Access* ou WPA2 rede sem fio (Wi-Fi) *Protected Access 802.11i* e abaixo será descrito um pouco mais sobre cada um desses.

O IEEE 802: é um grupo que desenvolve padrões de redes e práticas recomendadas para as redes LAN e MAN *Metropolitan Area Network* também conhecida como rede de área metropolitana, ou rede de maior alcance (D'AMBROSIA, 2019).

1. Protocolo de Segurança: WEP *(Wired Equivalent Privacy)* é um algoritmo de criptografia, que foi desenvolvido no ano de 1999 em conjunto com IEEE, 802.1lb. Esse protocolo

tem por objetivo fornecer uma comunicação segura via sinais de rádio entre o WLAN e o usuário final. A característica desse protocolo é trabalhar com o Algoritmo RC4 *Rivest Cipher 4* da RSA *Data security*, usando chave de 40 e 104 bits.

Funcionamento:

Para cada chave é adicionado um vetor de inicialização de 24 bits, este transmitido de forma direta. Esse protocolo usa CRC-32 para a integridade dos dados. Servidor: o texto simples é XOR com o fluxo de chaves, esse é gerado após o KSA e processo PRGA de RC4 e o texto é obtido. Cliente: o funcionamento ocorre de forma inversa ao servidor, isso claro usando a mesma chave (KUMKAR et al., 2012).

2. Protocolo de Segurança: *WPA (Wi-Fi Protected Access)*, a evolução da WEP vem a ser a WPA no ano de 2003. Também desenvolvido pela IEEE 802.11i. Esse protocolo foi desenvolvido logo após a primeira versão WEP (KUMKAR et al., 2012).

   Funcionamento:

   O Protocolo de Integridade de Chave Temporal (TKIP) vem como melhoria, porém esse também emprega o algoritmo RC4 com melhorias. Começa no ato da comunicação, no qual as chaves são alteradas de forma dinâmica e passam a ser de 48bits. Para fornecer a integridade dos dados durante a transmissão é usado um algoritmo novo, chamado Michael, e esse serve de integridade da mensagem (MIC). Sendo assim, em um tempo reduzido, o TKIP fornece mistura de chaves de pacote, realizando uma verificação de integridade da mensagem e mecanismo de chaveamento (KUMKAR et al., 2012).

3. Protocolo de Segurança: WPA-2 *(Wi-Fi Protected Access 802.11i)*, a evolução do WPA é o WPA2 ou 802.11i, um ano depois, 2004. Pelo grupo de tarefas i (TGi).

   Funcionamento: esse protocolo não emprega o RC4 como as versões anteriores. Esse emprega um modo contador com CBC - Protocolo MAC (CCMP) com o objetivo de criptografar o tráfego de rede. O CCMP emprega o Advanced Encryption Standard (AES) como algoritmo de criptografia. O 802.11i só é compatível com o WPA (KUMKAR et al., 2012).

2.2 Protocolos: rede de comunicação e camadas de IoT

Na estrutura de rede de computadores, existem alguns padrões já definidos, quando observada a camada de protocolos. Já no mundo de IoT ainda existem algumas lacunas quando aprofundada a visão para as camadas de protocolos. O motivo é decorrente da falta de padronização. Existem grupos de trabalhos que são organizados para refinar e buscar cada vez mais este tipo de alinhamento e padronização para o conceito de IoT (ALI et al., 2017).

2.2.1 Descrição

A rede de IoT se divide em cinco camadas: camada de percepção, camada de rede, camada de *middleware*, camada de aplicação e camada de negócios (Khan et al., 2012).

- Camada de percepção: na qual se encontram os objetos físicos e sensores. Exemplo: sensores de temperatura.
- Camada de rede: aquela em que ocorre o sistema de transmissão dos sensores para o sistema de processamento. Exemplo: as tecnologias 4G, rede sem fio (Wi-Fi), infravermelho e outros.
- Camada de *Middleware*: essa camada fica responsável por receber os dados da camada anterior e armazenar em um banco de dados, para que possa gerenciar as tomadas de decisões quanto ao processamento dos dados.
- Camada de aplicação: na camada de aplicação podem ser desenvolvidas "n"tipos de aplicações usados em IoT para atuar na gestão e execução.
- Camada de negócios: nessa camada se faz a gestão dos aplicativos e serviços, sendo local em que as regras e os modelos de negócios podem ser desenvolvidos e gerenciados (Khan et al., 2012).

A camada de aplicação é aquela em que ocorre uma concentração de gestão e interação maior entre os protocolos citados anteriormente. Nessa camada existe uma interação entre pessoas e objetos. Abaixo serão listados os protocolos mais utilizados:

- CoAP *(Constrained Application Protocol)*: usa o protocolo de transporta UDP *User Datagram Protocol* e como mecanismo de segurança usa o DTLS. Esse é um protocolo projetado para IoT. Esse é um protocolo síncrono. Possui uma arquitetura REST *Representational State Transfer*. Esse é um protocolo simples e tem interação com serviços *WEB*. Conta também com suporte *multicast* (RESCORLA; MODADUGU, 2012; DIZDAREVIĆ et al., 2019).
- MQTT *(Message Queue Telemetry Transport)*: usa o protocolo de transporte TCP. O requisito de energia para o uso do MQTT é baixo. Esse protocolo é adequado para uso em dispositivos com recursos limitados. O MQTT conta com três níveis de qualidade de serviço (QoS). Nível 0 oferece o melhor esforço possível, sem a confirmação na recepção da mensagem. Nível 1 garante a chegada das mensagens, mas é necessária a confirmação. Nível 2 garante que a mensagem será entregue exatamente uma vez, sem a duplicação. Para isso se usa um mecanismo de *handshake* de quatro vias (TANTITHARANUKUL et al., 2017; DIZDAREVIĆ et al., 2019).

- MQTT-SN: é uma versão do MQTT, mas direcionado para redes de sensores e que suporta o uso do protocolo UDP, em sua camada de transporte (Al-Fuqaha et al., 2015; DIZDAREVIĆ et al., 2019).

- HTTP REST: é um protocolo mais simples que o HTTP. Sua arquitetura é baseada em cliente - servidor. Esse é integrado também aos serviços de web. Utiliza as mesmas funções que o HTTP (Joshi et al., 2017).

- AMQP *(Advanced Message Queuing Protocol)*: esse protocolo preza pela interoperabilidade entre "n"dispositivos e várias linguagens de programação (ALI et al., 2017). Assim, permite que diferentes plataformas, implementadas em diferentes linguagens, troquem mensagens. Excelente para sistemas heterogêneos (LINDÉN, 2017).

- XMPP *(Extensible Messaging and Presence Protocol)*: protocolo que usa a linguagem XML para realizar a troca de mensagens. A arquitetura que este modelo tem usado se define como cliente / servidor. A dinâmica de funcionamento, em outros sistemas, operacionais é consideravelmente boa (YASSEIN; SHATNAWI et al., 2016; SAINT-ANDRE et al., 2004). Esse é um protocolo que não foi projetado para IoT, porém ultimamente a comunidade está colocando forças para tornar o mesmo mais adaptado para este tipo de aplicação (SCHUSTER et al., 2014; Hornsby; Bail, 2009).

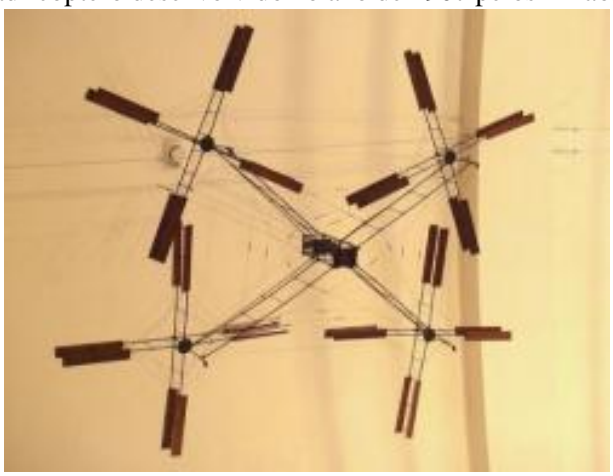
2.3 Veículo aéreo não tripulado - VANT

2.3.1 Descrição

Veículo aéreo não tripulado (VANT), também conhecido como Veículo Aéreo Remotamente Pilotado (VARP) ou simplesmente mais popular drone, palavra que traduzida significa zangão, e como é conhecido no Brasil. O seu termo oficial é *Unmanned Aerial Vehicle* (UAV) (MOHAMMED et al., 2016). Para fins de facilitar a interpretação neste estudo será definida a expressão VANT, que se trata de um conceito bastante antigo, utilizado pela primeira vez em 12 de julho de 1849, em um ato de ataque do Exército Austríaco à cidade de Veneza, Itália. O momento foi caracterizado pela estratégia de uso de balões, que carregavam explosivos traçando a rota a partir de um navio Austríaco, tendo como objetivo avançar sobre a cidade de Veneza para a explosão desses. Como resultado, alguns balões conseguiram concluir o objetivo, outros não tiveram o mesmo sucesso e assim retornando para as linhas Austríacas, o motivo do fracasso foi a alteração do vento (BASTOSN; ALMEIDAE, 2009).

Segundo (DORMEHL, 2018), no ano de 1907, foi criado o primeiro quadricóptero, desenvolvido pelos irmãos Jacques e Louis Bréguet, ambos tiveram o apoio do professor Charles Richet. Essa primeira versão tinha algumas limitações, a mais significativa era no momento da decolagem, pois precisava de quatro pessoas para estabilizá-lo no ar. Versão que desencadeou a evolução dos VANT atuais. Na Figura 4 é possível observar este primeiro modelo.

Figura 4 – O primeiro quadricóptero desenvolvido no ano de 1907 pelos irmãos Jacques e Louis Bréguet



Fonte: (DORMEHL, 2018)

As primeiras aeronaves não pilotadas de fato acabaram sendo desenvolvidas após a 1º Guerra Mundial (1914-1918). Essas aeronaves eram conhecidas como “torpedos aéreos”. Aqui, a grande evolução foi no desenvolvimento do controle remoto, adicionando o giroscópio visando anular as vibrações da própria aeronave, essa evolução ocorreu por Elmer Sperry, um norte-americano, conforme (BASTOSN; ALMEIDAE, 2009). Já segundo (PATIAS, 2016), esse primeiro drone nasceu na Marinha dos Estados Unidos da América. Elmer Sperry foi o fundador da empresa chamada de Sperry Corporação, empresa que atua em controle de navegação de voo.

Conforme (BASTOSN; ALMEIDAE, 2009), no ano de 1935, já outro norte-americano Reginald Denny evoluiu a aeronave para o rádio controlado, o primeiro VANT ficou conhecido como RP-1 ou RPV (Remote Piloted Vehicle). Pode-se considerar que a partir de então a evolução se tornou algo mais visado. Nascendo o RP-2, RP-3 e RP-4. Os anos se passaram e vários países foram desenvolvendo os seus próprios modelos, os pontos de maiores ensaios e focos aconteceram em atos de guerras militares de diversos países, em diversos anos. Atualmente, os drones vêm ganhando cada vez mais recursos tecnológicos e evoluindo em seus designs, como mostrado na Figura 5.

Já existem inúmeros tipos de VANT no mercado e cada modelo pode ser aplicado para diferentes necessidades, dessa maneira não será especificado ou direcionado modelo para determinadas funções, isso porque os critérios de escolha são sempre variáveis diferenciadas ponderando os vários contextos, de acordo com um determinado modelo as alterações se aplicam em características diferentes. Exemplo: número de hélices, tamanho e tecnologias (ALTAWY; YOUSSEF, 2016).

As características básicas entre um VANT e uma aeronave tripulada se assemelham, as variações mais significativas podem ser: o tamanho de modo geral, largura, comprimento, altura e envergaduras. Também se destaca a ausência do piloto local, assim possibilitando contextos

Figura 5 – Os fabricantes de VANT acrescentam cada vez mais recursos tecnológicos nesses dispositivos e, também, inovando em seus respectivos designs

Fonte: (DORMEHL, 2018)

diferentes e ações mais ousadas que um VANT pode assumir em relação a uma aeronave, conforme (BASTOSN; ALMEIDAE, 2009). Também existe uma diferença em relação ao tamanho e diferentes tecnologias de construção entre ambas, baseada em materiais e formas geométricas, que acabam reduzindo a reflexão das ondas eletromagnéticas, que são emitidas pelo radar.

Vale a ressalva em relação ao custo de operação, se analisadas as diferenças entre essas aeronaves. Nas aeronaves convencionais, os parâmetros de produção são de outro porte, desde o material de construção, tecnologias e dispositivos como motores. Assim, levando em consideração as aplicabilidades, uma aeronave adentra as suas responsabilidades, conforme (BASTOSN; ALMEIDAE, 2009). Para a usabilidade de um VANT, é preciso compreender o objetivo da aplicabilidade para assim definir o dispositivo correto, uma vez que as características que apresentam tais veículos são diversificadas. Segue abaixo:

- VANT: de acordo com número de hélice e tamanho;
- VANT: de acordo com seu peso;
- VANT: de acordo com a forma de controle;
- VANT: de acordo com sua interface de tecnologia;
- VANT: de acordo com sua usabilidade.

3 TRABALHOS RELACIONADOS

Este capítulo tem como objetivo apresentar os trabalhos relacionados que esta pesquisa tem como objetivo alcançar. Levando em consideração o tema proposto, foram analisados alguns trabalhos relacionados, observando a resolução e a abordagem de problemas semelhantes ao desta pesquisa. A apresentação deste capítulo ocorre enfatizando as seguintes seções: a seção 3.1, metodologia de pesquisa e escolha dos trabalhos relacionados. A seção 3.2 apresenta as análises dos trabalhos relacionados. A seção 3.3 descreve sobre análise e oportunidade de pesquisa. Finalizando com a seção 3.4 apontando as considerações parciais.

3.1 Metodologia de Pesquisa e Escolha dos Trabalhos Relacionados

Como esta pesquisa envolve várias tecnologias e de diferentes arquiteturas, os critérios de escolha de cada uma se desenvolveram de forma independente, da mesma maneira se descreve quanto à ação de busca em diferentes portais, *Google Scholar, IEEE-Xplorer Libraly, SciELO e ScienceDirect*. Abaixo seguem as *strings* como base em cada grupo:

Figura 6 – *String* de Pesquisa

“security" AND (IoT OR protocol OR unmanned vehicle) AND “security" AND (attack OR network OR parallel OR pentest)

Fonte: Elaborado pelo autor.

Para realizar a classificação dos artigos, foram adotados os seguintes pré-requisitos:

- Assunto referente ao protocolo para Internet das Coisas (IoT);
- Assunto que aborda sobre protocolos e VANT;
- Assunto que descreve sobre técnicas de ataques a redes sem fio (Wi-Fi) usando diferentes técnicas.

3.2 Análise dos Trabalhos

Esta seção apresenta pontos analisados dos artigos pesquisados. Os pontos listados devem ser observados para direcionar e auxiliar no projeto a ser desenvolvido.

Tabela 1 – Comparação dos trabalhos relacionados

Artigo	Tecnologia			Publicador
	IoT / VANT	Protocolos	Segurança (ataques)	
BASTOSN; ALMEIDAE, 2009	X		X	International Journal of Police Strategies& Management
LTAWY; YOUSSEF, 2016	X			ACM Transactions on Cyber-Physical Systems
WANG; LEE; AHN, 2016	X	X	X	Springer
MOHAMMED et al., 2016	X	X	X	IEEE
STEINMANN; BABICEANU; SEKER, 2016	X		X	IEEE
Emmanouil Vasilomanolakis et al., 2018	X	X	X	IEEE
PI, 2018	X			IEEE
PRIYA; SWETHA, 2019	X			International Journal of Research in Engineering
MILLER, 2011			X	IEEE
KUMKAR et al., 2012		X	X	I.Journal RC. Engineering Technology
PATTON et al., 2014		X	X	IEEE
MAHMOUD et al., 2016		X	X	ICITST
De Jimenez, 2017			X	IEEE
SHARON et al., 2017	X		X	IEEE
SHWARTZ et al., 2018		X	X	IEEE
SCTE-IUL et al., 2018		X	X	Systems, Management and Security
DIZDAREVI C et al., 2019		X		ACM Computing Surveys

Fonte: Elaborado pelo autor.

3.2.1 Internet das Coisas (IoT)

Nesta seção de Internet das Coisas (IoT), serão classificados os trabalhos de acordo com as características técnicas, aplicabilidades, modelos de equipamentos e outros detalhes que possam somar em conhecimento para o desenvolvimento desta pesquisa.

No estudo de (BASTOSN; ALMEIDAE, 2009), esse relata sobre o uso do VANT como um mecanismo de auxílio ao policiamento, uma vez que o autor cita sobre a preocupação em relação ao aumento da criminalidade. Essa ação seria uma forma de aumentar a segurança pública local. Estudo realizado no Estado da Bahia no Brasil.

Altawy (ALTAWY; YOUSSEF, 2016) realiza o estudo que executa a análise de aspectos relacionados à segurança e privacidade em relação ao uso de um tipo de VANT da classe civil, uma vez que a demanda de uso de VANT tem aumentado, de forma significativa, o artigo aponta para os próximos desafios relacionados à segurança de controle das aeronaves. Apresentam-se várias técnicas, como também diversas situações de ataques contra os VANTS. A preocupação é relacionada ao rápido crescimento dos dispositivos comercializados e o uso desses perante a sociedade.

Wang (WANG; LEE; AHN, 2016) descreve, em seu artigo, sobre a segurança entre links, VANT e o controlador, este localizado no solo. O texto apresenta sobre o link, a comunicação GCS (estação de controle de solo) e o link CNPC (comunicação de controle e não payload). O uso do link CNPC pode adicionar uma rede terrestre, neste caso seria LTE (Long Term Evolution), que realiza a comunicação entre o VANT e o GCS. Assim, o foco do artigo foi no desenvolvimento de uma arquitetura de comunicação para integrar a tecnologia LTE a rede CNPC, e focar na segurança dessa comunicação. Também é apresentada a modificação do protocolo de acordo com sua autenticação de chaves de entrega a rede. Na sequência foi realizada uma comparação com o protocolo LTE e o resultado apresentou que o protocolo modificado superou no ponto segurança, o protocolo LTE.

Mohammed (MOHAMMED et al., 2016) exibe, em seu artigo, aspectos sobre comunicação de redes e protocolos VANT e MANET. O significado de MANET é uma coleção de nós móveis independentes, esses são conectados via link sem fio. Usam protocolos como IEEE 802.11 a / b / g / n, 802.16 e outros. Esses protocolos da rede MANET configuram, de forma dinâmica, uma rede sem uma infraestrutura de torre e sim usando os nós móveis como roteadores e hosts, ou seja, os nós a todo momento estão em constante movimento, causando rapidamente mudanças na topologia, porém sempre em constante comunicação, assim garantindo a devida segurança. Esses nós, por suas características, são pequenos e têm um poder de processamento e energia limitado, assim tornando uma rede difícil de ser elaborada e gerenciada.

Steinmann (STEINMANN; BABICEANU; SEKER, 2016) descreve sobre a segurança, quando relacionados aos dados armazenados nos *chips* e memórias dos VANT, como o *link* de comunicação entre o VANT e a estação terrestre. Assim, o artigo propõe um método de chave de criptografia para dados particionados, armazenados e trocados com o VANT. O sistema GS-UAS usa um algoritmo de chave pseudoaleatório, que requer um atributo pseudoaleatório do GS, para criar uma chave pública pseudoaleatória para criptografar os dados. Dessa forma, auxilia o GS com o gerenciamento dos dados e chaves. Os benefícios dessa solução implicam em segurança dos dados, autenticação, garantia de que as UAS e o GS tenham confiança de que estão se comunicando. Segundo o artigo, as soluções de criptografia testadas usando um ambiente desenvolvido na linguagem JAVA e propostas para serem implementadas em placas de desenvolvimento FPGA para serem instaladas em VANT.

Emmanouil (Emmanouil Vasilomanolakis et al., 2018) apresenta a ideia de um *honeypot* para proteção de VANT. Técnica usada para auxiliar na identificação de atacantes em determinadas áreas. A técnica usada, que é apresentada neste artigo, adiciona o dispositivo chamado de *Raspberry Pi* com um adaptador sem fio ALFA AWU036NH (Wi-Fi) e um hostapd mais um dnsmasq, esses componentes adicionados ao VANT, cuja função é emular os rádios para telemetria AR dos Drones e MAVLink (Wi-Fi). O Honeypot tem a função de emular os sistemas de arquivos do VANT em combinação com o protocolo Telnet, SSH, FTP e emula o MAVLink. O software desenvolvido utiliza a linguagem de programação Python 2.7. O MAVLInk é usado para simulação de voos, assim o autor cita o uso de PyMAVLink, MAVProxy e Ardupilot SITL. Esses têm a função de simular o VANT para acesso ao MAVLink. O artigo apresenta dois ataques reais utilizando essas técnicas.

Pesquisa relacionada ao desenvolvimento de um dispositivo chamado de Auditor de WiFi, direcionado para a execução de auditorias. Essa solução soma *hardware e software*, sendo desenvolvida sobre uma arquitetura da versão *Raspberry Pi 3*. Serviços que este projeto visou: interferência deliberada, bloqueio e interferência em comunicações sem fio (Wi-Fi). Ação que pode ser realizada em um nó preciso ou na rede toda. Com este dispositivo é possível visualizar e selecionar determinados alvos para realização de ataques *"Man in the Miggle"*, ação que foca na inspeção dos dados, que fluem entre vítima e destino. Também é possível realizar a verificação de logs, emite relatórios via e-mail em intervalos definidos e identifica dispositivos

vulneráveis na rede. É possível fazer rastreamento, em tempo real, e monitorar alerta em relação a determinados dispositivos (PI, 2018).

Priya (PRIYA; SWETHA, 2019) apresenta vários tipos de VANT, principalmente, equipamentos para a agricultura, uma vez que as variedades são dinâmicas e possuem vastas possibilidades. O autor leva em consideração neste estudo várias características importantes dos VANT, como tamanho, número de hélices e desempenho desses.

3.2.2 Segurança da Informação e Protocolos

Nesta seção de segurança da informação serão classificados os trabalhos de acordo com as técnicas, aplicabilidades e outros detalhes que possam somar em conhecimento para o desenvolvimento desta pesquisa.

Miller (MILLER, 2011) concentra seus objetivos em realizar vários testes de ataques em dois grandes *players* voltados ao mundo dos sistemas operacionais, sendo esses: IOS e Android, ambos com maior número de usuários ativos. Os tópicos abordados nestes são: criptografia, bloqueios e privacidade. Os centros de atuação que o estudo desenvolve é sobre *malwares*, que significa ações do usuário como, *download* de um aplicativo, na sequência realiza a instalação e executa. Também o drive-by, que visa exploração por meio de vulnerabilidades de aplicativos já instalados no dispositivo do alvo. O autor foca em visualizar como os fabricantes APPLE e GOOGLE atuam sobre estes dois contextos.

Kumkar (KUMKAR et al., 2012) foca nas vulnerabilidades dos protocolos de segurança das redes sem fio (Wi-Fi), sendo esses conhecidos como WEP e WAP2. O estudo exibe as características de cada protocolo, sendo esses, WEP o primeiro protocolo a ser lançado e o menos seguro, o WAP, o segundo protocolo a ser lançado e, também, com falhas de segurança e o WAP2 último protocolo a ser lançado e com as devidas correções que seus antecessores apontavam como defeitos, uma vez que o WAP2 buscou a correção. O artigo também apresenta técnicas de invasão a estes protocolos. Técnicas de variadas características, assim comprovando que a segurança das conexões sem fio (Wi-Fi) não são cem por cento seguras, independente do protocolo usado.

Patton (PATTON et al., 2014) explora o assunto de segurança em dispositivos de Internet das Coisas (IoT). O artigo destaca a importância da segurança, conforme estimativa do alto crescimento de uso da tecnologia, uma vez que as variedades de aplicações de IoT visam abranger a sua confiabilidade, sendo essa levada em consideração. O foco desta pesquisa é na avaliação de vulnerabilidades emergentes que existem para quem usa esta tecnologia.

Mahmoud (MAHMOUD et al., 2016) descreve sobre arquitetura de Internet das Coisas (IoT) com foco em segurança da informação sobre as camadas: percepção, rede e aplicação. O artigo descreve os problemas sobre as devidas camadas, sendo essas:

Camada de Percepção: possui três problemas apontados pelo autor.

- Primeiro: força do sinal sem fio.

- Segundo: o nó sensor em dispositivo IoT pode ser interceptado, tanto pelo proprietário como pelo invasor, uma vez que a localização desses está em locais externos, nesse caso ocorre ataque físico aos dispositivos.

- Terceiro: a natureza inerente de topologia de rede que é dinâmica como os nós de IoT, uma vez que essa camada é formada por sensores, que em muitos casos são limitados ao consumo de energia e armazenamento de informações.

Camada de Rede: sujeito a ataques DoS, possível tipo de ataque à confidencialidade e privacidade da camada por análise de tráfego, espionagem e passivo de monitoramento. Essa camada está suscetível a ataques *Man-in-the-Middle*.

Camada de Aplicação: em função de falta de padronização dessa camada existem vários tipos de aplicativos com diferentes tipos de autenticação, que a dificuldade de garantir a privacidade dos dados acaba não sendo um padrão e nem uma prioridade.

Após apresentar os problemas relacionados sobre as camadas, o artigo foca também em uma abordagem rápida sobre o protocolo (IACAC) - autenticação de identidade e controle de acesso baseado na capacidade de IoT. Também abordou a importância da rede 5G e IPV6 no universo da Internet das Coisas.

De Jimenez (De Jimenez, 2017) escreve sobre ataques, usando técnicas de *Pentest* em aplicações web. O autor exibe diversas fases e técnicas para ação. O estudo exibe o conceito do *Pentest*, e aborda pontos em que podem ser encontradas vulnerabilidades relacionadas à web, sejam essas: via servidor ou via práticas de desenvolvimento. Segundo o artigo é o local em que se encontra o maior número de vulnerabilidades. O artigo também mostra os princípios da segurança da informação: autenticação, autorização, integridade e disponibilidade. O estudo enfatiza como são classificados os testes de penetração:

- Teste de penetração da caixa preta: uma vez que o atacante não tem nenhum conhecimento sobre o seu alvo, toda pesquisa e ação ocorre por conta desse.

- Teste de penetração da caixa branca: o atacante possui uma gama de informações e acesso à rede interna do cliente, dessa forma, o objetivo é focar em verificar os testes de fluxos de dados, testes de caminhos *loops* e outros.

- Teste de penetração da caixa cinza: o atacante possui informações parciais para realizar o ataque. Nesse caso, sua ação será de modo externo, ou seja, ataque externo para chegar internamente. Com grau de conhecimento sobre a infraestrutura de forma parcial e, também, o foco do seu ataque é mais direcionado a determinado *software* ou serviço.

Por fim, o artigo descreve algumas ferramentas usadas para ações de ataques usando as técnicas de *Pentest*.

O artigo exibe um estudo relacionado à criptografia, usando imagens para a mesma e automatiza o mesmo, usando o *Raspberry Pi*. O estudo utilizou as técnicas de criptografia e

esteganografia, uma vez que criptografia torna algo ilegível, mas não esconde a essência do segredo, e a esteganografia esconde o mesmo, assim a pesquisa objetiva unificar as duas técnicas (SHARON et al., 2017).

Shwartz (SHWARTZ et al., 2018) explora vários dispositivos de IoT, usando técnicas de caixa preta e engenharia reversa. A abordagem desse estudo aponta que vários dispositivos que são conectados na web não possuem práticas básicas de segurança. O estudo apresenta uma comparação sobre dezesseis dispositivos populares de IoT. As técnicas têm como objetivo a recuperação de *firmware*, também de senhas dos dispositivos. O estudo também exibe algumas sugestões de benefícios aos consumidores e recomendações para quem deseja tornar os dispositivos mais seguros. Existe uma abordagem entre as características técnicas dos sistemas operacionais usados em IoT. Em função de circunstâncias e, também, dispositivos com maior número de ataque, ou com uma vulnerabilidade maior.

Iscte-iul (ISCTE-IUL et al., 2018) aborda sobre as técnicas de *Pentest* usadas para exploração de redes sem fio (Wi-Fi), usando um *framework* chamado de *Evil-Twin* (ETF). O estudo elaborado por este artigo demonstra como são vulneráveis as conexões de redes sem fio (Wi-Fi). Em decorrência do crescimento de usuários, em diversos dispositivos e locais, a forma de explorar a conexão sem fio (Wi-Fi) só tem aumentado. A preocupação com a segurança e métodos corretos de prevenção acabam sendo deixados de lado. O estudo faz apontamentos sobre os protocolos WEP, WPA e WPA2. As formas de ataques usando *Evil-Twin* e *Karma* são consideradas como forma (Wi-Fi) *phishing*. O ETF se concentra, principalmente, na análise de vulnerabilidades no lado do cliente. Esse *framework* foi desenvolvido usando a linguagem de programação Python (versão 2). Esta arquitetura é formada por vários módulos, que se comunicam entre si. O ETF está aberto para a comunidade que deseja ajudar a contribuir para seu aprimoramento.

Estudo que realiza comparações entre vários tipos de protocolos usados em aplicações de IoT. Entre esses estão os mais conhecidos e usados MQTT e CoAP. Os vários apontamentos são sobre: largura de banda, desempenho, energia, segurança e uma observação geral. Como resultado dessas pesquisas, conclusões como, o protocolo CoAP consome menos largura de banda que o MQTT. Uma avaliação entre os diversos protocolos avaliados na pesquisa conclui que o CoAP é um protocolo mais econômico, quando relacionado ao consumo de energia. No aspecto segurança existem algumas situações em que seja possível contornar, usando TLS ou DTLS, mas ainda existe uma lacuna nesse ponto. Finalizando com uma colocação global informa que os protocolos MQTT e HTTP acabam sendo os mais utilizados atualmente (DIZDAREVIĆ et al., 2019).

3.3 Análise e oportunidade de pesquisa

Esta seção apresenta alguns pontos fracos em relação ao estudo realizado na seção 3.2. Uma breve análise na Tabela-1 demonstra o que foi encontrado nas pesquisas. Tabela elaborada para

relacionar trabalhos que têm objetivos e descrevem tecnologias e pesquisas semelhantes ao tema proposto.

Analisando dispositivos de IoT e VANT se observam pesquisas com enfoque na comunicação entre base e dispositivos. O motivo é a demanda e crescimento dessa tecnologia, juntamente com esses dispositivos, que estão disponíveis no mercado. Os dispositivos VANT, que são de fácil acesso no mercado, tratam de dispositivos baratos e com pouca tecnologia inclusa. Reflexo este que pode ser tratado como problema para uso desses equipamentos em território inadequado. Mesmo os VANT com tecnologias mais robustas também apresentam preocupações em relação ao controle e sua comunicação, ou seja, visivelmente existe ainda falta de padrões de segurança que atuam nesses pontos (BASTOSN; ALMEIDAE, 2009), (ALTAWY; YOUSSEF, 2016), (PRIYA; SWETHA, 2019) (WANG; LEE; AHN, 2016), (MOHAMMED et al., 2016), (STEINMANN; BABICEANU; SEKER, 2016), (Emmanouil Vasilomanolakis et al., 2018) e (PI, 2018).

O conceito de Internet das Coisas (IoT) se encontra em vários estudos, muitas novidades, alternativas de usabilidade e muita evolução em várias verticais de mercado e da ciência, mas a limitação de fatores como processamento, memória, transferência de dados e outros, que dificultam a padronização de processos como protocolos de comunicação entre estes dispositivos, seja *hardware* ou *softwares* (KUMKAR et al., 2012), (MAHMOUD et al., 2016), (SHARON et al., 2017), (ISCTE-IUL et al., 2018) e (DIZDAREVIĆ et al., 2019).

Com essa falta de padronização do conceito de IoT, os reflexos acabam sendo em diferentes contextos. De acordo com o contexto, em que não se têm padrões de alto nível para a implantação de protocolos, abre-se lacuna para a exploração de ataques a esses tipos de redes e também de dispositivos. As pesquisas que foram encontradas tratam de formatos de resolução e, também, de formas para correção de problemas pontuais, seja no modo de ataque como no modo de defesa (MILLER, 2011), (PATTON et al., 2014), (De Jimenez, 2017) e (SHWARTZ et al., 2018).

Por fim, observados os trabalhos que atuam na alteração de técnicas para realizar ações de defesa e ataques em relação ao conjunto de dispositivos ou redes de comunicação. Não encontrada a exploração de mais de uma técnica sobre ação de um dispositivo de IoT. Ainda, apesar de encontrados vários estudos sobre protocolos, que defendem e apontam seus favoritos, todos os que foram estudados deixam como lacuna a oportunidade de avançar no quesito segurança.

Dessa maneira, as lacunas a serem exploradas serão:

- Otimização de mais de uma técnica de ataque e execução, de forma paralela, com foco em redes sem fio (Wi-Fi), sendo executados em dispositivos de IoT, ou seja, com recursos de processamento e memória limitados.

- Trabalhar com protocolo de comunicação específico com a finalidade de execução em dispositivos de IoT, nos quais existe um processamento mais simplificado em relação aos grandes computadores. Ponto a ser levado em consideração é a segurança deste protocolo.

- O uso de um VANT para uma ação de realizar ataque a um determinado alvo.

3.4 Considerações parciais

Das várias tecnologias avaliadas na pesquisa e citadas na seção 3.3, se tornam mais claros pontos importantes, uma vez que cada um agrega ao Msis, compreendendo que vários pontos devem ser considerados para fins de melhoria e uma exploração adequada para que a proposta seja eficiente e atenda aos objetivos. O grande desafio fica alocado sobre as técnicas e melhorias relacionadas à segurança da informação no ponto de exploração e ataque, atribuindo as técnicas de *Brute Force* e *Evil-Twin*.

4 O MODELO MSIS

Este capítulo descreve sobre o modelo Msis, modelo proposto para auxiliar no processo de ataques cibernéticos em redes de internet sem fio (Wi-Fi). Para uma melhor compreensão deste capítulo, este será dividido da seguinte forma: seção 4.1 apresenta as decisões para a elaboração deste projeto. Na seção 4.2 se apresenta a arquitetura do Msis. A seção 4.3 descreve sobre o modelo da aplicação, em que o Msis é projetado e, finalizando, com a seção 4.4, que aborda sobre as considerações parciais de aspecto geral.

4.1 Decisões de Projeto

O modelo parte de duas premissas. Primeiro contexto, existe uma situação de risco ocorrendo em um determinado local, momento em que as autoridades são acionadas para efetuar a intervenção sobre o caso, a situação aponta um certo grau de risco, dessa forma é preciso cautela e uma base de informações do ambiente e da situação. No segundo contexto, em andamento se encontra uma investigação, na qual o cenário conta com fatores de comunicação digital e vários detalhes ocorrendo por este meio. As autoridades iniciam o período de investigação e precisam se aproximar e coletar o máximo de dados sobre o caso.

Em destaque se define que exista um time de especialistas em segurança da informação e outro em manipulação de equipamentos aéreos. A equipe de especialistas em segurança da informação possui vários dicionários, que contêm milhares de senhas e também computadores para processar informações com um alto nível de velocidade. Já a equipe, que atua com equipamentos de voo, possui consigo alguns VANTs e profissionais aptos ao manuseio desses.

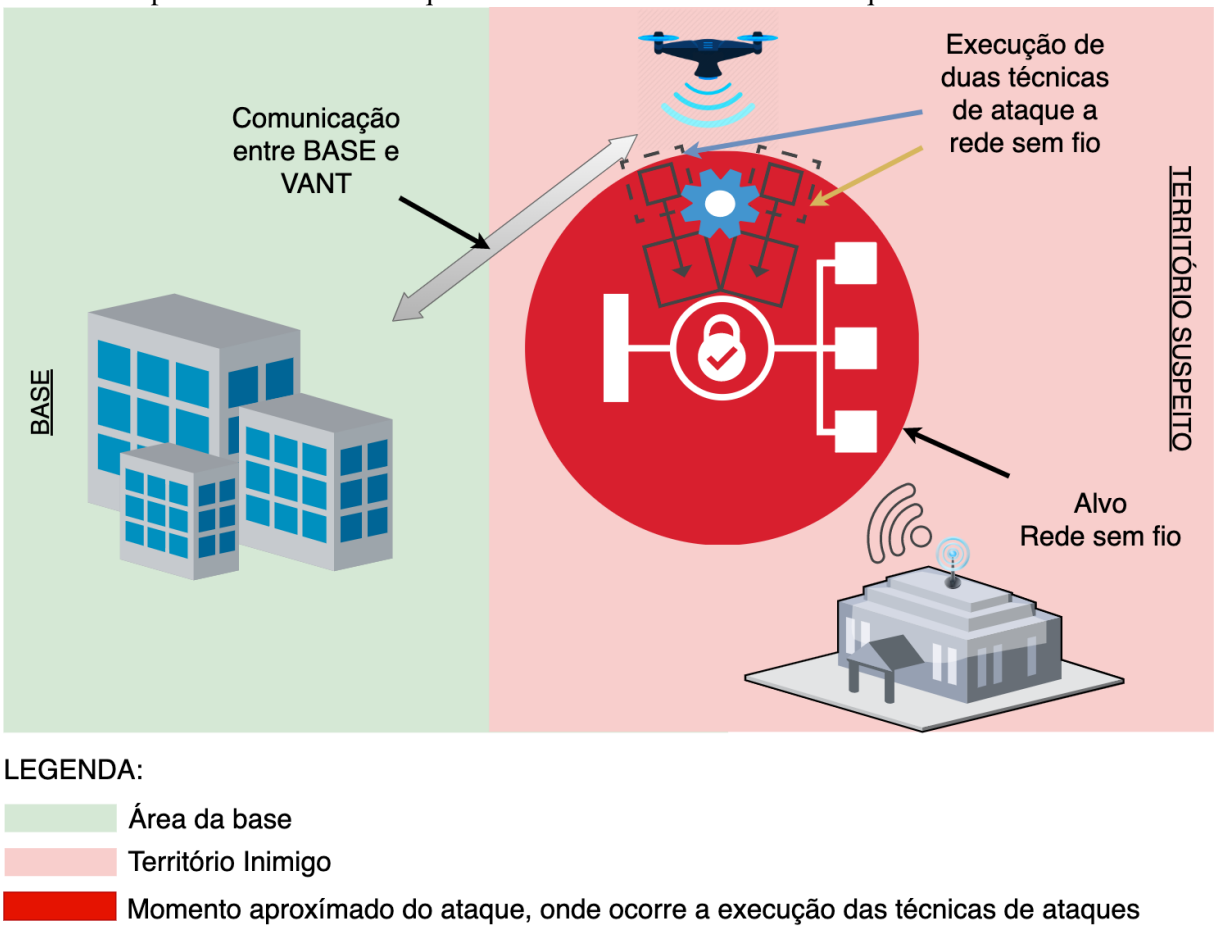
Como escopo de desenvolvimento do Msis:

- Uma primeira colocação é no desenvolvimento de um sistema que vai realizar a função de ataques em redes sem fio. Este tem como função e inovação unificar duas técnicas de ataques diferentes para que sejam exploradas de forma paralela. O sistema será executado em um dispositivo de IoT. Já o dispositivo de IoT, no modelo Msis, será acoplado a um VANT para que assim possa facilitar a aproximação a determinados pontos, sendo esses os que se deseja explorar nos ataques.

- Entra no escopo do Msis também, como segunda colocação, o desenvolvimento de um protocolo de comunicação, esse tem a função de fazer a comunicação dos módulos do Msis de forma segura, ou seja, contando com criptografia e compactação dos dados.

A Figura 7 exibe uma representação do modelo proposto, e a figura exibe um VANT sobre um determinado local e o mesmo realizando o ataque a rede sem fio (Wi-Fi), usando duas técnicas diferentes, porém sendo executadas ao mesmo tempo, conectado com a base via protocolo de comunicação, desenvolvido juntamente ao Msis, com a finalidade de que os dados transferidos entre o VANT e a base sejam criptografados.

Figura 7 – Resumo de operação do modelo Msis. VANT que é deslocado a um determinado território suspeito com finalidade de realizar uma varredura de rede e, assim, identificar um ponto de ataque. Após este, o VANT inicia o processo de ataque, processo esse que é executado por um especialista em segurança da informação. A figura exibe em destaque três cores que exemplificam a base de operação, o território suspeito e o momento em que o VANT realiza as técnicas de ataques



Fonte: Elaborado pelo autor.

4.2 Arquitetura do Msis

A Figura 8 apresenta, de forma detalhada, a arquitetura geral do modelo Msis, que é dividido em três módulos, sendo esses: Msis-A, Msis-P e Msis-C. As contribuições pontuais que o sistema Msis tem como objetivo alcançar se localizam nos módulos Msis-A e Msis-C. O módulo Msis-A é aquele no qual vai existir a unificação e execução em paralelo de duas técnicas de ataque, essas técnicas serão executadas em um dispositivo de IoT, que tem características mais objetivas, quando observado o contexto técnico. Exemplo: equipamentos com nível baixo de processamento, limitado ao armazenamento de informações, muitas vezes até um consumo de energia mais controlado. Para o modelo do Msis será usado um dispositivo conhecido como *Raspberry Pi*. O módulo Msis-C é responsável por atuar como o protocolo de comunicação entre ambos módulos (A e P). Para facilitar a compreensão, na arquitetura são destacados os pontos de contribuição na cor verde.

- Atores: como pré-requisito se tem a existência do especialista em segurança da informação e do piloto do VANT. O especialista em segurança da informação fica com a responsabilidade de interagir diretamente com o sistema Msis, esse possui controle total da aplicação nos três módulos (Msis-A, Msis-C e Msis-P). Já o piloto é o responsável em manipular o VANT. Entre esses profissionais a comunicação é indispensável, uma vez que o alinhamento do alvo e, também, da identificação da potência encontrada nas proximidades do mesmo.

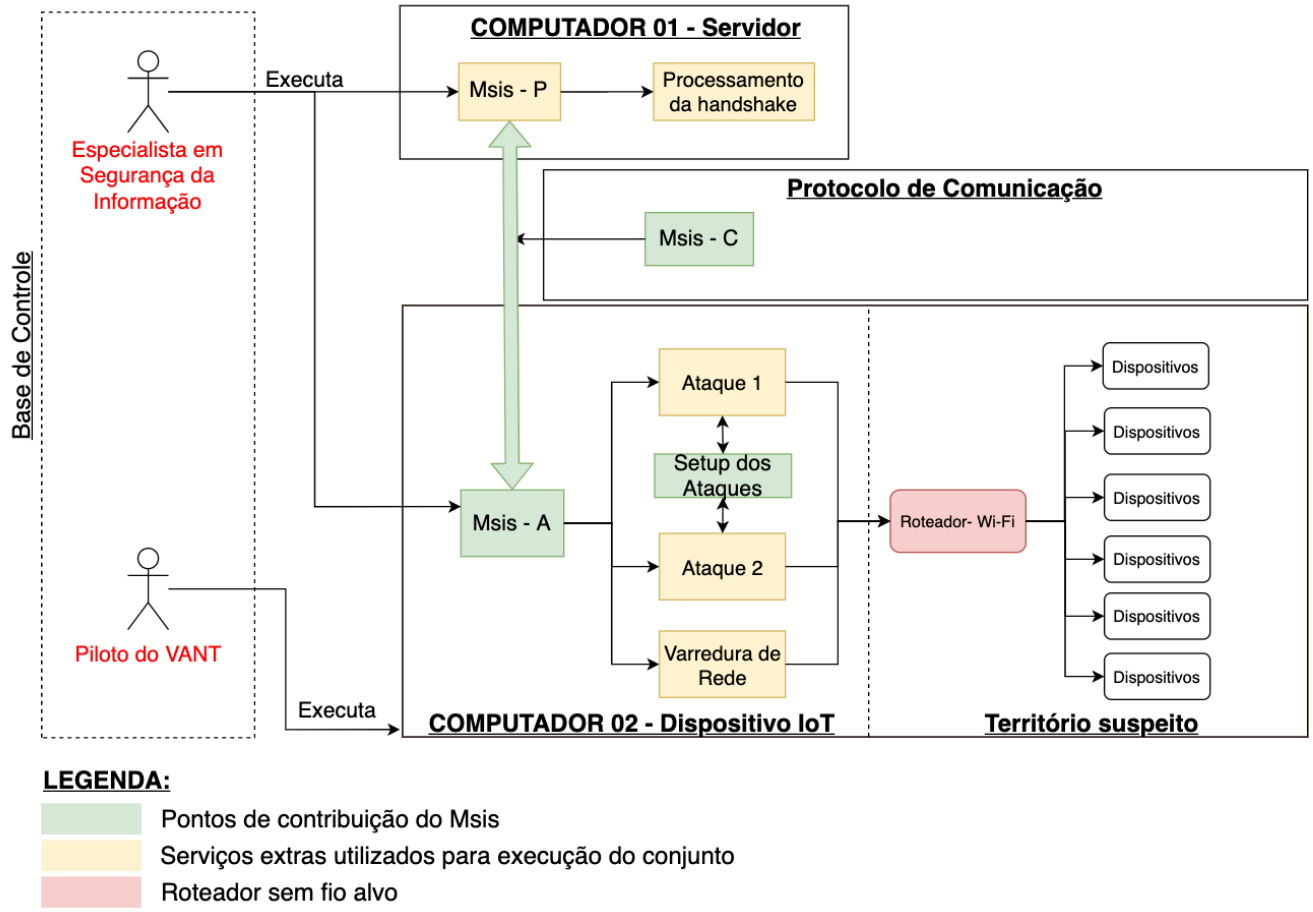
- Msis-P: esse módulo, que é executado no computador 01, conforme se observa na Figura 8. Recomenda-se que seja um equipamento com características de processamento elevado, uma vez que sua função é executar a quebra de senha, modelo adotado neste como o ataque de biblioteca, para comparar a *handshake* com uma variedade de possibilidades. O Msis-P não adentra sobre as melhores técnicas para a realização desse processo.

- Msis-A: este módulo que é representado na arquitetura no computador 02, conforme se observa na Figura 8. É executado em um dispositivo de IoT, ou seja, um equipamento com recursos de *hardware* limitado, seja em processamento, armazenamento, memória ou até outros. Equipamento no qual é adicionado a um VANT. A função deste módulo é de realizar a varredura de redes sem fio disponível em um determinado local, para posteriormente dar a opção ao operador, se o mesmo deseja realizar o ataque a determinada rede usando uma ou duas técnicas de ataque. No entanto, o operador pode escolher a alternativa de unificação de duas técnicas para realizar um ataque de maneira mais rápida e, também, com uma chance maior de sucesso.

- Msis-C: componente representado como protocolo de comunicação e localizado entre o Computador 1 e 2, conforme se observa na Figura 8. A sua importância na arquitetura é responsável por fazer a comunicação entre o módulo A e o P, comunicação que é existente para envio da *handshake* capturada pelo Msis-A, após seu ataque. Este módulo realiza a função de comunicação e, também, realiza a criptografia da *handshake* no ato do envio, também a descriptografia, após o recebimento ao módulo Msis-P. Este protocolo foi projetado para atuar juntamente com diversos tipos de criptografia, porém no modelo que foi escolhido para este é o Ccrypt, em função de sua estrutura e também a comunidade que atua em melhorias deste de forma contínua.

- Território suspeito: é o local no qual fica localizado o ponto onde será realizada a atividade de ataque. Neste ponto se encontram todos os dispositivos que serão atacados. A aproximação do VANT para essa área é de extrema importância para que o sinal da rede sem fio (Wi-Fi) seja adequado para o sucesso do ataque. Os possíveis territórios, que devem ser explorados, são de contextos relacionados às investigações e, também, aos apoios precisos das autoridades.

Figura 8 – Arquitetura do Msis, que demonstra o fluxo de informação e funcionamento entre os componentes e, também, a interação com os atores, representados pelo especialista em segurança da informação e o piloto do VANT. Os componentes do Msis se encontram classificados nas cores verde e amarelo. O destaque do Msis que visa contribuição se identifica na cor verde, assim o amarelo destaca ferramentas e infraestrutura já existentes no mercado. Já o alvo do ataque está representado pelas cores vermelho e branco

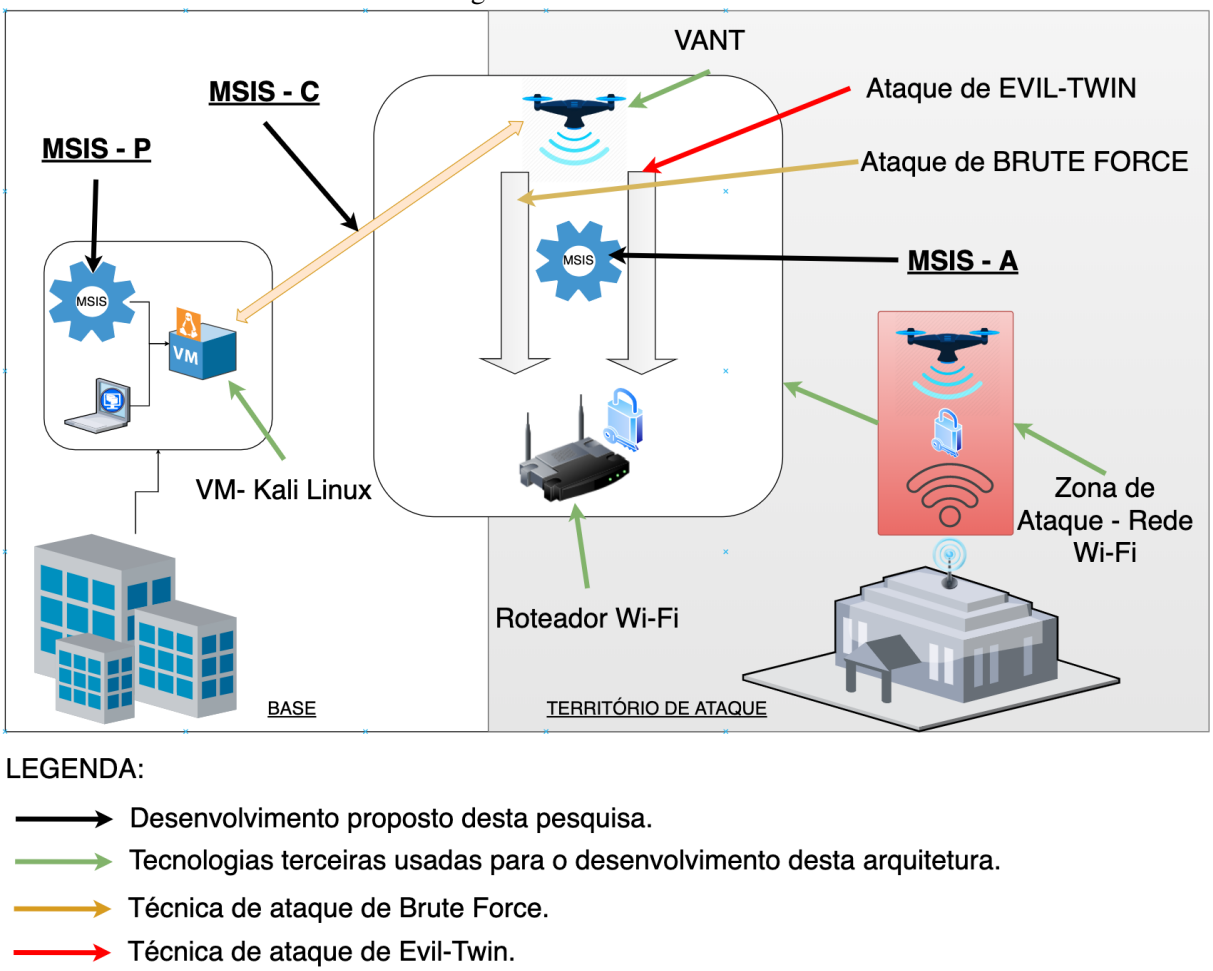


Fonte: Elaborado pelo autor.

4.3 Modelo do Msis

Nesta seção será apresentado o modelo do Msis, que está representado pela Figura 9, que está exibindo todo o cenário no qual o Msis será acoplado para fins de projeção de contribuição. Para facilitar a compreensão, abaixo da Figura 9 se localiza a legenda, que de forma objetiva exibe as setas de cor preta, ambas apontam para os pontos nos quais o modelo Msis tem como objetivo atuar.

Figura 9 – Modelo do Msis



Fonte: Elaborado pelo autor.

4.3.1 Msis-A

A variedade de dispositivos de IoT existentes, atualmente, é considerada elevada e ainda com expectativas deste número apenas crescer. Assim, soluções diversas surgem para explorar as mais diversas necessidades da sociedade, mas o fator que acaba sendo preocupante é a segurança desses dispositivos, ou dos dados que esses dispositivos geram, muitos ainda se encontram totalmente vulneráveis (SHWARTZ et al., 2018). O módulo Msis-A é desenvolvido para ser executado em uma arquitetura de dispositivos de IoT, usado para realizar a ação de ataques a determinadas redes sem fio (Wi-Fi).

Já na fase de pesquisas e definições de algumas técnicas para uso, tendo sido identificada a técnica chamada *Evil-Twin* essa que após alguns pontos importantes mencionados em (ISCTE-IUL et al., 2018) foi absorvida e implantada juntamente ao módulo, da mesma maneira que a técnica de *Brute Force* (GILLELA; PRENOSIL; Venkat Reddy, 2019) e (Bošnjak; Sreš; Brumen, 2018).

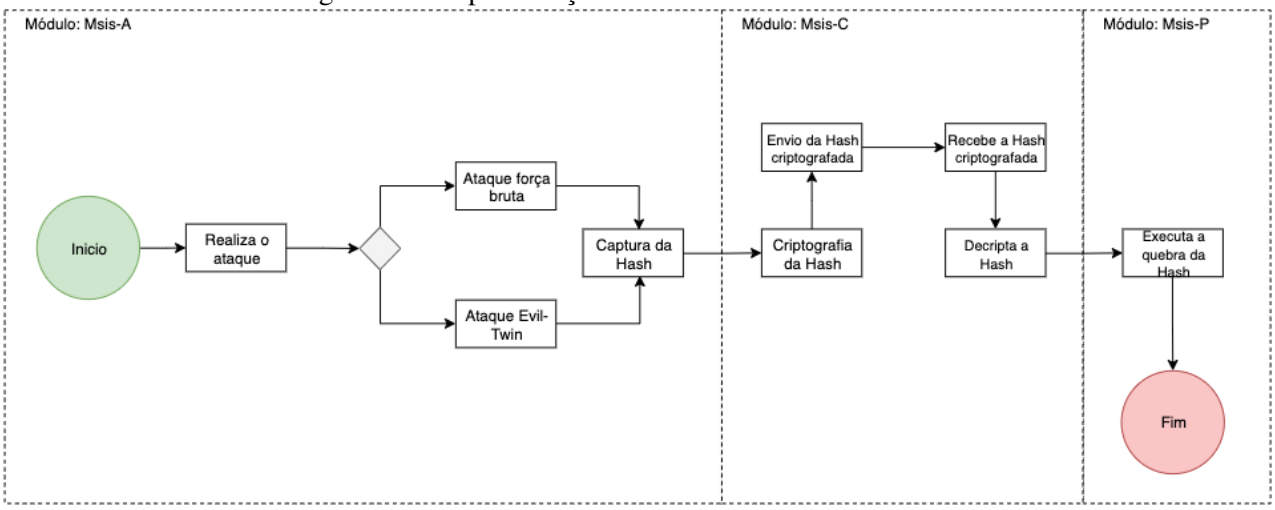
Na implantação das técnicas ao módulo foram possibilitadas as seguintes situações:

- Opção 1: ataque usando apenas a técnica *Brute Force*;
- Opção 2: ataque usando apenas a técnica *Evil-Twin*;
- Opção 3: um ataque usando as duas técnicas de forma simultânea.

As opções listadas acima têm como objetivo a captura da *handshake* para posterior quebra da *hash*, técnica que será tratada adiante. Neste momento, o Msis-A realiza o ataque, deixando a escolha do analista em segurança da informação acerca de qual das opções listadas acima usar. Após a execução dos ataques, a *handshake* é enviada através do Msis-C ao Msis-P para processamento e quebra da senha.

O Fluxo de dados que o modelo Msis desenvolveu é apresentado na Figura 10.

Figura 10 – Representação do fluxo de dados do Msis



Fonte: Elaborado pelo autor.

4.3.2 Msis-C

Existem diversos modelos e protocolos disponíveis para o uso em dispositivos de IoT, mas tamanha diversidade acaba gerando várias lacunas, entre essas é possível destacar a comunicação e a segurança. Em função das características dos dispositivos de IoT, se destaca a limitação de recursos computacionais, seja processamento, armazenamento e outros. Como resultado, muitos protocolos acabam sendo desenvolvidos e configurados para uma utilização mais objetiva, assim ignorando princípios de segurança (DIZDAREVIĆ et al., 2019) e (Basinya; Yushmanov, 2019).

O módulo em questão se torna responsável por fazer a comunicação e envio de dados entre os módulos Msis-A e Msis-P. Baseado nesta projeção e no formato da aplicação acerca do modelo Msis que é proposto, a questão de segurança para este procedimento é um requisito.

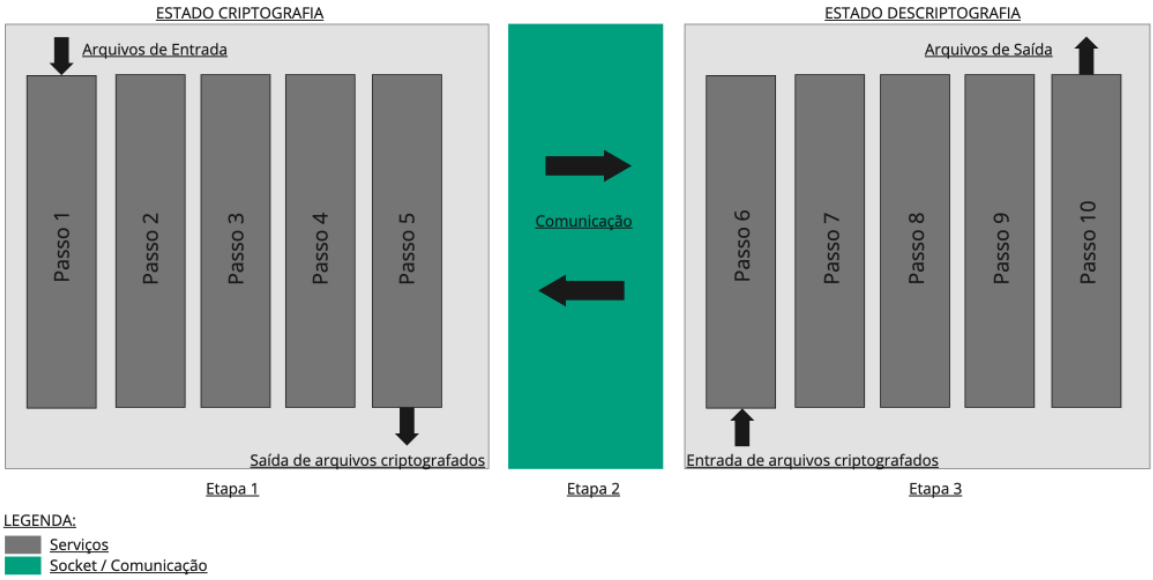
Depois de realizar algumas pesquisas na literatura foram identificados alguns modelos mais utilizados, como é o caso do MQTT e HTTP para projetos IoT (AL-JOBOURY; AL-HEMIARY, 2018).

No modelo atual, os dados que são gerados e transferidos têm características baseadas em arquivos mais densos com um fluxo de transição entre os módulos menores, em função do ponteiro de tempo. Levando em consideração a estrutura da aplicação sobre o dispositivo usado é que surge a alternativa de desenvolver seu próprio protocolo. Uma das lacunas dos protocolos de IoT é o cenário de segurança (DIZDAREVIĆ et al., 2019). Assim, de forma objetiva se foca na segurança dos dados em transmissão entre dispositivos de IoT e server. Para isso, se faz o uso de criptografia e, na sequência, aplicação de *socket* de comunicação.

Para descrever, de maneira mais completa, o fluxo de passos e serviços em decorrência das etapas que este protocolo foi arquitetado, abaixo esse será apresentado pela Figura 11, em que se tem o modelo com uma visão mais compacta, em função da elaboração dos passos. Na sequência são apresentadas as etapas de modo individual para descrever os serviços que são executados, sendo esses representados pelas Figuras 12, 13 e 14.

Figura 11 – Arquitetura do Protocolo Msis-C. Apresenta as três etapas e, também, de forma objetiva, os passos compostos dentro de cada etapa. Dentro de cada passo é executado um serviço, que será apresentado adiante com mais detalhes

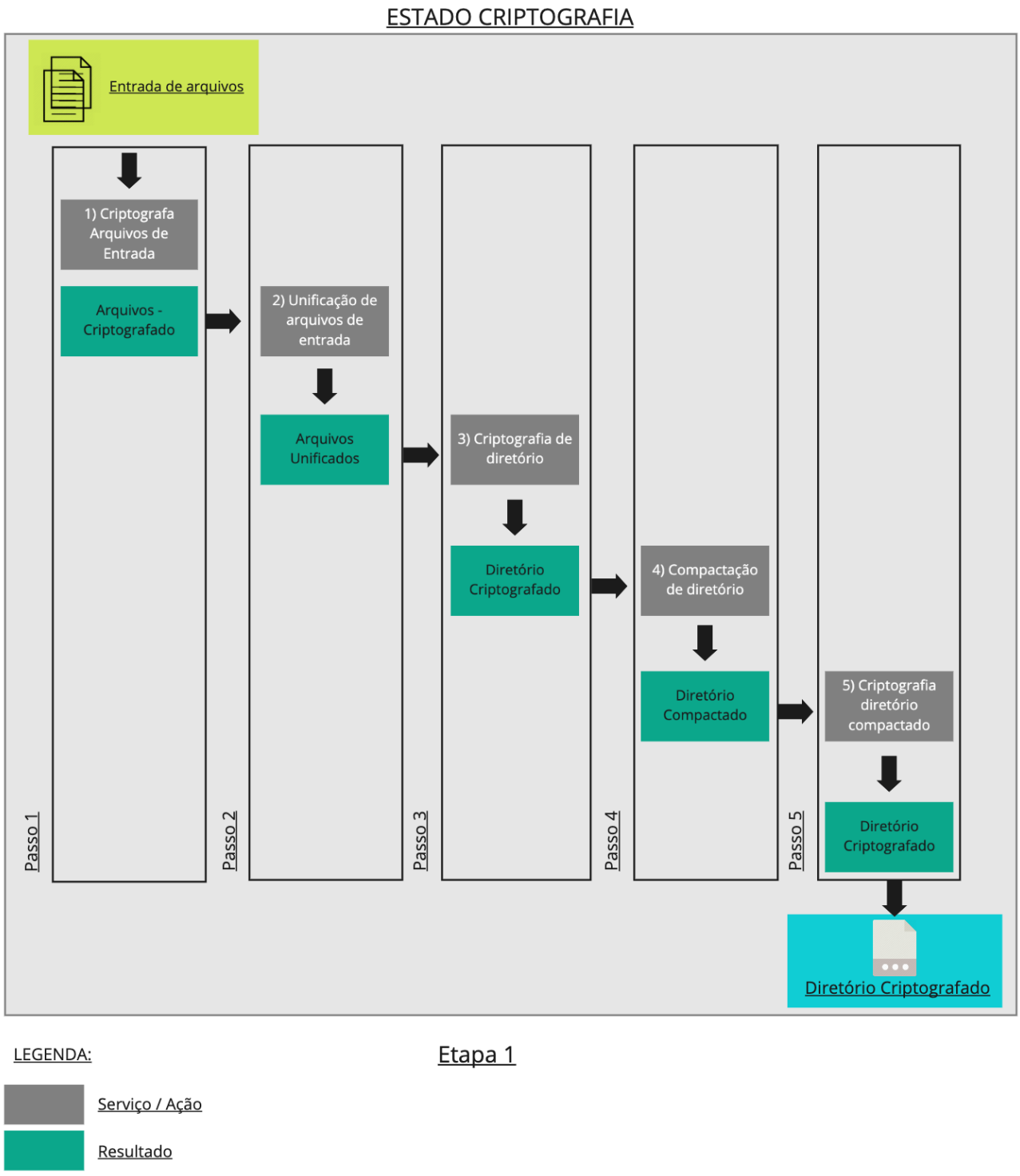
Fonte: Elaborado pelo autor



A Figura 12 exibe informações sobre a Etapa 1, na qual são descritos os serviços que são executados dentro de cada passo, e também apresenta os resultados que são obtidos após a execução desses. Os passos 1, 3 e 5 são responsáveis pela execução das camadas de criptografia.

Depois que a Etapa 1 é executada, os dados já se encontram criptografados, assim na sequência se tem o momento do envio das informações via internet para o local desejado, neste caso

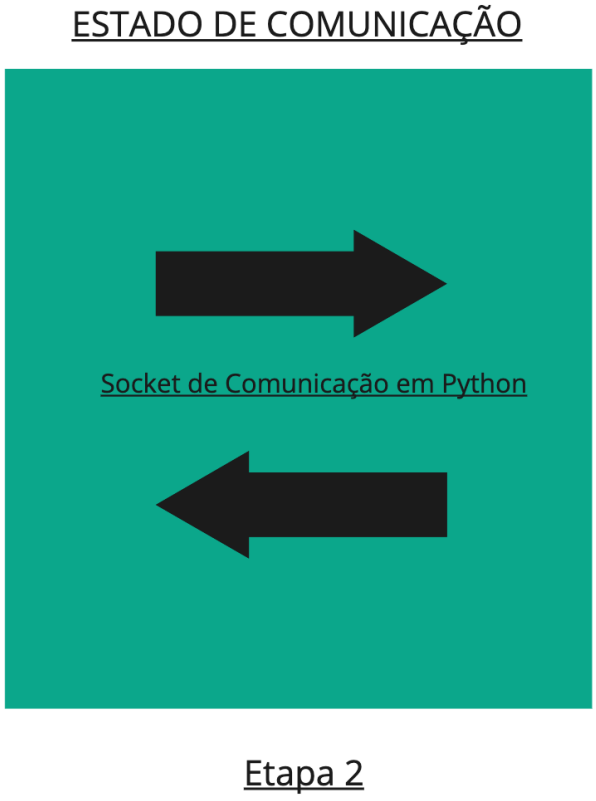
Figura 12 – Protocolo Msis-C - Etapa 1 - Dividida em cindo passos, representados pelo quadro cinza, que significa que serviço é executado sobre o dado que entra. Já pela cor verde se tem a exibição do resultado que o serviço anterior realizou. Dessa forma, a figura descreve os serviços que são explorados em cada passo. Etapa que é responsável por realizar a criptografia dos dados de entrada



Fonte: Elaborado pelo autor.

o servidor Msis-P. Assim, a Figura 13 demonstra a Etapa 2, na qual o fator comunicação é executado.

Figura 13 – Protocolo Msis-C - Etapa 2 - Etapa que representa o momento em que os dados são enviados do dispositivo de IoT para o servidor, com a utilização do protocolo de rede TCP/IP



Fonte: Elaborado pelo autor.

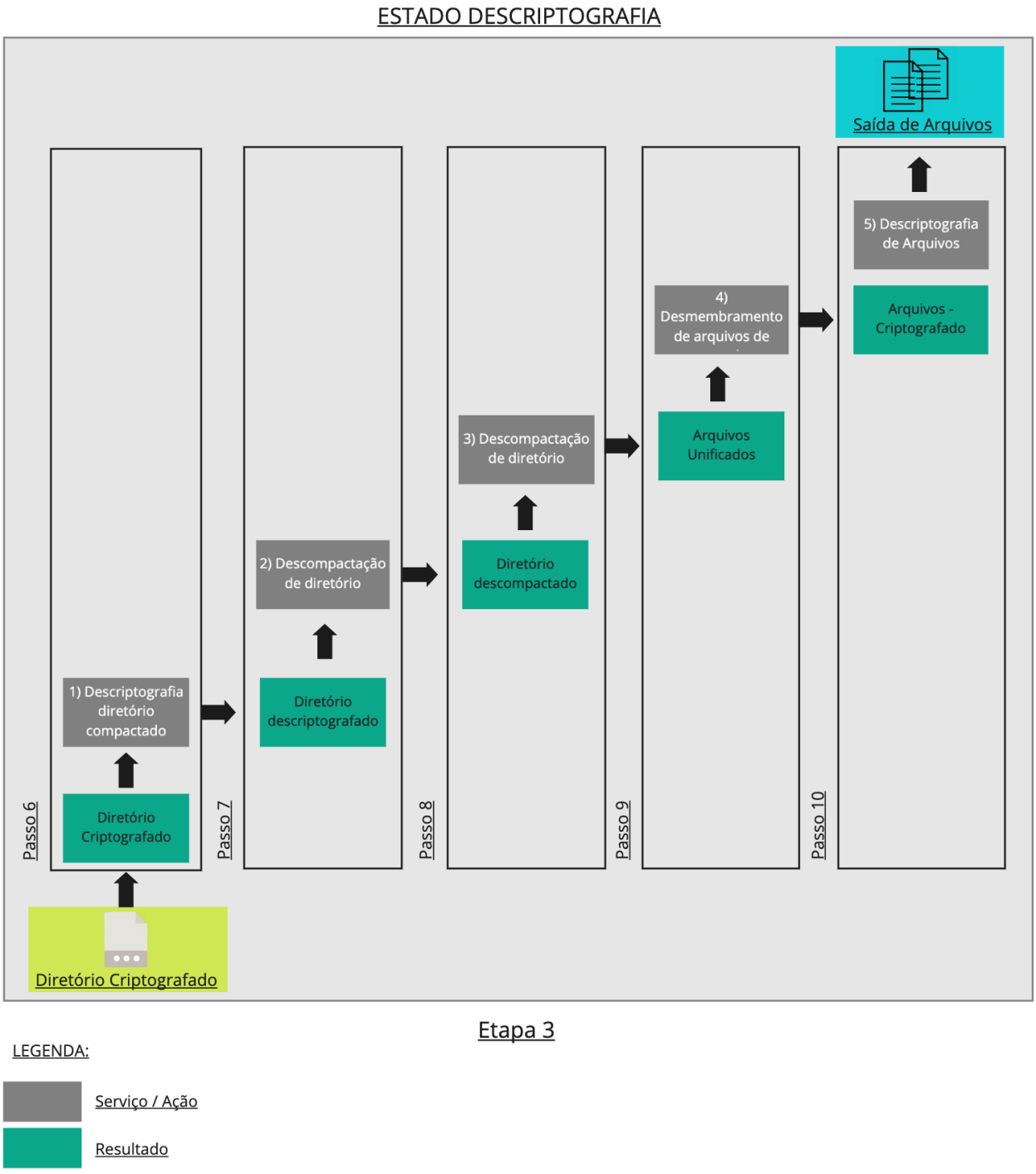
A Etapa 3, representada pela Figura 14 é a etapa final, momento em que são recebidos os dados criptografados. Os serviços são executados com finalidade de realizar a descriptografia dos dados. Como na Etapa 1 se seguiu uma lógica de organização dos dados, respeitando os passos, para realizar a descriptografia, esse processo é realizado de acordo com a estrutura elaborada.

4.3.3 Msis-P

Com a finalidade de usar a técnica de quebra de senha por dicionário, o módulo Msis-P é projetado para ser executado em uma camada externa ao local de onde opera o Msis-A. Levando em conta que a técnica de quebra de senha deste formato pode exigir várias técnicas e, também, um nível de poder computacional elevado.

Este modelo é um componente importante do Msis, lembrando que existem algumas maneiras mais abrangentes referentes às manipulações de bibliotecas de comparações. Prática de comparação da *handshake* recebida após a coleta do Msis-A.

Figura 14 – Protocolo Msis-C - Etapa 3 - Também é dividida em cinco passos, representados pelo quadro cinza, significa o serviço que é executado sobre o dado que é recebido. A cor verde é a exibição do resultado que o serviço anterior realizou no decorrer dos passos. Esta etapa é responsável por realizar a descriptografia dos dados recebidos



Fonte: Elaborado pelo autor.

4.4 Considerações Parciais

O modelo Msis apresentado visa atuar como um modelo para o auxílio na quebra de senha ou *handshake* de determinada rede sem fio (Wi-Fi). Dessa forma, esse modelo acaba se tor-

nando um protótipo um tanto extenso, pois as características que envolvem toda ação acabam ocorrendo em vários contextos. Sendo assim se apresentou um modelo que busca facilitar todo este envolvimento do processo, em que o foco mais dedicado foi na elaboração de ataques de forma unificada, ou seja, dois ataques ao mesmo tempo, isso para fins de agilidade, ganho de tempo e também no protocolo desenvolvido com finalidade de uma comunicação com características específicas para o tratamento de dados mais formatados, ou seja, um formato específico de arquivos juntamente com uma estratégia de elevar, em três níveis de criptografia, os dados a serem transitados de um dispositivo de IoT até um *Cloud Computing*.

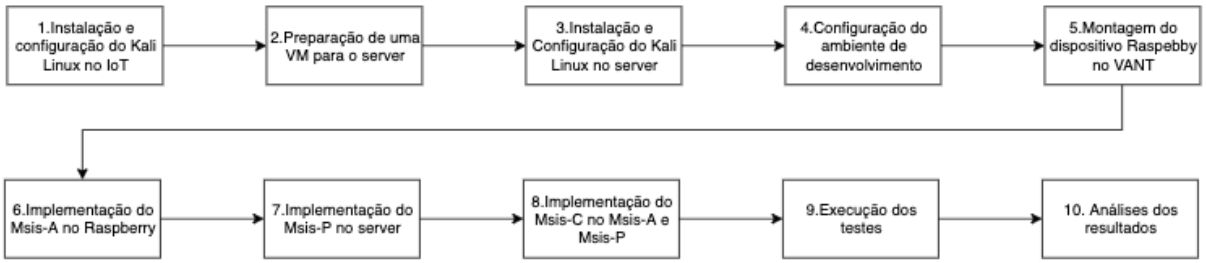
5 METODOLOGIA DE AVALIAÇÃO

O Msis é estruturado em três módulos, sendo esses desenvolvidos com finalidade de realizar o ataque, na sequência para realizar a comunicação e, por fim, para realizar o processamento de quebra de *hash*. Esses três módulos se complementam, assim tornando o protótipo capaz de realizar ação de ataque, fazer a comunicação da *hash* para o servidor de processamento de quebra de senha. Esse fluxo em poucos minutos. Dessa forma, o objetivo da avaliação é verificar se todo o fluxo de identificação e envio de dados ao servidor ocorre dentro do tempo estimado, levando em consideração agilidade e curto espaço de tempo de voo possível de um VANT, dispositivo que é usado para ação de aproximação do alvo. Sendo assim, na seção 5.1 é apresentado as etapas de desenvolvimento do modelo. A seção 5.2 descreve sobre implementação, para facilitar esta seção ela é dividida entre a seção 5.2.1 que é apresentado o protótipo e seus componentes e 5.2.2 que se detalham os testes que serão realizados com o modelo. Finalizando, na seção 5.3 se apresenta o ambiente de testes e, na seção 5.4 são apresentadas as métricas que serão utilizadas para a avaliação do modelo.

5.1 Etapas de desenvolvimento

Para facilitar a demonstração das etapas relacionadas ao desenvolvimento do protótipo, segue a Figura 15 exibida abaixo.

Figura 15 – Etapas do desenvolvimento do protótipo



Fonte: Elaborado pelo autor.

Seguindo as etapas, primeiramente foram realizadas a instalação e configuração do sistema operacional Kali Linux, tanto no *Raspberry Pi* quanto no servidor, etapas demonstradas pela representação 1, 2 e 3. No momento em que foi instalado o sistema operacional no *Raspberry Pi*, foram instaladas duas antenas (Wi-Fi) no mesmo, momento em que também foi realizada a atualização geral do sistema operacional (SO). O servidor do protótipo foi preparado em uma estação de trabalho Dell Optiplex 360. Não foi criado nenhum tipo de padrão de avaliação referente à escolha do VANT, sendo que as características de ambos não se dominam de forma trivial para a escolha.

Em um próximo momento foi realizada a configuração do ambiente de desenvolvimento,

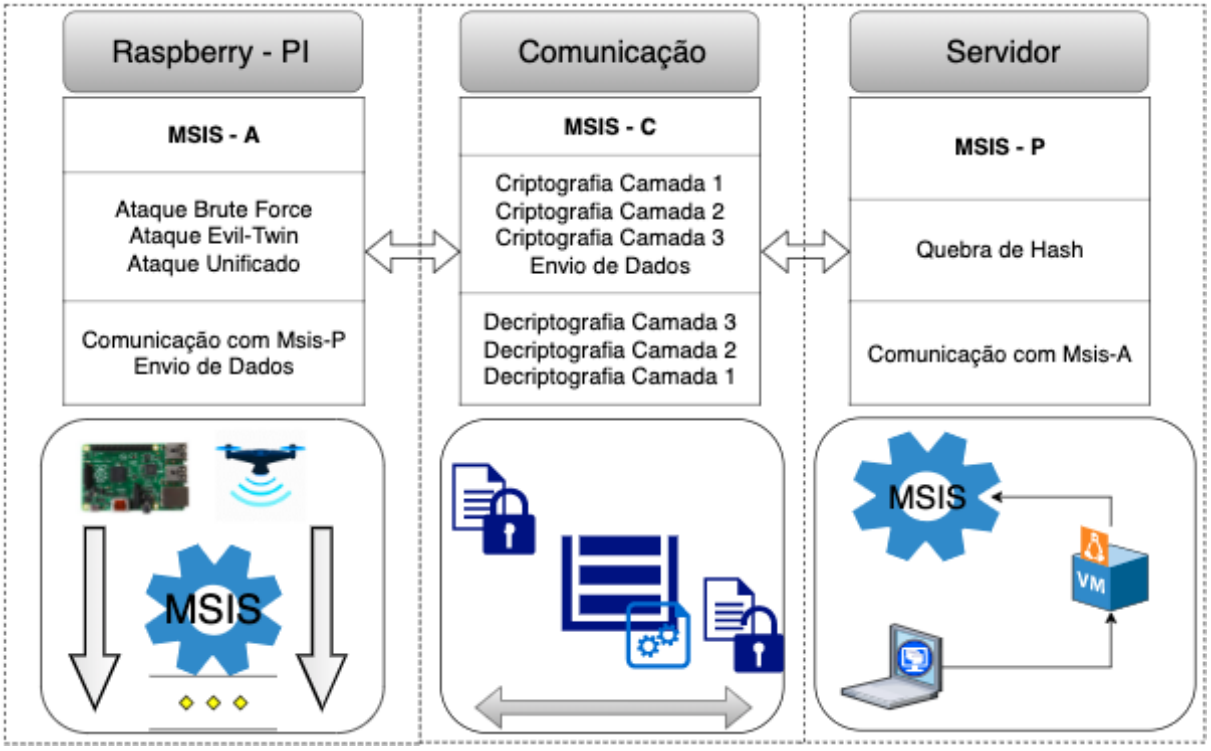
etapa demonstrada pela representação 4. Linguagem de programação escolhida para o protótipo foi Python e *Shell Script*. Na sequência foi realizada a acoplagem do *Raspberry Pi* ao VANT, juntamente com uma bateria extra, com finalidade de alimentar a energia do *Raspberry Pi*, etapa 5 da representação.

Na sequência entram as etapas de implementação dos módulos do Msis ao protótipo, começando pelo Msis-A, juntamente ao *Raspberry Pi*, após o Msis-P ao servidor e para finalizar o Msis-C em ambos componentes *Raspberry Pi* e server. Esses são representados pelas etapas 6, 7 e 8. Depois de todos os componentes devidamente instalados e configurados, teve início o momento de realizar os testes, assim, na sequência, foram feitas as análises dos resultados obtidos, que são apresentados no fluxo pelas etapas 9 e 10.

5.2 Implementação

Seção na qual serão detalhados alguns pontos do protótipo desenvolvido para a avaliação do modelo Msis. A Figura 16 exibe os três módulos do Msis com referências ao modelo, mas apresentando detalhes sobre suas funções, em decorrência dos locais de aplicabilidade sobre a arquitetura.

Figura 16 – Representação dos módulos do Msis, exibindo detalhes das funções que cada uma representa e, também, o local em que cada função é projetada



Fonte: Elaborado pelo autor.

5.2.1 Protótipo Desenvolvido

O protótipo foi desenvolvido nas seguintes linguagens de programação, Python e Shell Script, sendo dividido em três partes: Msis-A, Msis-C e Msis-P, em que cada uma atua, de forma individual, sobre cada dispositivo diferente e, por fim, ambos se complementam. Na Figura 16, na parte superior da mesma, foram listadas algumas observações de funcionalidades que cada módulo possui, e na parte inferior uma breve representação do ponto de atuação sobre o contexto do protótipo.

Na parte de desenvolvimento foi utilizada a linguagem Python e Shell Script, tendo sido realizada a utilização de bibliotecas, como: python.os, python.threading, python sockets, python.sys e crypt. Já referente aos sistemas operacionais, as escolhas foram baseadas nas necessidades decorrentes do protótipo. Sistemas voltados para as atividades específicas de *Pentesters*, nesse caso seria a versão Kali Linux, tanto para ser executada no *Raspberry Pi* quanto no servidor. Vale a ressalva que essa versão é de classificação OpenSource, ou seja, código aberto e sem custos.

Para realizar as técnicas de ataque, as funções utilizadas no Msis-A são as seguintes:

- airmon: [1]usado para manipulação do *status* da placa de rede.
- airbase-ng: [2] é uma ferramenta considerada mais ofensiva, realiza diversas operações destinadas aos ataques de redes.
- airodump-ng: [3] essa ferramenta já é usada para a captura de pacotes de frames.
- aireplay-ng: [4] pode-se dizer que sua função principal está na geração de tráfego para facilitar a coleta de dados de forma mais rápida.
- aircrack-ng: [5] pode executar mais de uma função, mas uma de suas principais está na captura de pacotes e na exportação desses para arquivos de texto. Também pode realizar a desautenticação de pontos em roteadores.

Os *hardwares* utilizados no protótipo são:

- VANT: marca Syma e modelo X8 PRO;
- Raspberry Pi 3 Model B+;
- Antenas de rede sem fio (Wi-Fi): 802.11n - Ralink Technology, Corp RT5370 Wireless Adapter;

[1]https://www.aircrack-ng.org_doku.php?id=pt-br:airmon-ng
[2]https://www.aircrack-ng.org_doku.php?id=airbase-ng
[3]https://www.aircrack-ng.org_doku.php?id=pt-br:airodump-ng
[4]https://www.aircrack-ng.org_doku.php?id=pt-br:aireplay-ng
[5]https://www.aircrack-ng.org

- Servidor: um computador *desktop* - Dell Optiplex 360 - com sistema operacional Kali Linux (64 Bits) - memória: 4 GB, 2 processador virtuais, disco rígido de 250GB;
- Bateria Portátil: Bateria de 4000 mA;
- Chip de telefonia móvel;

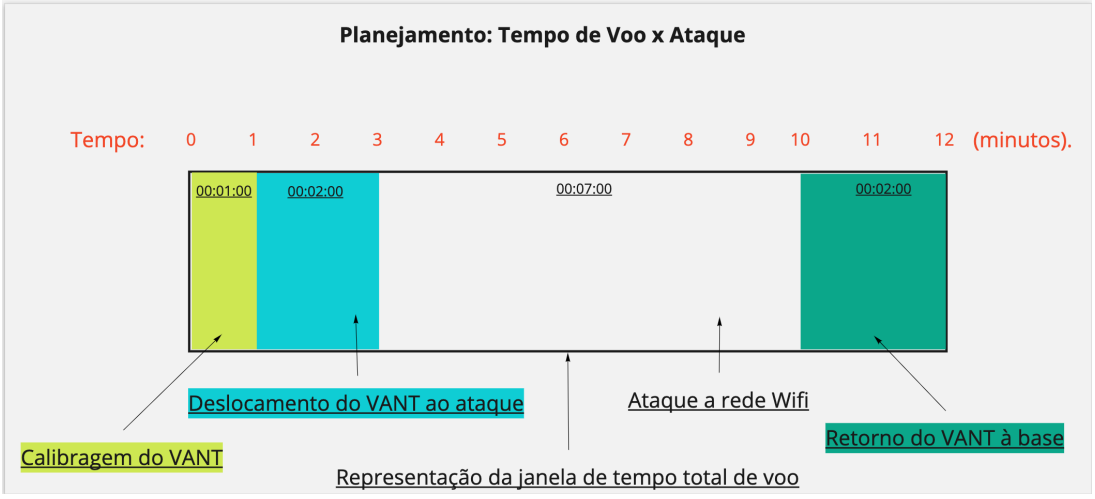
5.2.2 Ambiente de Simulação

O ambiente de simulação tem como objetivo fazer a avaliação do protótipo. A principal característica deste é a realização de um ataque a uma determinada rede sem fio (Wi-Fi), utilizando técnicas de ataques, protocolo de comunicação específico e um VANT. No momento em que o VANT é instanciado para a utilização tem um ponto fundamental que é preciso ser considerado, que é a autonomia de voo.

Para medir a autonomia geral do VANT e, assim, classificar todos os detalhes que devem ser levados em conta, a Figura 17 apresenta os ciclos de tempo projetados. O VANT que foi utilizado no protótipo possui uma autonomia considerada baixa. Para realizar a sua calibragem leva em torno de um minuto, para realizar o voo da sua base até o local do ataque leva praticamente dois minutos, sendo assim, o mesmo tempo foi considerado para retorno do VANT até a sua base. Dessa forma, a janela de tempo, que sobrou para realização do ataque, envolve o período de sete minutos.

Nesse momento é importante considerar que o dispositivo *Raspberry Pi* é anexado ao VANT, porém não consome carga de energia, pois é conectado a uma segunda bateria que também é anexada junto ao VANT. A limitação de autonomia desse não foi levada em consideração, pois possui um tempo mais elevado, assim não causando maiores problemas.

Figura 17 – Planejamento: Voo x Ciclos de tempo. Tempo total de 12 minutos, este foi dividido em alguns ciclos para poder levar em consideração uma estimativa mais precisa para realização do ataque



Fonte: Elaborado pelo autor.

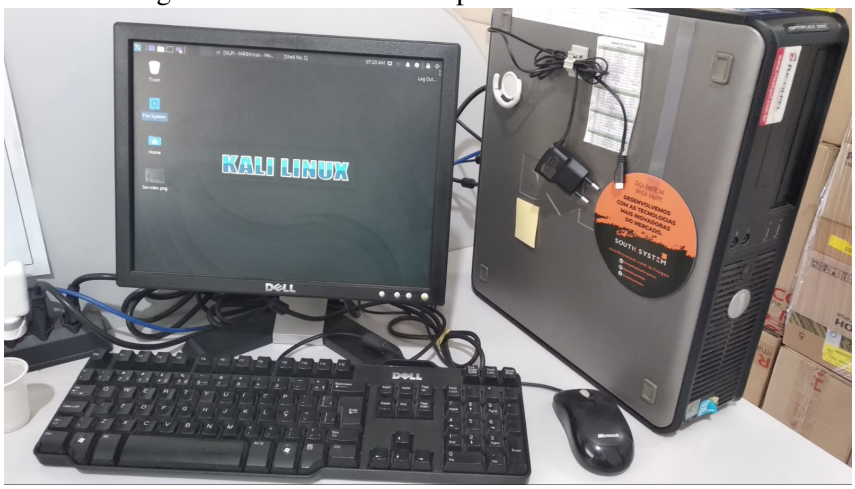
Outro ponto que será avaliado é o tempo em que os dados serão enviados do Msis-A ao Msis-P. Juntamente aos dados, também será avaliado o tamanho dos arquivos após serem criptografados em três camadas. Encerrando esta etapa se realiza a avaliação observando se os dados, que serão enviados entre os módulos, vão de fato cumprir o requisito de criptografia e, assim, não serem identificados como informações legíveis no ato da transferência.

5.3 Infraestrutura de Testes

O protótipo é elaborado sobre os seguintes itens:

- 1 Servidor: um computador *desktop* - Dell Optiplex 360 - com sistema operacional Kali Linux (64 Bits) - memória: 4 GB, 2 processador virtuais, disco rígido de 250GB;

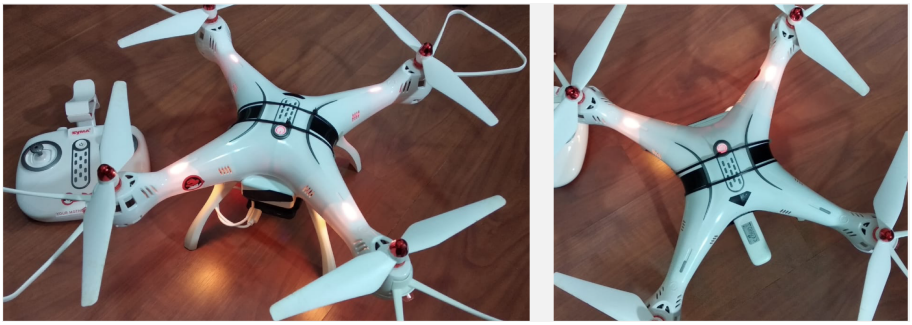
Figura 18 – Servidor usado para executar o Msis-P



Fonte: Elaborado pelo autor.

- 1 unidade - VANT: Syma X8 PRO;

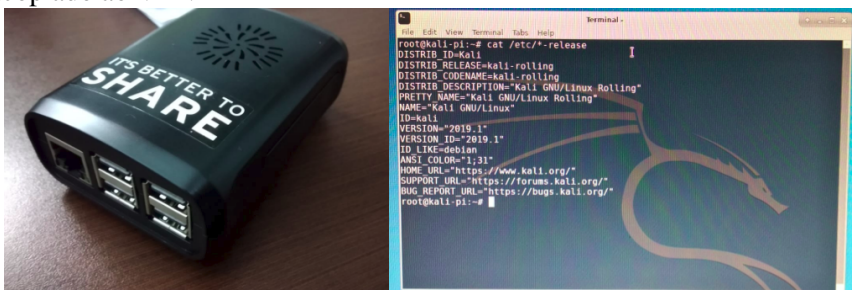
Figura 19 – VANT - Marca: SYMA, Modelo X8 PRO. Equipamento usado para realizar os testes desta pesquisa



Fonte: Elaborado pelo autor.

- 1 unidade - Raspberry PI 3 Model B+;

Figura 20 – Dispositivo *Raspberry Pi* geração 3 B+ usado para executar o Módulo Msis-A e também o Msis-C este é acoplado ao VANT



Fonte: Elaborado pelo autor

- 2 unidades - Antenas sem fio (Wi-Fi) adicionais: 802.11n - Ralink Technology, Corp. RT5370 Wireless Adapter;

Figura 21 – Antena adicional usada ao *Raspberry Pi*. Antena: Ralink Technology, Corp. RT5370 Wireless Adapter

Fonte: Elaborado pelo autor.

- 1 unidade - bateria portátil - 4.000mA.

Figura 22 – Bateria portátil usada para o funcionamento do *Raspberry Pi*. Bateria de 4.000 mA

Fonte: Elaborado pelo autor.

Ambiente de execução dos testes:

A infraestrutura pode ser dividida em duas partes, a primeira pode se denominar de laboratório, ou seja, um ambiente fechado, com equipamentos conectados o mais próximo possível do VANT. Já em um segundo momento, os testes foram levados a um ambiente externo, para que assim o VANT fosse ativado, tendo espaço físico para realizar o voo e se aproximar do local onde os equipamentos a serem atacados estivessem conectados a energia elétrica e configurados de acordo, simulando uma residência. Abaixo seguem listados os equipamentos que foram alvos de testes.

- 1 unidade - Marca: TP-Link - Modelo: TL-WR841ND - Roteador Wireless N300Mbps;
- 1 unidade - Marca: D-Link Modelo: DIR-615;
- 1 unidade - Marca: Technicolor e Modelo: TD5130.

5.4 Métricas de Avaliação

Primeiramente, será avaliado o sucesso da captura da *handshake*, após a execução da técnica unificada, que o Msis-A tem proposta de realizar. Esta técnica realiza o ataque a determinada rede, usando o ataque de *Brute Force* e também *Evil-Twin*, de forma paralela, utilizando *threads* de processamento para tal.

Em um segundo momento será avaliado o comportamento do protocolo Msis-C, aqui se dividindo em duas avaliações:

- a primeira avaliação é referente às informações capturadas e enviadas do dispositivo IoT para o servidor, ou seja, do módulo Msis-A ao módulo Msis-P, observando se está cumprindo com o requisito de dados criptografados. Detalhe em que é possível garantir que a ação seja realizada com total segurança, evitando qualquer tipo de *sniffer* de terceiros na rede Msis.
- a segunda avaliação é em relação ao tempo de transferência de dados criptografados, utilizando rede 4G disponível para o protótipo.

Na sequência e não menos importante estão os resultados com as características de autonomia do dispositivo utilizado no protótipo, o VANT. Será levado em consideração se é possível realizar tal ação dentro de um curto espaço de tempo. De tal forma que seja possível direcionar equipamentos de porte mais avançado ou de equipamentos mais simples, sendo esses capazes de realizar tal ação com sucesso.

5.5 Considerações parciais

Capítulo no qual foi apresentada a metodologia de avaliação do Msis, expondo sobre as etapas de desenvolvimento da pesquisa, de uma forma global, na sequência foram descritas as

características do protótipo em relação ao seu contexto previsto, ou seja, no cenário geral e quais os pontos nos quais o Msis atuará. Também foi descrito todo o protótipo, que é dividido em três módulos, ferramentas de *software* e *hardwares* utilizados nesse, explicando-se como é realizada a avaliação sobre o protótipo e os pontos relevantes. Assim, foram citados também aspectos sobre a infraestrutura geral a que os testes foram submetidos. E finalizando se apresenta a formatação das métricas que foram levadas em conta para avaliação do mesmo.

6 RESULTADOS

Nesse capítulo serão apresentados os resultados obtidos pelo modelo Msis. Os resultados apresentados são baseados na metodologia apresentada no capítulo 5. Assim este capitulo é dividido nas seguintes seções, 6.1 que descreve sobre os ataques reais que foram realizados em um ambiente externo. Na seção 6.2 é apresentado os resultados referente aos ataques realizados pelo Msis-A usando as três técnicas propostas na pesquisa. A seção 6.3 apresenta a diferença dos valores que foram encontrados na realização dos testes, tanto em laboratório como em execução real, como também os resultados dos arquivos criptografados pelo protocolo Msis-C. A comparação do estado da arte é apresentado na Seção 6.4. Finalizando com a seção 6.5 as considerações parciais.

6.1 Ataques realizados em redes sem fio (Wi-Fi)

Como o modelo projeta a captura da *hash* de uma determinada rede sem fio (Wi-Fi), os testes que foram executados para a coleta destes dados são divididos na seguinte ordem:

- Ataque Unificado: utilização de *Threads* para executar duas técnicas de invasão de forma paralela;
- Ataque *Evil-Twin*: utilizando apenas a técnica de *Evil-Twin*.
- Ataque *Brute Force*: utilizando apenas a técnica de *Brute Force*.

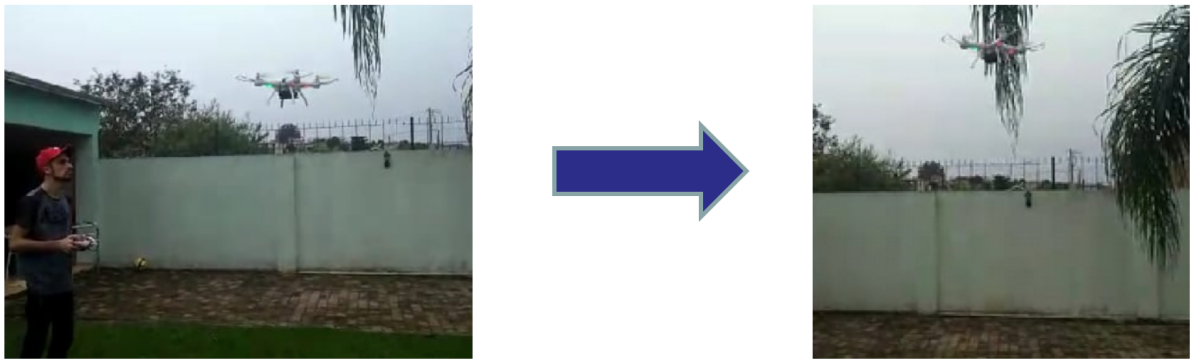
Nesta etapa dos testes foram executados "n"ataques a uma determinada rede, utilizando um VANT como meio de aproximação do alvo, todas as tentativas que foram realizadas tiveram sucesso na captura da *hash*, assim como o envio dos dados entre o módulo Msis-A e o Msis-P. Para a realização de cada ataque foi concluído todo o ciclo de ação que envolve este. Ciclo que se inicia do momento em que é ligado o VANT, sendo assim realizado o deslocamento do mesmo até o alvo, desenvolvendo a varredura de redes, dando início ao ataque, sendo esse finalizado, com os dados criptografados, sendo enviados os mesmos para o servidor e, assim, retornando com o VANT para o seu ponto de decolagem.

Todas as ações dos testes foram executadas em um ambiente real, porém controlado, os dispositivos que o VANT realizou os ataques são para finalidade acadêmica, assim não infringindo nenhum tipo de conexão ou rede de terceiros. O VANT teve uma altitude de aproximadamente 2,5 a 3,5 metros em relação ao solo e uma variação de 4,5 a 6,0 metros do alvo, o roteador. No ato em que os ataques estavam em execução, o mesmo permaneceu no ar.

Figura 23 – Dispositivo em testes. VANT - Ponto de decolagem e pouso

Fonte: Elaborado pelo autor.

Figura 24 – Dispositivo em testes. VANT no momento de seu percurso ao ponto de ataque



Fonte: Elaborado pelo autor.

6.1.1 Ataque unificado Msis-A: utilização de *Threads* para executar duas técnicas de invasão de forma paralela;

A primeira etapa teve início com o Msis-A, sua proposta é a de realizar os ataques usando duas técnicas simultaneamente, sendo possível esta ação em decorrência do contexto dos ataques, que foram divididos por *Threads* para que assim suas funções pudessem ser executadas no mesmo momento.

Para documentar os testes foi elaborada a Tabela 2 e a mesma dividida em seis colunas. A primeira coluna apresenta o número de tentativas de ataques. A segunda e terceira coluna

apenas marcam um "X"indicando se o modelo que está em execução foi configurado para a utilização de *Threads*. A quarta coluna está informando quatro estágios, sendo que as linhas que estão em branco são padrão, pois pertencem à operação real do VANT. Assim, apenas são alterados os dados referentes às linhas que se encontram marcadas na cor azul. Seguindo para a próxima coluna se tem o tempo de cada etapa. Finalizando com o tempo total programado para que este conjunto de operações seja executado dentro do tempo descrito.

Para a execução dessa bateria de testes, levando em conta apenas essa modalidade de ataque, Msis-A, foram realizadas oito tentativas de ataque. Cada tentativa corresponde a um ciclo completo, isso significa que o VANT precisou realizar a decolagem e se deslocar até seu alvo, dessa mesma maneira realizar os passos que constam descritos na Tabela 2, que são de preparação do VANT, ataque a rede sem fio e na sequência o envio dos dados para o Msis-P.

Tabela 2 – Valores referentes ao ataque paralelo

Nº Tentativa(s)	**Utilização de Threads**		**Descrições / Etapas**	**Tempo**	**Tempo Limite do Ciclo**
	Sim	**Não**			
1	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:03:00	
			Config/Envio dados	00:01:00	
2	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:02:00	
			Config/Envio dados	00:01:00	
3	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:01:00	
			Config/Envio dados	00:01:00	
4	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:00:30	
			Config/Envio dados	00:01:00	
5	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:04:00	
			Config/Envio dados	00:01:00	
6	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:01:00	
			Config/Envio dados	00:01:00	
7	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:02:00	
			Config/Envio dados	00:01:00	
8	X		Preparação / Conf	00:01:00	00:07:00
			Brute Force Evil-Twin	00:03:00	
			Config/Envio dados	00:01:00	

Fonte: Elaborado pelo autor.

6.1.2 Ataque *Brute Force*:

A segunda etapa segue com a técnica de ataque conhecida como *Brute Force*. A Tabela 3 também apresenta as mesmas características de organização e informações que a Tabela 2. Para a execução dessa bateria de testes, levando em conta apenas essa modalidade de ataque, *Brute Force*, foram realizadas oito tentativas de ataque. Cada tentativa corresponde a um ciclo completo, isso significa que o VANT precisou realizar a decolagem e se deslocar até seu alvo, dessa mesma maneira realizando os passos que constam descritos na Tabela 3, que são de preparação e de configuração do ataque, ataque e envio dos dados para o Msis-P.

Tabela 3 – Valores referentes ao ataque usando a técnica *Brute Force*

Nº Tentativa(s)	**Utilização de Threads**		**Descrições / Etapas**	**Tempo**	**Tempo Limite do Ciclo**
	Sim	**Não**			
1		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:03:00	
			Config/Envio dados	00:01:00	
2		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:02:00	
			Config/Envio dados	00:01:00	
3		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:06:00	
			Config/Envio dados	00:01:00	
4		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:03:00	
			Config/Envio dados	00:01:00	
5		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:02:00	
			Config/Envio dados	00:01:00	
6		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:01:00	
			Config/Envio dados	00:01:00	
7		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:04:00	
			Config/Envio dados	00:01:00	
8		X	Preparação / Conf	00:01:00	00:07:00
			Brute Force	00:04:00	
			Config/Envio dados	00:01:00	

Fonte: Elaborado pelo autor.

6.1.3 Ataque *Evil-Twin*:

A terceira etapa segue com a técnica de ataque conhecida como *Evil-Twin*. A Tabela 4 também exibe as mesmas características das tabelas apresentadas pelos testes anteriores, diferenciando-se apenas os valores que foram apresentados ao longo dos testes juntamente com as diferentes abordagens.

Para a execução dessa bateria de testes, levando em conta apenas essa modalidade de ataque, *Evil-Twin*, foram realizados oito ataques. Cada ataque corresponde a um ciclo completo, isso significa que o VANT precisou realizar a decolagem e se deslocar até seu alvo, dessa mesma maneira realizar os passos que constam descritos na Tabela 4, que são de preparação e de configuração do ataque, ataque e envio dos dados para o Msis-P.

Tabela 4 – Valores referentes ao ataque usando a técnica *Evil-Twin*

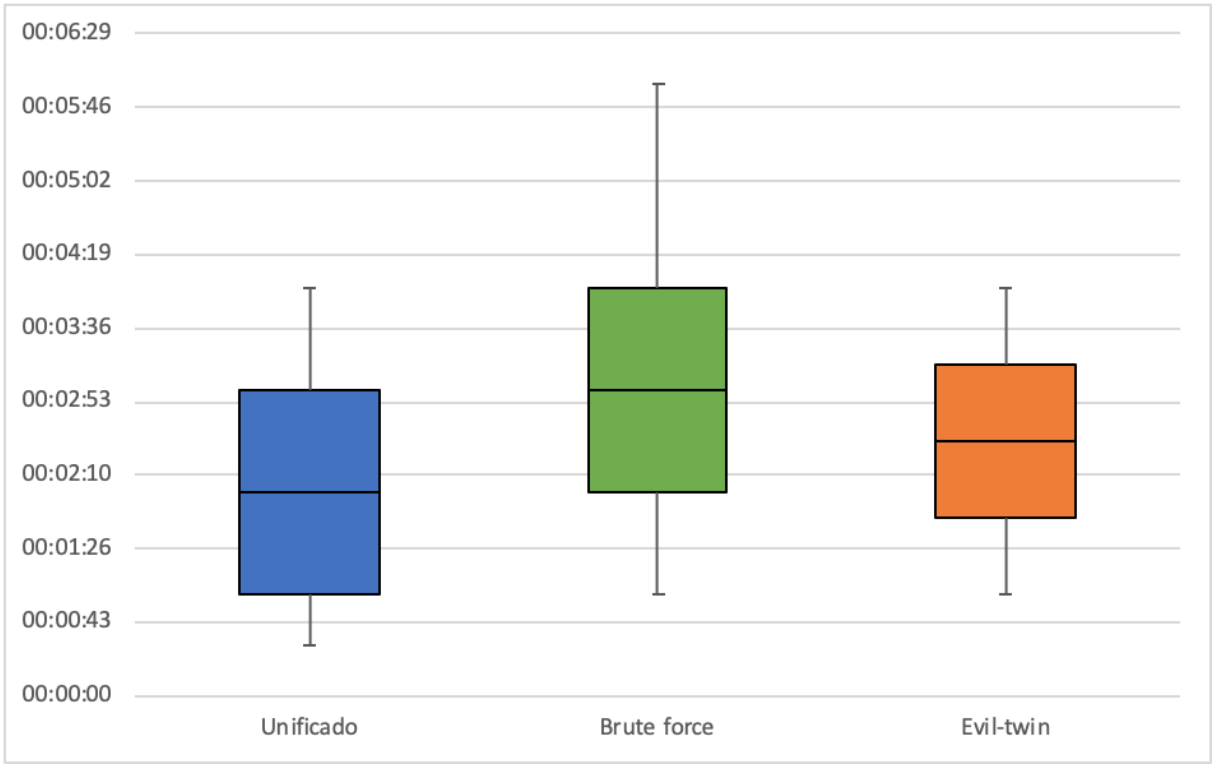
Nº Tentativa(s)	**Utilização de Threads**		**Descrições / Etapas**	**Tempo**	**Tempo Limite do Ciclo**
	Sim	**Não**			
1		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:01:00	
			Config/Envio dados	00:01:00	
2		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:02:00	
			Config/Envio dados	00:01:00	
3		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:03:00	
			Config/Envio dados	00:01:00	
4		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:04:00	
			Config/Envio dados	00:01:00	
5		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:01:00	
			Config/Envio dados	00:01:00	
6		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:02:00	
			Config/Envio dados	00:01:00	
7		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:03:00	
			Config/Envio dados	00:01:00	
8		X	Preparação / Conf	00:01:00	00:07:00
			Evil-Twin	00:04:00	
			Config/Envio dados	00:01:00	

Fonte: Elaborado pelo autor.

6.2 Resultados dos ataques realizados pelo Msis-A: ataques paralelo usando *Threads*

Após realizar a coleta dos dados das diferentes técnicas de ataques e apresentação dos resultados nas tabelas anteriores, a Figura 25 apresenta os valores no modo gráfico, comparando os três formatos de ataques, unificado, *Brute Force* e *Evil-Twin*.

Figura 25 – Apresenta a relação entre os três tipos de ataques realizados, informações divididas por tipos de ataque x tempo de execução



Fonte: Elaborado pelo autor.

No ataque unificado, a representação do valor mínimo é abaixo das técnicas de *Brute Force* e *Evil-Twin*, o valor foi de trinta segundos com relação a um minuto das duas outras técnicas. Com relação ao valor máximo a técnica de unificação e *Evil-Twin* se igualaram nos quatro minutos, tempo menor que a técnica de *Brute Force* que chegou nos seis minutos. Analisando a mediana das três técnicas, o ataque unificado ficou com o tempo em dois minutos, já *Brute Force* chegou em três minutos e *Evil-Twin* em dois minutos e trinta segundos, visualizando estes dados, pode-se concluir a vantagem da técnica, unificado em relação a *Brute Force* e *Evil-Twin*.

6.3 Resultados do protocolo Msis-C: criptografia x tamanho de arquivos

Seção que vai exibir as duas camadas de testes, realizados sobre o protocolo Msis-C. Iniciando pela observação do comportamento de arquivos, que são submetidos à criptografia com posterior validação dos testes feitos sobre a transferência de arquivos criptografados.

6.3.1 Resultados da quantidade de arquivos x camadas de criptografia x tamanho dos arquivos

A Tabela 5 exibe os resultados realizados no desenvolvimento de testes que atuam na quantidade de arquivos e aplicam as três camadas de criptografia para assim visualizar o tamanho total do arquivo final criptografado.

Tabela 5 – Tabela Comparativa: Arquivos Criptografados x Camadas de Criptografia x Tamanho

Sem Criptografia			**Criptografia 1**		**Criptografia 2**		**Criptografia 3**	
Arquivos			**Arquivos**		**Diretório**		**Diretório Zipado**	
Qtd	**Tamanho**	**Total**	**Qtd Arq**	**Tamanho**	**Qtd Arq**	**Tamanho**	**Qtd Arq**	**Tamanho**
1	1byte	1byte	1	33bytes	1	65bytes	1	433bytes
1	2bytes	2bytes	1	34bytes	1	66bytes	1	434bytes
1	11bytes	11bytes	1	43bytes	1	75bytes	1	443bytes
1	434bytes	434bytes	1	466bytes	1	498bytes	1	866bytes
1	1MB	1MB	1	1MB	1	1MB	1	1MB
1	2,65MB	2,65MB	1	2,65MB	1	2,65MB	1	2,65MB
5	2,65MB	13,3MB	5	13,3MB	5	13,3MB	5	13,26MB
10	2,65MB	26,5MB	10	26,5MB	10	26,5MB	10	26,53MB
20	2,65MB	53MB	20	53MB	20	53,1MB	20	53,06MB
30	2,65MB	79,6MB	30	79,6MB	30	79,6MB	30	79,59MB
50	2,65MB	132,6MB	50	132,6MB	50	132,6MB	50	132,65MB

Fonte: Elaborado pelo autor.

Como o protocolo Msis-C realiza três camadas de criptografia nos dados, estes que são enviados do Msis-A para o Msis-P. O objetivo destes testes é de validar o comportamento de um determinado arquivo que é submetido a esta ação de criptografia. A Tabela 5 é dividida em algumas partes, sendo essas:

- Camada sem criptografia: na qual se encontra listada a quantidade de arquivos e o tamanho desses.
- Camada de criptografia 1: na qual está listada a quantidade de arquivos e o tamanho dos mesmos após aplicar a primeira camada de criptografia.
- Camada de criptografia 2: lista a quantidade de arquivos e o tamanho desses, com informações geradas após o arquivo passar pela segunda camada de criptografia.
- Camada de criptografia 3: novamente se tem lista da quantidade de arquivos e apresenta o valor final do arquivo ou dos arquivos. Nesse momento já se encontra finalizada a aplicação da terceira camada.

Observando os dados lançados na tabela anterior, esses mostram que o protocolo Msis-C eleva o tamanho dos arquivos após aplicar as camadas de criptografia. Estes resultados para o protótipo Msis é totalmente aceitável. Para aplicar o protocolo Msis-C em outros ambientes se deve fazer uma análise para verificar a viabilidade de aplicação deste.

Em destaque, na Tabela 5, na cor amarela, é perceptível que arquivos muito pequenos acabam se tornando arquivos mais densos. Já arquivos com um tamanho mais elevado, o resultado se mostrou pouco relevante, uma vez que se ganha como benefício um arquivo criptografado e, assim, garantindo que terceiros não consigam interpretá-los.

6.3.2 Resultados dos arquivos gerados pelo ataque Msis x criptografia

Os resultados que estão sendo apresentados na Tabela 6 são oriundos da seção de oito ataques realizados em cenário real. Estes dados estão sendo representados com base nos formatos dos ataques que foram realizados. Ataque unificado, proposto nesta pesquisa, ação realizada usando duas técnicas de ataques em paralelo. Ataque de *Brute Force*, ação que é oriunda usando apenas esta técnica. Finalizando com o ataque *Evil-Twin*, ação especifica desta técnica.

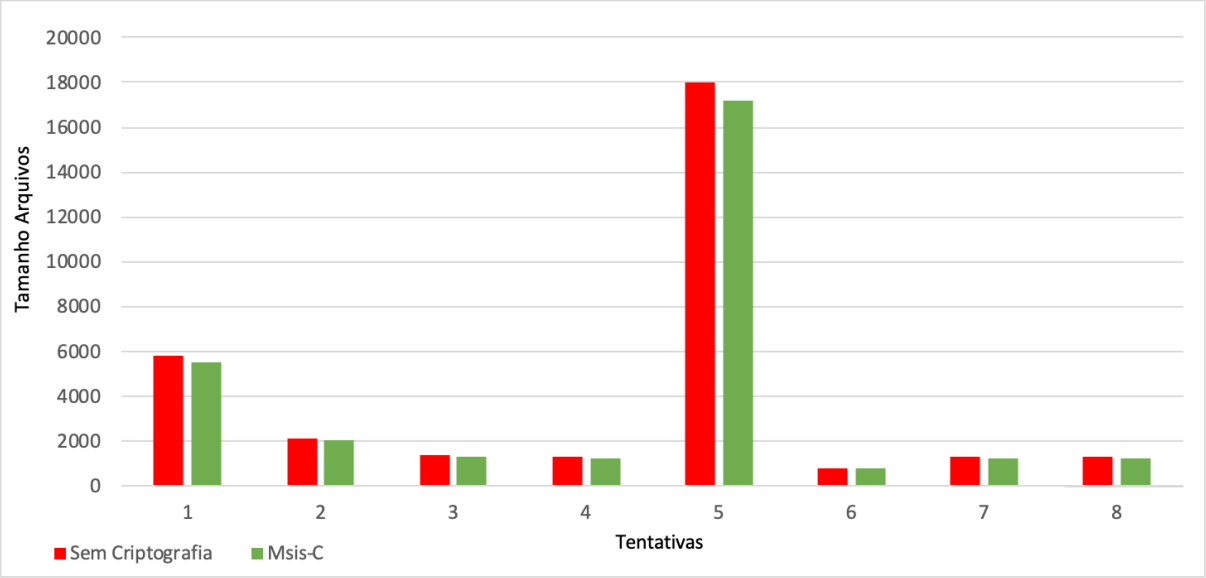
Dentro de cada formato de ataque é apresentado os dados com base nas informações seguintes, sem criptografia e utilizando o protocolo Msis-C. Todos os dados que são exibidos na Tabela 6 foram extraídos em tempo real dos ataques realizados. Para apresentar uma média geral, é destacado na cor em amarelo a última linha da tabela.

Tabela 6 – Comparação de dados sem criptografia x Msis-C

Tentativas	**Ataque Unificado**		**Ataque Brute Force**		**Ataque Evil-Twin**	
	Sem Criptografia	**Msis-C**	**Sem Criptografia**	**Msis-C**	**Sem Criptografia**	**Msis-C**
1	5836,8 kb	5529,6 kb	3891,2 kb	3788,8 kb	12390,4 kb	11878,4 kb
2	2108,4 kb	2048 kb	1331,2 kb	1331,2 kb	6451,2 kb	6144 kb
3	1387 kb	1331,2 kb	8294,4 kb	7884,8 kb	4608 kb	4403,2 kb
4	1274,5 kb	1228,8 kb	826,3 kb	808 kb	3993,6 kb	3788,8 kb
5	18022,4 kb	17203,2 kb	657 kb	642,6 kb	3993,6 kb	3788,8 kb
6	770,2 kb	753,6 kb	332 kb	325,2 kb	4710,4 kb	4505,6 kb
7	1273,4 kb	1228,8 kb	5222,4 kb	5017,6 kb	3788,8 kb	3686,4 kb
8	1282,6 kb	1228,8 kb	2252,8 kb	2150,4 kb	8089,6 kb	7680 kb
Média	**3994 kb**	**3819 kb**	**2851 kb**	**2744 kb**	**6003 kb**	**5734 kb**

O gráfico representado pela Figura 26 exibe as informações com relação ao tipo de ataque unificado que é apresentado pela Tabela 6. Com o objetivo de facilitar a interpretação das informações, destaca-se em vermelho os dados que foram transferidos sem ação de criptografia, e representados pela cor verde os dados que foram transferidos utilizando o protocolo Msis-C.

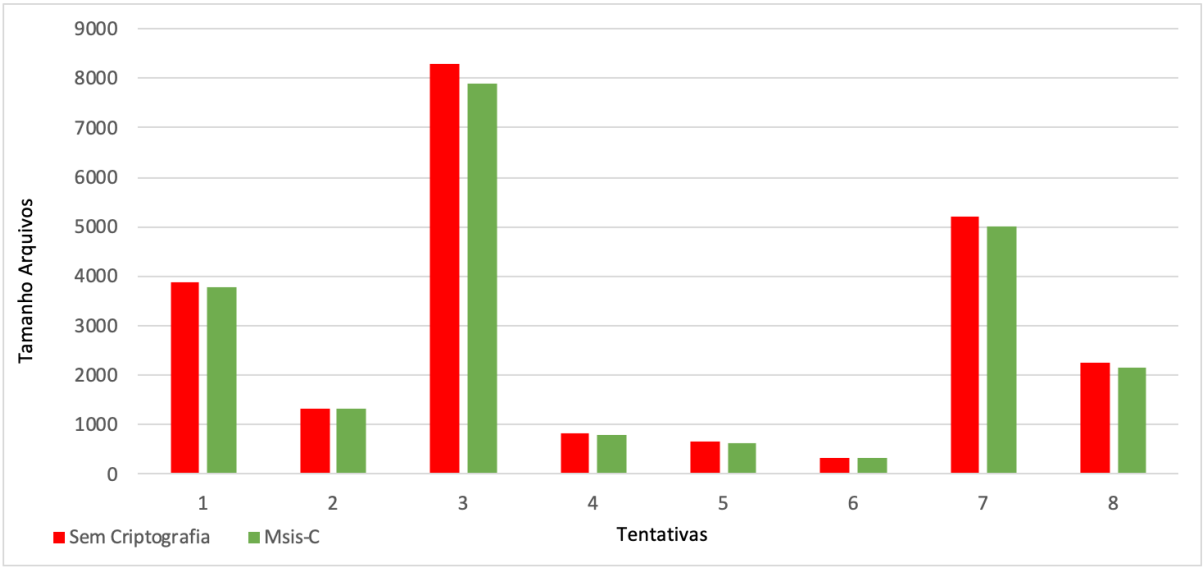
Figura 26 – Ataque Unificado: Comparação de dados sem criptografia x Msis-C



Fonte: Elaborado pelo autor.

O gráfico representado pela Figura 27 exibe as informações com relação ao tipo de ataque *Brute Force*, este também é apresentado na Tabela 6. Com o objetivo de facilitar a interpretação das informações, destaca-se em vermelho os dados que foram transferidos sem ação de criptografia, e representados pela cor verde os dados que foram transferidos utilizando o protocolo Msis-C.

Figura 27 – Ataque *Brute Force*: Comparação de dados sem criptografia x Msis-C

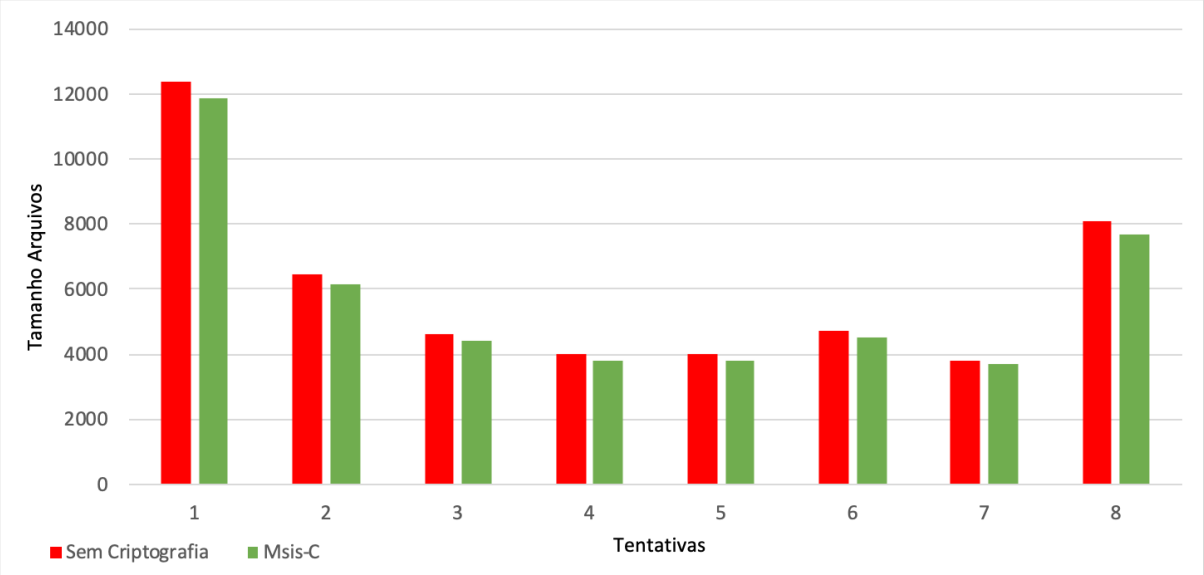


Fonte: Elaborado pelo autor.

Finalizando o gráfico representado pela Figura 28 exibe as informações com relação ao tipo de ataque *Evil-Twin*. Seguindo as mesmas regras citadas anteriormente visando facilitar

a interpretação das informações, destaca-se em vermelho os dados que foram transferidos sem ação de criptografia, e representados pela cor verde os dados que foram transferidos utilizando o protocolo Msis-C.

Figura 28 – Ataque *Evil-Twin*: Comparação de dados sem criptografia x Msis-C



Fonte: Elaborado pelo autor.

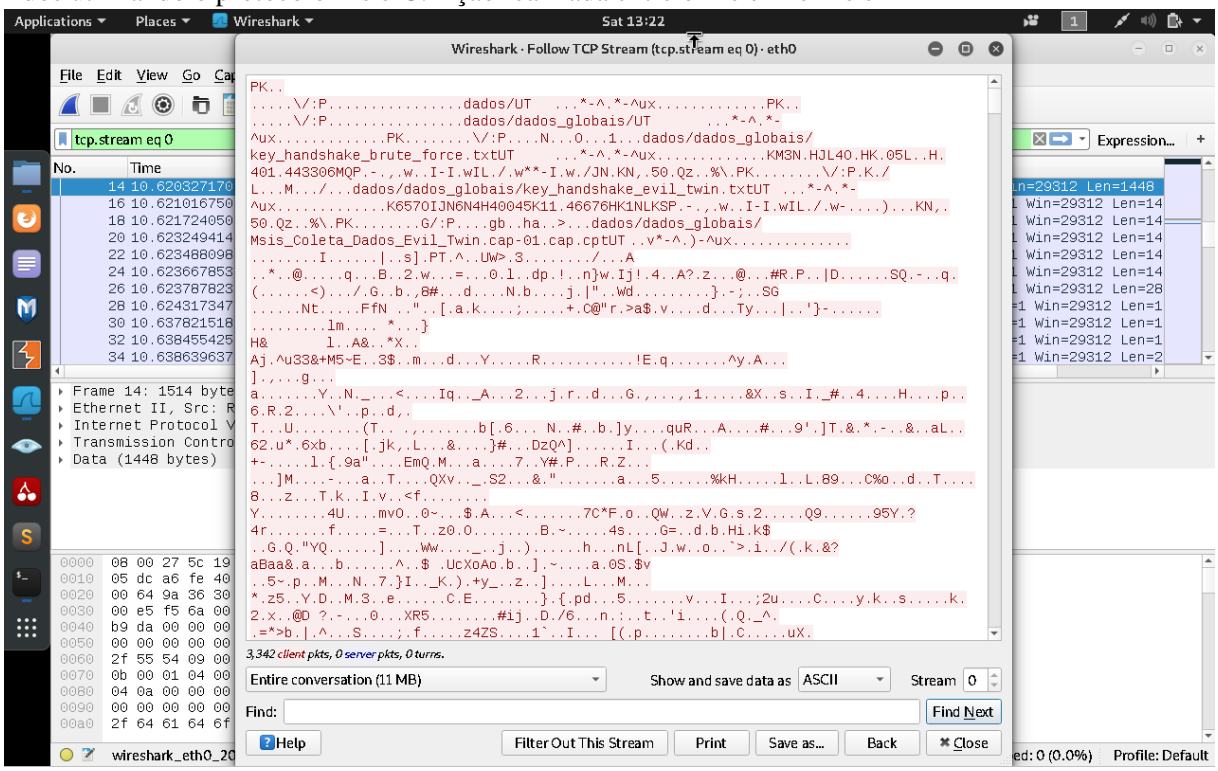
Posterior a coleta de todos os dados, exibição dos mesmos em tabela e em formato de gráficos é possível observar que o comportamento do módulo Msis-C na relação a compactação dos dados criptografados se mostrou mais eficiente se comparado com nenhuma ação aplicada.

6.3.3 Resultados da validação da criptografia aplicada nos dados

O protocolo Msis-C tem como característica a segurança dos dados, a forma com que o Msis-C foi projetado para realizar esta segurança ocorreu por meio do uso de criptografia dos dados. Na seção anterior, os testes validaram a densidade relacionada ao tamanho dos arquivos criptografados. Nesta seção foi realizado um *sniffer* na rede entre Msis-A e o Msis-P com finalidade de capturar todos os dados que por essa estavam sendo enviados, como mostra a Figura 29.

O resultado do *sniffer* demonstra a confirmação de que todos os dados que pela criptografia foram submetidos se encontraram criptografados e, consequentemente, ilegíveis para a identificação de qualquer tipo de informação. Ação essa realizada pelo Wireshark, sendo executada sobre um sistema operacional considerado de utilidade de profissionais da segurança da informação, Kali Linux, uma distribuição *Open source*, ou seja, de código aberto.

Figura 29 – Exibe a tela do *software* Wireshark, realizando a interceptação de dados que foram transferidos utilizando o protocolo Msis-C. Ação realizada entre o Msis-A e Msis-P



Fonte: Elaborado pelo autor.

6.4 Comparação com estado-da-arte

Comparando o modelo com o estado da arte, vale a ressalva que não foi encontrado nenhuma citação em relação a ataques paralelos à rede sem fio (Wi-Fi). Prática esta que contribuí para diminuir o tempo de ataque. Na literatura, (SHARON et al., 2017; Emmanouil Vasilomanolakis et al., 2018) descrevem técnicas de ataques que são direcionadas a dispositivos de IoT, porém limitando-se a uma única técnica de ataque. Uma das características do Msis, envolve ação de ataque duplo que unifica duas técnicas de ataques diferentes, estes ataques são executados de modo paralelo. Este tipo de estratégia, na literatura, é tratado com outros meios, exemplo: ao invés de direcionar mais técnicas se foca em utilização de uma antena de maior potência. Ou seja, altera-se a característica do ataque mas permanece usando a mesma técnica.

O protocolo Msis-C foi direcionado em aplicar várias camadas de criptografia e a compactação de dados em arquivos mais densos, porém com menor fluxo de transição, isso para garantir a segurança na troca de dados entre um módulo e outro do Msis. Na literatura, (DIZDAREVIĆ et al., 2019), os protocolos de maior utilização em dispositivos de IoT têm características diferentes, uma vez que seu foco não está em segurança, mas sim na sua capacidade de largura de banda, desempenho e energia.

6.5 Considerações parciais

O sistema Msis foi desenvolvido para atuar em um determinado contexto. A unificação dos ataques *Brute Force* e *Evil-Twin* foram escolhidos após algumas observações relacionadas a suas características de funcionamento. É possível adicionar mais técnicas desde que sigam algumas características semelhantes a ambas já escolhidas e, também, que o dispositivo para as ações de ataque possua recursos de processador disponíveis.

O protocolo Msis-C foi projetado para atuar na criptografia dos dados, compactação dos mesmos e garantir a segurança desses, quando realizado a comunicação de um ponto a outro. Não foi foco pensar em desenvolver nenhum modo e ou chave de criptografia. No caso do Msis-C, esse segue o uso do Ccrypt [1].

[1] http://ccrypt.sourceforge.net/

7 CONCLUSÃO

O Msis *(Mobile Security Intrusion System)* é um sistema projetado para auxiliar autoridades em operações especiais, tais como: em investigação policial, sequestros, captura de informação ou casos em que seja necessária a invasão e coleta de informação sobre alguma outra situação. O Msis é projetado para realizar ações de ataques em redes sem fio (Wi-Fi) e capturar a *hash* da senha de determinado roteador. Depois que a captura é realizada, os dados são transferidos com segurança de um módulo a outro, e assim na sequencia seja realizada a técnica de ataque de dicionário. O Msis é um sistema arquitetado para o funcionamento em dispositivos de IoT, ou seja, dispositivos de recursos limitados. Neste protótipo, o Msis foi embarcado sobre um VANT (Veículo aéreo não tripulado) para assim facilitar a chegada em locais restritos.

Análises teóricas foram feitas considerando duas situações, primeira, modo de executar dois ataques de forma paralela, tendo como objetivo para essa abordagem ganhar tempo nesta ação e buscar ser o mais efetivo possível. Situação que se descreve pelo fato de o Msis ser usado em um dispositivo de IoT com recursos de energia e tempo para ação reduzida. A segunda técnica atua na transferência de arquivos do módulo Msis-A para o Msis-P, de modo em que os dados sejam criptografados e caso haja qualquer ação de ataque contra o Msis, os dados que estão em transferência não sejam de fácil interpretação.

Os resultados mostraram que a técnica de executar dois ataques, de forma paralela, é efetiva em relação ao tempo de combate e, também, a captura da *hash*. Assim, todo o ciclo que envolve um ataque foi possível de ser concluído com sucesso, usando um VANT com características usadas pelo protótipo. Da mesma maneira, ficou claro que para o Msis a aplicação do protocolo Msis-C atende a necessidade do Msis e, assim, garante uma comunicação efetiva e, também, segura entre os módulos.

7.1 Contribuições

O modelo Msis teve como objetivo atuar nas lacunas identificadas pelo estado da arte com base da avaliação dos trabalhos relacionados. Abaixo seguem os apontamentos detalhados.

1. Ataques a redes sem fio (Wi-Fi) usando duas técnicas para execução de forma paralela: a primeira contribuição foca na utilização de duas técnicas de ataques paralelo a determinada rede sem fio (Wi-Fi). Este é um modelo que atua tendo como base de utilização dispositivos de IoT para a execução destes ataques. Ambas técnicas foram arquitetadas para serem executadas utilizando *Threads* em dispositivos limitados como IoT.

2. Protocolo de comunicação com criptografia entre os módulos: a segunda contribuição foca na atuação de um protocolo específico para realizar a comunicação entre os módulos do Msis (Msis-A e Msis-P) e aplicar várias camadas de criptografia para que os dados transmitidos não sejam identificados durante a transição dos mesmos.

Conforme apresentado no capítulo 3, em que se encontram os trabalhos relacionados, se observam maneiras de desenvolver tipos de ataques às redes sem fio ou a dispositivos de IoT (ISCTE-IUL et al., 2018), (SETHURAMAN; DHAMODARAN; VIJAYAKUMAR, 2019) e (SHWARTZ et al., 2018). O Msis implementa mais de uma técnica de ataque e demonstra que estas técnicas podem ser executadas, de forma paralela, para que isso seja possível esta ação utiliza *Threads* para efetivar esta proposta.

Quando avaliado, trabalhos que tratam sobre protocolos, muitas abordagens sobre desempenhos, consumo de banda e energia são descritos e com vários trabalhos atuando sobre estes pontos. Reflexo deste é que a lacuna em segurança acaba sendo mencionada em vários trabalhos (DIZDAREVIĆ et al., 2019). O Msis atua na camada de aplicação, priorizando a criptografia dos dados que são enviados por esse. Sua característica é de trabalhar com arquivos. No ato de gerar a criptografia, o Msis realiza uma divisão de camadas para que possam ser unificados mais arquivos, compactados e, assim, criptografados em três camadas. Contudo, esta é uma forma de facilitar a transição dos dados, diminuir o tamanho dos arquivos mais densos e garantir maior segurança.

Além das contribuições para o estado da arte, o Msis também apresenta contribuições para a sociedade. Com o Msis, as autoridades de investigação podem se beneficiar deste para buscar a efetividade de ações estratégicas em cenários identificados como críticos e que necessitam de certas agilidades, como exemplo: ações em que é preciso realizar um ataque a uma determinada rede sem fio (Wi-Fi), de uma maneira discreta e rápida. O modelo Msis foi projetado para ser preciso, ágil e também garantir que todos os dados de comunicação entre o VANT e a *cloud* sejam feitos com segurança.

7.2 Limitações

Nesta seção serão descritas as limitações encontradas durante o desenvolvimento do protótipo.

- O protótipo utilizou um dispositivo VANT para realizar as ações de voo sobre determinado local. Este VANT é considerado um equipamento de qualidade baixa em relação à autonomia de voo. Como reflexo, o protótipo teve que ser adequado a esta capacidade.

- O servidor que foi usado para realizar a quebra da *hash* também é um servidor limitado quanto ao requisito de alto nível de processamento, dessa forma, todas as bibliotecas utilizadas para validar as *hash* foram desenvolvidas de forma com menos recursos de tentativas. Este detalhe não afetou diretamente o desempenho e nem a validação dos dados e testes realizados.

- A rede de comunicação que foi usada é a rede 4G, rede que era disponível até o determinado momento no local em que os testes foram realizados. Pode-se afirmar que mesmo com esta tecnologia, a taxa de transferência dos dados não teve sérias complicações.

7.3 Trabalhos futuros

Para trabalhos futuros se têm vários contextos que podem ser explorados com finalidade de melhorar e otimizar o Msis. A forma de trabalhar com paralelismo, no Msis foram abordadas as duas técnicas, que abrem possibilidades para novas pesquisas, cujo foco pode ser de implantar novas técnicas ou adicionar o número de técnicas desejadas.

A possibilidade de implantar o Msis como sistema direto em um VANT, sem o uso de qualquer outro dispositivo computacional. Exemplo: *Raspberry Pi* usado no Msis. Também abre lacuna para estudos futuros. Assim se concentra em um único dispositivo em todo o sistema. Como oportunidade, o consumo de energia também pode ser explorado em novas pesquisas. A utilização de outras técnicas de criptografia pode ser adicionada ao protocolo Msis-C, com o objetivo de otimizar suas camadas de criptografia ou até mesmo modificá-las para otimizar o seu desempenho.

REFERÊNCIAS

Al-Fuqaha, A. et al. Internet of things: a survey on enabling technologies, protocols, and applications. **IEEE Communications Surveys Tutorials**, [S.l.], v. 17, n. 4, p. 2347–2376, Fourthquarter 2015.

AL-JOBOURY, I. M.; AL-HEMIARY, E. H. Performance Analysis of Internet of Things Protocols Based Fog / Cloud over High Traffic. , [S.l.], v. 10, p. 176–181, 2018.

ALI, A. et al. Technologies and challenges in developing machine-to-machine applications: a survey. **Journal of Network and Computer Applications**, [S.l.], v. 83, p. 124–139, 2017.

Alladi, T. et al. Consumer iot: security vulnerability case studies and solutions. **IEEE Consumer Electronics Magazine**, [S.l.], v. 9, n. 2, p. 17–25, March 2020.

ALTAWY, R.; YOUSSEF, A. M. Security, Privacy, and Safety Aspects of Civilian Drones. **ACM Transactions on Cyber-Physical Systems**, [S.l.], v. 1, n. 2, p. 1–25, 2016.

AMIN, R. et al. An enhanced anonymity resilience security protocol for vehicular ad-hoc network with scyther simulation. **Computers & Electrical Engineering**, [S.l.], v. 82, p. 106554, 2020.

Basinya, E. A.; Yushmanov, A. A. Development of a comprehensive security system. In: DYNAMICS OF SYSTEMS, MECHANISMS AND MACHINES (DYNAMICS), 2019., 2019. **Anais...** [S.l.: s.n.], 2019. p. 1–7.

BASTOSN, A.; ALMEIDAE, I. a Análise Do Emprego Do Veículo Aéreo Não Tripulado (Vant) Nas Ações E Operações Pm a Análise Do Emprego Do Veículo Aéreo Não Tripulado (Vant) Nas Ações E Operações Pm. **Policing: An International Journal of Police Strategies & Management**, [S.l.], 2009.

Bošnjak, L.; Sreš, J.; Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. In: INTERNATIONAL CONVENTION ON INFORMATION AND COMMUNICATION TECHNOLOGY, ELECTRONICS AND MICROELECTRONICS (MIPRO), 2018., 2018. **Anais...** [S.l.: s.n.], 2018. p. 1161–1166.

D'AMBROSIA, J. **Ieee802**. 2019.

De Jimenez, R. E. L. Pentesting on web applications using ethical - Hacking. **2016 IEEE 36th Central American and Panama Convention, CONCAPAN 2016**, [S.l.], n. 503, p. 1–6, 2017.

DIZDAREVIĆ, J. et al. 00017_A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. **ACM Computing Surveys**, [S.l.], v. 51, n. 6, p. 1–30, 2019.

DORMEHL, L. **The history of drones in 10 milestones**. 2018.

Dorri, A.; Kanhere, S. S.; Jurdak, R. Towards an optimized blockchain for iot. In: IEEE/ACM SECOND INTERNATIONAL CONFERENCE ON INTERNET-OF-THINGS DESIGN AND IMPLEMENTATION (IOTDI), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 173–178.

Emmanouil Vasilomanolakis et al. Don't Steal my Drone: catching attackers with an unmanned aerial vehicle honeypot. In: 2017 , 2018. **Anais...** IEEE, 2018. p. 2.

GILLELA, M.; PRENOSIL, V.; Venkat Reddy, G. Parallelization of brute-force attack on MD5 hash algorithm on FPGA. In: INTERNATIONAL CONFERENCE ON VLSI DESIGN, VLSID 2019 - HELD CONCURRENTLY WITH 18TH INTERNATIONAL CONFERENCE ON EMBEDDED SYSTEMS, ES 2019, 32., 2019. **Proceedings...** Institute of Electrical and Electronics Engineers Inc., 2019. p. 88–93.

GUBBI, J. et al. Internet of things (iot): a vision, architectural elements, and future directions. **Future generation computer systems**, [S.l.], v. 29, n. 7, p. 1645–1660, 2013.

Hornsby, A.; Bail, E. xmpp: lightweight implementation for low power operating system contiki. In: INTERNATIONAL CONFERENCE ON ULTRA MODERN TELECOMMUNICATIONS WORKSHOPS, 2009., 2009. **Anais...** [S.l.: s.n.], 2009. p. 1–5.

ISCTE-IUL, I. U. D. L. et al. Wi-Fi N etwork T esting U sing an I ntegrated Evil- Twin F ramework. **2018 Fifth International Conference on Internet of Things: Systems, Management and Security**, [S.l.], p. 216–221, 2018.

Joshi, J. et al. Performance enhancement and iot based monitoring for smart home. In: INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING (ICOIN), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 468–473.

Khan, R. et al. Future internet: the internet of things architecture, possible applications and key challenges. In: INTERNATIONAL CONFERENCE ON FRONTIERS OF INFORMATION TECHNOLOGY, 2012., 2012. **Anais...** [S.l.: s.n.], 2012. p. 257–260.

KUMKAR, V. et al. Vulnerabilities of Wireless Security protocols (WEP and WPA2). **International Journal of Advanced Research in Computer Engineering & Technology**, [S.l.], v. 1, n. 2, p. 2278–1323, 2012.

Leo, M. et al. A federated architecture approach for internet of things security. In: EURO MED TELCO CONFERENCE (EMTC), 2014., 2014. **Anais...** [S.l.: s.n.], 2014. p. 1–5.

LINDÉN, E. **A latency comparison of iot protocols in mes**. 2017.

MAHMOUD, R. et al. Internet of things (IoT) security: current status, challenges and prospective measures. **2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015**, [S.l.], p. 336–341, 2016.

MILLER, C. Mobile attacks and defense. **IEEE Security and Privacy**, [S.l.], v. 9, n. 4, p. 68–70, 2011.

MING, X.; CHEN, Y.; GUO, J. Analysis of computer network information security and protection strategy. In: MATEC WEB OF CONFERENCES, 2019. **Anais...** [S.l.: s.n.], 2019. v. 267, p. 02013.

MIORANDI, D. et al. Internet of things: vision, applications and research challenges. **Ad hoc networks**, [S.l.], v. 10, n. 7, p. 1497–1516, 2012.

MOHAMMED, F. et al. Towards Trusted and Efficient UAV-Based Communication. **Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S**, [S.l.], n. 31, p. 388–393, 2016.

MOKHTARI, G.; ANVARI-MOGHADDAM, A.; ZHANG, Q. A new layered architecture for future big data-driven smart homes. **Ieee Access**, [S.l.], v. 7, p. 19002–19012, 2019.

PATIAS, P. Introduction to Unmanned Aircraft Systems. **Photogrammetric Engineering & Remote Sensing**, [S.l.], v. 82, n. 2, p. 89–92, 2016.

PATTON, M. et al. Uninvited connections: a study of vulnerable devices on the internet of things (iot). **Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014**, [S.l.], p. 232–235, 2014.

PI, R. Wireless Security Audit & Penetration Test using. **2018 International Conference on Smart City and Emerging Technology (ICSCET)**, [S.l.], p. 1–4, 2018.

PRIYA, J. J.; SWETHA, B. A Study on Various Devices of Agriculture Drone in IoT. , [S.l.], v. 9, n. 2, 2019.

RESCORLA, E.; MODADUGU, N. Datagram transport layer security version 1.2. , [S.l.], 2012.

SAINT-ANDRE, P. et al. Extensible messaging and presence protocol (xmpp): core. , [S.l.], 2004.

SCHUSTER, D. et al. Global-scale federated access to smart objects using xmpp. In: IEEE INTERNATIONAL CONFERENCE ON INTERNET OF THINGS (ITHINGS), AND IEEE GREEN COMPUTING AND COMMUNICATIONS (GREENCOM) AND IEEE CYBER, PHYSICAL AND SOCIAL COMPUTING (CPSCOM), 2014., 2014. **Anais...** [S.l.: s.n.], 2014. p. 185–192.

SETHURAMAN, S. C.; DHAMODARAN, S.; VIJAYAKUMAR, V. Intrusion detection system for detecting wireless attacks in IEEE 802.11 networks. **IET Networks**, [S.l.], v. 8, n. 4, p. 219–232, jul 2019.

SHARON, V. et al. Stego Pi: an automated security module for text and image steganography using raspberry pi. **Proceedings of 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016**, [S.l.], n. 978, p. 579–583, 2017.

SHWARTZ, O. et al. Reverse Engineering IoT Devices: effective techniques and methods. **IEEE Internet of Things Journal**, [S.l.], v. 5, n. 6, p. 4965–4976, 2018.

STEINMANN, J. A.; BABICEANU, R. F.; SEKER, R. UAS SECURITY : encryption key negotiation for partitioned data background information on uas data security issues proposed uas data security model. , [S.l.], p. 1–7, 2016.

TANTITHARANUKUL, N. et al. Mqtt-topics management system for sharing of open data. In: INTERNATIONAL CONFERENCE ON DIGITAL ARTS, MEDIA AND TECHNOLOGY (ICDAMT), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 62–65.

VILLAGE, M. G. Disponível em: <http://www.alltechuav.com/products$_list/pmcId = 23pageNo_FrontProducts_list01 - 1481851362854 = 2pageSize_FrontProducts_list01 - 1481851362854 = 3.html>.Acessoem : 28dezembro$ 2018.

WANG, G.; LEE, B. S.; AHN, J. Y. Authentication and key management in an LTE-Based unmanned aerial system control and non-payload communication network. **Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016**, [S.l.], p. 355–360, 2016.

WEBER, R. H. Internet of things–need for a new legal environment? **Computer law & security review**, [S.l.], v. 25, n. 6, p. 522–527, 2009.

YASSEIN, M. B.; SHATNAWI, M. Q. et al. Application layer protocols for the internet of things: a survey. In: INTERNATIONAL CONFERENCE ON ENGINEERING & MIS (ICEMIS), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p. 1–4.