Uso de IoT em drones em Sistemas Agrícolas

1st Christian Matheus de Paula Melo
Instituto de Informática (INF)
Universidade Federal de Goiás (UFG)
Goiânia, Brasil
christian.matheus@discente.ufg.br

2° Matheus Felipe Araújo de Moraes
Instituto de Informática (INF)
Universidade Federal de Goiás (UFG)
Goiânia, Brasil
moraes_felipe@discente.ufg.br

3° Jefferson Frota Campos
Instituto de Informática (INF)
Universidade Federal de Goiás (UFG)
Goiânia, Brasil
jeffersonfrota@discente.ufg.br

***Resumo*—O uso de drones em Sistemas agrícolas é cada vez maior, devido a todas funcionalidades e diversificação de tarefas que permite. No entanto, quanto maior a utilização e sofisticação, maior a quantidade de dados gerados pelos drones, uma vez que utilizam de IoT (internet of things) para comunicação, coleta e outras atividades. Por essa razão, um dos principais problemas na utilização dos drones é a segurança e privacidade dos dados. Neste relatório, realizamos uma busca bibliográfica sobre esse problema e possíveis soluções para que os usuários os utilizem sem hesitação.**

Keywords*—*IoT, drones, privacidade, segurança, sistemas agrícolas.

I. Introdução

A utilização de drones, que utilizam IoT, em Sistemas Agrícolas está moldando e trnasformando o modo como produz (1,2). Benefícios como monitoramento ambiental, de pragas, gestão dos recursos são apenas alguns (2). No entanto, quanto maior a utilização, maior é a quantidade de dados geradas por esses dispositivos (2) e com isso, problemas relacionados a segurança e privacidade dos dados são cada vez mais frequentes (3). Pesquisas realizadas demonstram problemas neste tema e ainda buscam as melhores soluções para resolvê-los (3, 4). Neste relatório, realizamos uma busca bibliográfica sobre os problemas de privacidade e segurança de dados, a respeito dos drones que utilizam IoT e possíveis soluções para o assunto.

II. Fundamentos Teóricos

A. Biometria e PUF

O seguinte trabalho criou um esquema chamado MAKA (5) e que foi utilizado para superar falhas de segurança e garantir mais recursos e privacidade em drones. Eles utilizaram biometria e tecnologias de funções físicas não clonáveis (PUF) para fornecer robustez e resistir a vários ataques, incluindo divulgação de chave de sessão, vazamento de tabela de verificação, representação, ESL e ataques internos privilegiados. Por fim, usaram um modelo Real ou Aleatório (RoR) e lógica Burrows-Abadi-Needham (BAN) para testar e comprovar o nível de segurança. Também simularam o esquema MAKA por meio da Verificação Automatizada de Protocolos e Aplicações de Segurança da Internet (AVISPA), demonstrando que o esquema é resiliente contra ataques replay e MITM.

B. Blockchain

Utilizando um novo esquema denomidado AKA, leve e de autenticação baseado em blockchain, o seguinte trabalho (6) desenvolveu um esquema denominado HCALA, que é referente a curva hiperelíptica. O esquema ainda utiliza HECC, operação OR exclusiva (XOR) e uma função hash (SHA-1). Neste trabalho, também verificaram a segurança por meio da AVISPA, além de comprovarem o mecanismo de autenticação utilizando a ferramente "ROM". O esquema HCALA forneceu privacidade e anonimento, não permitindo rastreabilidade de fontes externas, autenticação mútua (drone e usuário) e integridade e confidencialidade. O esquema também é resistente a ataques de repetição, ataques de negação de serviço, ataques MTM, ataques de modificação, ataques físicos de captura de drones, ataques conhecidos de chave de sessão, ataques de dispositivos inteligentes roubados e ataques de personificação. Por fim, o esquema HCALA demonstrou segurança na utilização de drones e um desempenho eficiênte, no quesito de funcionalidades e questões de manutenção (energia e bateria). No entanto, todos os resultados são apenas laboratoriais, sendo assim, necessários testes no mundo real para comprovar todas as qualificações dadas.

Um outro trabalho, também utilizou blockchain para criar um sistema mais seguro para drones (7). O esquema criado foi chamado de ACSUD-IoD. Transações autenticadas são colocadas em blocos, verificadas e adicionadas na blockchain do projeto, então usados para mineração na blockchain, por meio da Tolerância Prática a Falhas Bizantinas (PBFT). O novo esquema demonstrou ser robusto contra muitos ataques a drones. Os testes foram realizados por meio da análise formal de segurança, utilizando o modelo Real ou Aleatório (RoR), e por verificação formal de segurança, com o software de Verificação Automatizada de Protocolos e Aplicações de Segurança da Internet (AVISPA), igual ao projeto que usou Biometria e PUF (1). Após todas os testes, o ACSUD-IoD se mostrou eficiente em termos de sobrecarga de comunicação e sobrecarga e, robustez nas questões de segurança e funcionalidades.

III. Metodologia

Com o intuito de apresentar os problemas de segurança e privacidades enfrentados por drones, em sistemas agrícolas, que utilizam IoT e possíveis soluções, nosso trabalho realizou um pequeno levantamento bibliográfico, durante 1 semana no mês de Janeiro.

A. Base de dados

Optamos por realizar a pesquisa em bases de dados conhecidas, confiáveis e com trabalhos que possuem altos fatores de impactos. As bases selecionadas foram duas: Web of Science e AMC-DL. Os resultados obtidos foram filtrados por relevância

B. Palavras-chave

Na base de dados Web of Science, a combinação usada foi: "IoT" AND "drones" AND "Security protocols". E na base AMC-DL: "drones" AND "IoT" AND "Security protocols".

C. *Seleção dos artigos*

A escolha dos materiais seguiu alguns critérios de seleção. Primeiro, filtramos, por relevância, os artigos retornados pela busca das palavras-chave,. Na sequência, selecionamos os possíveis títulos que eram relacionados ao nosso tema. Posteriormente, a leitura dos resumos permitiu verificarmos se os trabalhos se enquadravam no nosso assunto. Por fim, a leitura integral do material foi realizada para confirmarmos a escolha dos artigos.

IV. Resultados e Conclusões

Após a leitura dos artigos encontrados na literatura pode-se levantar quais as conclusões que os autores tiveram acerca das propostas de solução para os problemas expostos.

O artigo 5, que trouxe a proposta de utilização do sistema MAKA usando biometria e tecnologias PUF, analisou um sistema de segurança já existente que utilizava autenticação entre usuários e drones em redes de Internet de Drones. Ele constatou as diversas vulnerabilidades de segurança que o sistema analisado permitia. No entanto, o sistema MAKA se mostrou robusto e seguro para resistir a ataques utilizando autenticação mútua, sigilo de encaminhamento perfeito e anonimato. Por fim, apresentou custos razoáveis de computação e comunicação, confiabilidade, e comunicação rápida em ambiente de Internet de Drones.

O artigo 6, que projetou o sistema HCALA baseado na curva hepereliptica, também se mostrou muito seguro e pôde fornecer privacidade e anonimato, não rastreabilidade, autenticação mútua, acordo de chave de sessão, integridade e confidencialidade. Além disso, se mostrou eficiente contra vários tipos de ataques, mantendo eficiência energética do drone desempenhando boa performance.

O artigo 7, que propôs novo esquema de controle de acesso em Internet de Drones usando blockchain, se mostrou resiliente em relação a ataques e comparado com Sistemas existentes, também se desempenhou bem em termos de sobrecarga de computação e comunicação, juntamente com recursos de segurança.

Com os resultados mostrados, é possível concluir que os artigos tiveram êxito ao apresentar soluções para o problema da privacidade e segurança nos drones que utilizam IoT, e pelo menos contribuíram para a produção científica na área. Nesse sentido, artigo presente consegue reunir esses resultados para que os leitores possam replica-los posteriormente, e aperfeiçoa-los, enriquecendo assim ainda mais a lliteratura.

Agradecimentos

A pesquisa para o presente trabalho se mostrou bastante rica em informações e agregadora para nossos conhecimentos. Agradecemos a todos os envolvidos no projeto, direta e indiretamente.

Referências

O número entre parênteses, no corpo do texto, representam as citações dos materiais utilizados no presente trabalho.

[1] P. Vikram, A. Nayyar, and L. Raja. "Agriculture drones: A modern breakthrough in precision agriculture." Journal of Statistics and Management Systems 20.4 (2017): 507-518.

[2] https://agrihub.com.br/os-impactos-da-iot-na-agricultura/

[3] O. M. Mbock, G. Okeyo, and J. M. Wafula. "A survey on privacy and security of Internet of Things." Computer Science Review 38 (2020): 100312.

[4] T. Ali, and A. Ş. Tosun. "An experimental framework for investigating security and privacy of IoT devices." Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments: First International Conference, ISDDC 2017, Vancouver, BC, Canada, October 26-28, 2017, Proceedings 1. Springer International Publishing, 2017.

[5] P. Yohan, D. Ryu, D. Kwon, and Y. Park. "Provably secure mutual authentication and key agreement scheme using PUF in internet of drones deployments." Sensors 23, no. 4 (2023): 2034.

[6] B. A. D. Eddine, M. A. Ferrag, B. Farou, and H. Seridi. "HCALA: Hyperelliptic curve-based anonymous lightweight authentication scheme for Internet of Drones." Pervasive and Mobile Computing 92 (2023): 101798.

[7] B. Basudeb, A. K. Das, and A. K. Sutrala. "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment." Computer Communications 166 (2021): 91-109.