Jurnal Sains dan Ilmu Terapan
Volume 6 Nomor 2 Desember 2023
e-ISSN: 2621-766X; p-ISSN: 2986-4380, Hal 73-82
DOI: https://doi.org/10.59061/repit.v3i4.1284
Available online at: https://e-journal.poltek-kampar.ac.id/index.php/JSIT

Analisis Kinerja dan Keamanan Jaringan Sensor Nirkabel untuk Pemantauan Lahan Kelapa Sawit: Rancangan Penelitian

Muhammad Firjatullah Nur Akbar[1*]
[1] Universitas Pahlawan Tuanku Tambusai, Bangkinang, Indonesia
**Penulis Korespondensi: mfirjanurakbar@gmail.com*

Abstract. *Research on sensor networks in oil palm plantations tests small prototypes over short periods and rarely addresses security, while research on agricultural sensor network security is simulated on generic topologies that ignore canopy attenuation, so the two streams have developed separately. This article presents an integrated research design for analyzing wireless sensor network performance and security in oil palm land monitoring. As a research design article, its purpose is to formulate a replicable methodological framework rather than report measurements. The design combines NS-3 simulation across 36 treatment combinations replicated thirty times, yielding 1,080 runs, with twelve months of field testing on two canopy conditions using fifteen LoRa SX1278 nodes per block. Four security configurations are compared against four attack scenarios, with operational definitions specified for five performance and three security indicators. Four hypotheses are formulated, of which the interaction between topology and security configuration is the most consequential because it determines whether recommendations can be stated generally.*

Keywords: *Energy Efficiency; Network Security; Oil Palm Plantation; Research Design; Wireless Sensor Network.*

Abstrak. Penelitian jaringan sensor pada perkebunan kelapa sawit menguji purwarupa berskala kecil dalam durasi singkat dan jarang membahas keamanan, sementara penelitian keamanan jaringan sensor pertanian disimulasikan pada topologi generik tanpa memperhitungkan atenuasi kanopi, sehingga kedua aliran berkembang terpisah. Artikel ini menyajikan rancangan penelitian terpadu untuk menganalisis kinerja dan keamanan jaringan sensor nirkabel pada pemantauan lahan kelapa sawit. Sebagai artikel rancangan penelitian, tujuannya merumuskan kerangka metodologis yang dapat direplikasi, bukan melaporkan hasil pengukuran. Rancangan memadukan simulasi NS-3 pada 36 kombinasi perlakuan dengan tiga puluh ulangan sehingga menghasilkan 1.080 jalannya simulasi, disertai pengujian lapangan dua belas bulan pada dua kondisi kanopi menggunakan lima belas simpul LoRa SX1278 per blok. Empat konfigurasi keamanan dibandingkan terhadap empat skenario serangan, dengan definisi operasional ditetapkan untuk lima indikator kinerja dan tiga indikator keamanan. Empat hipotesis dirumuskan, dan interaksi antara topologi dan konfigurasi keamanan merupakan yang paling penting karena menentukan apakah rekomendasi dapat dinyatakan secara umum.

Kata kunci: Efisiensi Energi; Jaringan Sensor Nirkabel; Keamanan Jaringan; Perkebunan Kelapa Sawit; Rancangan Penelitian.

1. LATAR BELAKANG

Jaringan sensor nirkabel menjadi tulang punggung pemantauan lahan perkebunan kelapa sawit karena mampu mengumpulkan data kelembapan tanah, suhu, dan curah hujan secara berkelanjutan pada areal yang luas. Karakteristik lokasi perkebunan yang umumnya berada di luar jangkauan jaringan listrik dan seluler menuntut simpul sensor beroperasi dengan sumber daya baterai atau pemanenan energi, sehingga efisiensi energi menjadi kendala perancangan yang paling menentukan (Khernane dkk., 2024).

Persoalan menjadi lebih rumit ketika aspek keamanan dipertimbangkan. Data produksi dan kondisi lahan bernilai komersial, sedangkan simpul sensor yang tersebar di areal terbuka mudah diakses secara fisik. Ancaman yang relevan mencakup penyadapan lalu lintas data, penyisipan simpul palsu, pemalsuan pembacaan sensor, hingga serangan penolakan layanan

Naskah Masuk: 09 November 2023; Revisi: 1 Desember 2023; Diterima: 25 Desember 2023; Terbit: 30 Desember 2023

yang menguras baterai simpul. Sharma dkk. (2024) menegaskan bahwa keterbatasan sumber daya simpul membuat mekanisme keamanan konvensional sulit diterapkan secara langsung.

Di sinilah muncul ketegangan yang menjadi inti persoalan penelitian ini. Mekanisme keamanan seperti autentikasi dan enkripsi menambah muatan komunikasi dan beban komputasi, sehingga meningkatkan konsumsi energi dan memperpendek umur jaringan. Sebaliknya, konfigurasi yang mengoptimalkan umur baterai cenderung mengurangi perlindungan. Pertukaran antara kinerja dan keamanan ini belum banyak diukur secara sistematis pada konteks perkebunan kelapa sawit dengan kanopi rapat yang membatasi pemanenan energi surya.

Tinjauan terhadap literatur menunjukkan bahwa penelitian jaringan sensor pada perkebunan kelapa sawit umumnya menguji purwarupa berskala kecil dalam durasi singkat dan jarang membahas keamanan. Sementara itu, penelitian keamanan jaringan sensor pertanian umumnya diuji melalui simulasi pada topologi generik tanpa mempertimbangkan hambatan propagasi sinyal akibat kanopi. Kedua kelompok penelitian tersebut berkembang secara terpisah.

Artikel ini menyajikan rancangan penelitian untuk menganalisis kinerja dan keamanan jaringan sensor nirkabel pada pemantauan lahan kelapa sawit secara terpadu. Sebagai artikel rancangan penelitian, tujuan utamanya adalah merumuskan kerangka metodologis yang dapat direplikasi, bukan melaporkan hasil pengukuran. Tiga pertanyaan penelitian dirumuskan: (1) bagaimana kinerja jaringan pada kondisi kanopi kelapa sawit; (2) seberapa besar biaya energi dan kinerja dari penerapan mekanisme keamanan; dan (3) konfigurasi mana yang memberikan keseimbangan terbaik antara keduanya.

2. KAJIAN TEORITIS

Pemantauan lahan berbasis jaringan sensor merupakan salah satu wujud penerapan *internet of things* pada sektor pertanian. Tzounis dkk. (2017) serta Ayaz dkk. (2019) memetakan cakupan penerapannya mulai dari pemantauan lingkungan tumbuh hingga penelusuran rantai pasok, sedangkan Kour dan Arora (2020) mencatat bahwa keterbatasan daya dan jangkauan komunikasi tetap menjadi hambatan yang berulang. Bagian ini menguraikan empat landasan yang mendasari rancangan penelitian, yaitu karakteristik jaringan sensor nirkabel, teknologi komunikasi LoRa, ancaman serta mekanisme keamanan, dan pertukaran antara kinerja dan keamanan.

Jaringan Sensor Nirkabel dan Kendala Energi

Jaringan sensor nirkabel tersusun atas sejumlah simpul berkemampuan penginderaan, pengolahan terbatas, dan komunikasi nirkabel yang bekerja sama mengirimkan data menuju gerbang penghubung. Akyildiz dkk. (2002) merumuskan karakteristik dasar jaringan ini, yaitu keterbatasan daya, keterbatasan memori, dan kerentanan terhadap kegagalan simpul tunggal. Yick dkk. (2008) melanjutkan telaah tersebut dan menunjukkan bahwa perancangan protokol pada jaringan sensor selalu merupakan penyeimbangan antara keandalan pengiriman dan penghematan daya.

Karena komunikasi menyerap porsi energi terbesar, sejumlah protokol dirancang untuk menekan jumlah dan jarak transmisi. Heinzelman dkk. (2002) memperkenalkan arsitektur protokol berbasis pengelompokan yang merotasi peran kepala klaster untuk meratakan beban energi, sebuah gagasan yang tetap menjadi rujukan pada pengembangan protokol hemat energi berikutnya (Roberts & Ramasamy, 2022; Surenther dkk., 2023). Pada konteks pertanian, Khernane dkk. (2024) menelaah pemanenan energi terbarukan sebagai pelengkap penghematan daya, meskipun efektivitasnya bergantung pada paparan sinar matahari yang pada perkebunan kelapa sawit dibatasi kerapatan kanopi.

Teknologi LoRa dan Propagasi pada Kanopi

LoRa merupakan teknologi modulasi spektrum tersebar yang dirancang untuk komunikasi berjangkauan jauh dengan konsumsi daya rendah. Augustin dkk. (2016) menelaah karakteristik LoRa dan menunjukkan hubungan antara faktor penyebaran, laju data, dan jangkauan komunikasi, yang menjadi dasar penyetelan parameter pada penerapan lapangan. Ruslan dkk. (2021) menerapkan modul LoRa untuk pemantauan tanah pada perkebunan kelapa sawit, sedangkan Sadowski dan Spachos (2020) membandingkannya dengan teknologi nirkabel lain pada simpul berkemampuan pemanenan energi.

Kanopi kelapa sawit yang rapat menimbulkan atenuasi sinyal yang tidak tertangkap oleh model kanal ruang bebas. Akibatnya, hasil pengujian pada lahan terbuka maupun simulasi dengan topologi generik cenderung menghasilkan estimasi jangkauan yang optimistis. Kondisi inilah yang menuntut kalibrasi model kanal menggunakan pengukuran kekuatan sinyal terima pada lokasi sesungguhnya.

Ancaman dan Mekanisme Keamanan

Butun dkk. (2020) memetakan kerentanan, serangan, dan penanggulangan pada sistem berbasis IoT, sedangkan Zhang dkk. (2021) menyusun survei ancaman yang khas pada jaringan sensor nirkabel. Keduanya menempatkan penyadapan, penyisipan simpul palsu, pemalsuan data, dan serangan penolakan layanan sebagai ancaman yang paling lazim. Ferrag dkk. (2020)

menelaah keamanan dan privasi pada pertanian berbasis IoT dan mencatat bahwa nilai komersial data pertanian menjadikan sektor ini sasaran yang menarik.

Dari sisi penanggulangan, Zhu dkk. (2006) merancang mekanisme pengelolaan kunci yang ringan bagi jaringan sensor berskala besar dengan memisahkan kunci berdasarkan pola komunikasi, sehingga muatan tambahan dapat ditekan. Pendekatan berbasis deteksi juga berkembang, mulai dari sistem deteksi penyusupan waktu nyata yang dirancang Raza dkk. (2013) hingga pemanfaatan pembelajaran mesin untuk mengenali serangan penyuntikan (Gaber dkk., 2022) dan serangan penolakan layanan (Quincozes dkk., 2023). Sharma dkk. (2024) menerapkan pendekatan serupa secara khusus pada jaringan sensor pertanian.

Pertukaran antara Kinerja dan Keamanan

Setiap mekanisme keamanan menuntut sumber daya. Enkripsi menambah beban komputasi, autentikasi menambah panjang paket, dan penyegaran kunci menambah lalu lintas kendali. Pada perangkat berdaya besar, tambahan tersebut dapat diabaikan, tetapi pada simpul sensor bertenaga baterai tambahan itu berpengaruh langsung terhadap umur jaringan. Literatur yang tersedia umumnya membahas kinerja dan keamanan secara terpisah, sehingga besaran pertukaran antara keduanya pada kondisi perkebunan kelapa sawit belum terukur. Kesenjangan inilah yang hendak diisi oleh rancangan penelitian yang diusulkan dalam artikel ini.

3. METODE PENELITIAN

Penelitian yang dirancang menggunakan pendekatan kuantitatif eksperimental dengan dua tahap yang saling melengkapi, yaitu simulasi dan pengujian lapangan. Simulasi digunakan untuk menjelajahi ruang konfigurasi yang luas dengan biaya rendah, sedangkan pengujian lapangan digunakan untuk memvalidasi temuan simulasi pada kondisi propagasi sinyal yang sesungguhnya.

Tahap Simulasi

Tahap simulasi menggunakan perangkat lunak NS-3 dengan model kanal yang dikalibrasi menggunakan pengukuran kekuatan sinyal terima di lapangan. Topologi yang diuji meliputi bintang, pohon, dan jala, masing-masing dengan tiga tingkat kerapatan simpul, yaitu 15, 30, dan 60 simpul pada areal sepuluh hektare. Setiap konfigurasi disimulasikan sebanyak tiga puluh kali dengan benih acak berbeda untuk memperoleh selang kepercayaan yang memadai.

Tahap Pengujian Lapangan

Tahap pengujian lapangan dirancang pada blok kebun kelapa sawit dengan umur tanaman berbeda, yaitu tanaman belum menghasilkan dan tanaman menghasilkan dengan

kanopi rapat. Pembedaan ini penting karena kerapatan kanopi memengaruhi baik propagasi sinyal maupun paparan sinar matahari ke panel surya simpul. Setiap blok dipasang lima belas simpul berbasis modul LoRa SX1278 dengan sensor kelembapan tanah, suhu, dan pH, serta satu gerbang penghubung. Pengujian dijadwalkan berlangsung dua belas bulan agar mencakup musim hujan dan kemarau.

Konfigurasi Keamanan dan Skenario Serangan

Empat konfigurasi keamanan dibandingkan, yaitu tanpa mekanisme keamanan sebagai kendali, enkripsi AES-128 saja, enkripsi disertai autentikasi berbasis kode autentikasi pesan, serta konfigurasi lengkap yang menambahkan penyegaran kunci berkala. Skenario serangan yang diujikan meliputi penyadapan pasif, penyisipan simpul palsu, pemalsuan pembacaan, dan serangan penolakan layanan berupa banjir permintaan.

Indikator dan Teknik Analisis Data

Indikator kinerja yang diukur mencakup rasio pengiriman paket, latensi ujung ke ujung, konsumsi energi per simpul per hari, umur jaringan yang didefinisikan sebagai waktu hingga sepuluh persen simpul kehabisan daya, serta luaran efektif jaringan. Indikator keamanan mencakup tingkat deteksi serangan, tingkat kesalahan positif, dan muatan tambahan komunikasi. Analisis dilakukan menggunakan analisis varians dua arah untuk menguji pengaruh topologi dan konfigurasi keamanan, dilanjutkan uji lanjutan Tukey.

4. HASIL DAN PEMBAHASAN

Kerangka Analisis yang Diusulkan

Rancangan pengukuran indikator disajikan pada Tabel 1. Kerangka ini disusun agar setiap indikator memiliki definisi operasional yang tidak bermakna ganda, sehingga hasil penelitian dapat dibandingkan dengan penelitian lain.

Tabel 1. Definisi Operasional Indikator Penelitian

Indikator	Definisi Operasional	Instrumen Pengukuran
Rasio pengiriman paket	Paket diterima gerbang dibagi paket dikirim simpul	Catatan gerbang dan simpul
Latensi ujung ke ujung	Selisih waktu pembacaan sensor hingga tercatat di server	Penanda waktu tersinkronisasi
Konsumsi energi	Rata-rata arus dikali tegangan selama dua puluh empat jam	Modul pengukur daya INA219
Umur jaringan	Waktu hingga sepuluh persen simpul kehabisan daya	Pemantauan tegangan baterai
Tingkat deteksi serangan	Serangan terdeteksi dibagi serangan disuntikkan	Catatan sistem keamanan

Keterangan: seluruh indikator diukur pada keempat konfigurasi keamanan

Definisi umur jaringan pada ambang sepuluh persen simpul mati dipilih karena pada konteks perkebunan, kehilangan sebagian kecil simpul masih menyisakan cakupan pemantauan yang memadai, sedangkan definisi umum berupa waktu hingga simpul pertama mati terlalu ketat dan menghasilkan estimasi yang pesimistis bagi pengelola kebun.

Rancangan Matriks Eksperimen

Matriks kombinasi perlakuan yang akan diuji disajikan pada Tabel 2.

Tabel 2. Matriks Kombinasi Perlakuan Eksperimen

Faktor	Taraf	Jumlah Taraf	Keterangan
Topologi jaringan	Bintang, pohon, jala	3	Diuji pada simulasi dan lapangan
Kerapatan simpul	15, 30, 60 simpul	3	Hanya pada tahap simulasi
Konfigurasi keamanan	Nihil, AES, AES+MAC, lengkap	4	Diuji pada kedua tahap
Kondisi kanopi	Belum menghasilkan, menghasilkan	2	Hanya pada tahap lapangan

Keterangan: MAC = message authentication code; konfigurasi lengkap mencakup penyegaran kunci berkala

Tahap simulasi menghasilkan 36 kombinasi perlakuan dari perkalian tiga topologi, tiga kerapatan, dan empat konfigurasi keamanan, masing-masing diulang tiga puluh kali sehingga menghasilkan 1.080 jalannya simulasi. Tahap lapangan menghasilkan 24 kombinasi dari perkalian tiga topologi, empat konfigurasi keamanan, dan dua kondisi kanopi, dengan pengamatan berkelanjutan selama dua belas bulan.

Hipotesis dan Ekspektasi Teoretis

Berdasarkan telaah literatur, empat hipotesis dirumuskan sebagaimana disajikan pada Tabel 3. Hipotesis ini akan diuji melalui prosedur statistik yang telah dijelaskan.

Tabel 3. Rumusan Hipotesis Penelitian

Kode	Rumusan Hipotesis	Dasar Teoretis	Uji Statistik
H1	Topologi jala menghasilkan rasio pengiriman paket tertinggi	Redundansi jalur	ANOVA dua arah
H2	Kanopi rapat menurunkan rasio pengiriman paket secara signifikan	Atenuasi sinyal	Uji t berpasangan
H3	Konfigurasi keamanan lengkap menaikkan konsumsi energi di bawah sepuluh persen	Muatan autentikasi	ANOVA dua arah
H4	Terdapat interaksi antara topologi dan konfigurasi keamanan	Muatan berbeda per topologi	Uji interaksi

Sumber: Rumusan berdasarkan telaah literatur (2025)

Hipotesis ketiga merujuk pada temuan penelitian terdahulu yang melaporkan bahwa penambahan mekanisme autentikasi pada jaringan sensor pertanian meningkatkan konsumsi energi pada kisaran satu hingga tujuh persen. Penelitian ini akan menguji apakah rentang tersebut tetap berlaku pada kondisi perkebunan kelapa sawit dengan jarak antarsimpul yang lebih besar dan kondisi propagasi yang lebih buruk.

Hipotesis keempat merupakan yang paling penting secara praktis. Apabila terdapat interaksi antara topologi dan konfigurasi keamanan, maka rekomendasi konfigurasi keamanan tidak dapat diberikan secara umum melainkan harus disesuaikan dengan topologi yang dipilih. Pengujian interaksi semacam ini jarang dilakukan pada penelitian jaringan sensor pertanian, sehingga temuan yang ada cenderung disajikan sebagai rekomendasi tunggal yang belum tentu berlaku lintas konfigurasi.

Kontribusi yang Diharapkan dan Keterbatasan Rancangan

Rancangan penelitian ini diharapkan memberikan tiga kontribusi. Pertama, data empiris mengenai kinerja jaringan sensor pada kondisi kanopi kelapa sawit yang selama ini belum tersedia. Kedua, kuantifikasi biaya energi dari mekanisme keamanan pada konteks tersebut, yang dapat menjadi dasar keputusan bagi pengelola kebun. Ketiga, kerangka evaluasi terpadu yang menempatkan kinerja dan keamanan sebagai satu kesatuan analisis, bukan sebagai dua kajian terpisah.

Rancangan ini memiliki keterbatasan yang perlu diakui sejak awal. Pengujian lapangan pada dua blok kebun dalam satu wilayah tidak dapat mewakili keragaman kondisi tanah dan iklim di seluruh sentra kelapa sawit. Durasi dua belas bulan mencakup satu siklus musim, sehingga variasi antartahun akibat anomali iklim tidak tertangkap. Skenario serangan yang diujikan juga terbatas pada empat jenis yang paling lazim, sedangkan serangan yang lebih canggih seperti serangan lubang cacing tidak termasuk dalam cakupan.

Pertimbangan etik dan perizinan juga perlu diperhatikan. Pengujian serangan dilakukan pada jaringan uji yang terisolasi dari sistem produksi kebun, dan seluruh kegiatan memerlukan persetujuan tertulis dari pengelola kebun. Data yang dikumpulkan bersifat teknis dan tidak memuat informasi pribadi, namun data produksi tetap diperlakukan sebagai informasi rahasia perusahaan dan dilaporkan dalam bentuk teragregasi.

5. KESIMPULAN

Artikel ini merumuskan rancangan penelitian terpadu untuk menganalisis kinerja dan keamanan jaringan sensor nirkabel pada pemantauan lahan kelapa sawit. Rancangan menggabungkan tahap simulasi berbasis NS-3 dengan 1.080 jalannya simulasi dan tahap

pengujian lapangan selama dua belas bulan pada dua kondisi kanopi, dengan empat konfigurasi keamanan dan tiga topologi sebagai faktor perlakuan.

Kontribusi utama rancangan ini terletak pada penyatuan dua aliran penelitian yang selama ini berkembang terpisah, yaitu kajian kinerja jaringan sensor perkebunan yang mengabaikan keamanan dan kajian keamanan jaringan sensor pertanian yang diuji pada topologi generik tanpa memperhitungkan hambatan kanopi. Pengujian interaksi antara topologi dan konfigurasi keamanan diharapkan menghasilkan rekomendasi yang kontekstual, bukan rekomendasi tunggal yang belum tentu berlaku pada semua konfigurasi jaringan.

DAFTAR REFERENSI

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A study of LoRa: Long range and low power networks for the internet of things. *Sensors, 16*(9), 1466. https://doi.org/10.3390/s16091466

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., & Aggoune, E.-H. M. (2019). Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk. *IEEE Access, 7*, 129551–129583. https://doi.org/10.1109/ACCESS.2019.2932609

Butun, I., Österberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access, 8*, 32031–32053. https://doi.org/10.1109/ACCESS.2020.2973178

Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. *Physical Communication, 52*, 101685. https://doi.org/10.1016/j.phycom.2022.101685

Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications, 1*(4), 660–670. https://doi.org/10.1109/TWC.2002.804190

Khernane, S., Bouam, S., & Arar, C. (2024). Renewable energy harvesting for wireless sensor networks in precision agriculture. *International Journal of Networked and Distributed Computing, 12*(1), 8–16. https://doi.org/10.1007/s44227-023-00017-6

Kour, V. P., & Arora, S. (2020). Recent developments of the internet of things in agriculture: A survey. *IEEE Access, 8*, 129924–129957. https://doi.org/10.1109/ACCESS.2020.3009298

Quincozes, S. E., Kazienko, J. F., & Quincozes, V. E. (2023). An extended evaluation on machine learning techniques for denial-of-service detection in wireless sensor networks. *Internet of Things, 22*, 100684. https://doi.org/10.1016/j.iot.2023.100684

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the internet of things. *Ad Hoc Networks, 11*(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Roberts, M. K., & Ramasamy, P. (2022). Optimized hybrid routing protocol for energy-aware cluster head selection in wireless sensor networks. *Digital Signal Processing, 130*, 103737. https://doi.org/10.1016/j.dsp.2022.103737

Ruslan, A. A., Salleh, S. M., Wan Mohd Hatta, S. F., & Sajak, A. A. B. (2021). IoT soil monitoring based on LoRa module for oil palm plantation. *International Journal of Advanced Computer Science and Applications, 12*(5), 231–238. https://doi.org/10.14569/IJACSA.2021.0120527

Sadowski, S., & Spachos, P. (2020). Wireless technologies for smart agricultural monitoring using internet of things devices with energy harvesting capabilities. *Computers and Electronics in Agriculture, 172*, 105338. https://doi.org/10.1016/j.compag.2020.105338

Sharma, V., Bhardwaj, A., & Kaushik, K. (2024). Enhancing agricultural wireless sensor network security through integrated machine learning approaches. *Security and Privacy, 7*(5), e437. https://doi.org/10.1002/spy2.437

Surenther, I., Sridhar, K. P., & Roberts, M. K. (2023). Maximizing energy efficiency in wireless sensor networks for data transmission: A deep learning-based grouping model approach. *Alexandria Engineering Journal, 83*, 53–65. https://doi.org/10.1016/j.aej.2023.10.016

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of Things in agriculture, recent advances and future challenges. *Biosystems Engineering, 164*, 31–48. https://doi.org/10.1016/j.biosystemseng.2017.09.007

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002

Zhang, J., Yan, X., & Wang, Y. (2021). Security threats and countermeasures in wireless sensor networks: A survey. *Wireless Personal Communications, 121*, 1–28. https://doi.org/10.1007/s11277-021-08683-x

Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks, 2*(4), 500–528. https://doi.org/10.1145/1218556.1218559