



BRAIN. Broad Research in Artificial Intelligence and Neuroscience

e-ISSN: 2067-3957 | p-ISSN: 2068-0473

Covered in: Web of Science (ESCI); EBSCO; JERIH PLUS (hkdir.no); IndexCopernicus; Google Scholar; SHERPA/RoMEO; ArticleReach Direct; WorldCat; CrossRef; Peeref; Bridge of Knowledge (mostwiedzy.pl); abcdindex.com; Editage; Ingenta Connect Publication; OALib; scite.ai; Scholar9; Scientific and Technical Information Portal; FID Move; ADVANCED SCIENCES INDEX (European Science Evaluation Center, neredataltics.org); ivySCI; exaly.com; Journal Selector Tool (letpub.com); Citefactor.org; fatcat!; ZDB catalogue; Catalogue SUDOC (abes.fr); OpenAlex; Wikidata; The ISSN Portal; Socolar; KVK-Volltitel (kit.edu) 2025, Volume 16, Issue 2, pages: 353-365.

Submitted: March 4th, 2025 | Accepted for publication: May 10th, 2025

Security in Wireless Sensor Networks for Precision Agriculture: Threats, Prevention, and Protection Mechanisms

Marius Susa

Petroleum-Gas University of Ploiești, Systems Engineering, Romania.

marius.susa@upg-ploiesti.ro

<https://orcid.org/0009-0005-1500-0542>

Kristijan Cincar

West University of Timișoara, Faculty of Mathematics and Computer Science, Romania.

Tibiscus University of Timișoara, Romania.

SC Nikola Tesla, Vrsac, Serbia.

kristijan.cincar80@e-uvt.ro

k.cincar@tibiscus.ro

<https://orcid.org/0000-0002-5740-6680>

Andrea Amalia Minda *

Babeș-Bolyai University of Cluj-Napoca, Engineering Faculty, Romania.

andrea.minda@ubbcluj.ro

<https://orcid.org/0000-0001-7219-827X>

Abstract: *This paper explores the security challenges associated with data transmission in precision agriculture, emphasising the vulnerabilities introduced by wireless sensor networks (WSNs). To mitigate these risks, we provide a comprehensive analysis of different types of cyberattacks targeting WSNs, along with detection, prevention, and defense strategies to safeguard agricultural data and ensure the reliability of smart farming systems.*

Keywords: *wireless sensor networks; precision agriculture; data security; attack detection; protection mechanisms.*

How to cite: Susa, M., Cincar, K., & Minda, A. A., (2025). Security in wireless sensor networks for precision agriculture: Threats, prevention, and protection mechanisms. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, 16(2), 353-365. <https://doi.org/10.70594/brain/16.2/25>

* Corresponding author



1. Introduction

Nowadays, wireless sensor networks (WSN) are widely used in agricultural monitoring to improve the quality and productivity of farming. In this application, sensors gather different types of data (e.g., humidity, carbon dioxide level, and temperature) in real-time scenarios (Jackson, 2016). They consist of a large number of sensor nodes deployed across a specific area to monitor various physical phenomena, such as temperature, air or soil humidity, air pressure, and the concentration of specific chemical compounds. The data collected in this way is transmitted wirelessly in real time, at predefined intervals, or on demand to an appropriate base station and then to a data processing centre.

Sensor nodes used in precision agriculture (PA) can range from highly complex (tracking locations, analysing images) to simple (monitoring temperature, pressure, humidity, pH levels, water levels, etc.). These nodes enable precise tracking of key environmental changes, significantly improving agricultural yields through continuous data collection, storage, and processing (Jawhar et al., 2014).

Despite its advantages, WSN implementation in agriculture faces several challenges, including optimal node deployment, measurement intervals, routing protocol selection, energy efficiency, data transmission methods, scalability, fault tolerance, and data security (Ojha, Misra, & Raghuwanshi, 2015).

For a WSN to be considered secure, it must ensure availability, confidentiality, integrity, and authentication of transmitted data. This paper explores security threats in PA data transmission and proposes possible solutions.

2. Security Issues in Precision Agriculture

WSNs used in PA have unique characteristics that make them susceptible to various attacks (Bhushan & Sahoo, 2017). To ensure communication and system reliability, simplified protocols for topology management and security are necessary. However, security remains a critical concern across all application areas. Key security constraints of WSNs in precision agriculture include:

- Limited node resources: Sensor nodes have restricted memory, energy, computational power, bandwidth, and communication range.
- Ad hoc deployment: Nodes are deployed without fixed infrastructure, making them vulnerable to physical attacks.
- Dynamic topology: Frequent topology changes hinder consistent security monitoring.
- Security-performance tradeoff: Robust security protocols may degrade system performance due to increased resource consumption.
- Open communication channels: Wireless transmissions can be intercepted or disrupted by malicious actors.

Another problem is unauthorised access. Many nodes lack strong authentication mechanisms, making them vulnerable to hackers who can manipulate data or use the node to attack the broader network. Additionally, data transmission is often not encrypted, exposing sensitive agricultural information to interception or alteration during communication. Sensor nodes are also prone to energy drain attacks, such as Denial of Service (DoS), which overload nodes with data requests, quickly depleting their batteries. Similarly, firmware vulnerabilities can allow attackers to inject malicious code, compromising the node's functionality or even the entire network.

Network-based attacks are another concern. For example, attackers can create fake nodes (Sybil attacks) or redirect network traffic (sinkhole or wormhole attacks), disrupting data flow and decision-making. Privacy is also at risk, as sensitive farm data, such as geolocation or crop health, can be stolen or misused if not adequately protected. To address these challenges, it is crucial to implement stronger security measures, such as encryption, authentication, and regular firmware updates. Physical

protections, like tamper-proof enclosures and redundant nodes, can also improve resilience. By taking these steps, sensor nodes can operate securely and provide reliable data for precision agriculture.

Table 1. Summary of Trade-offs

Security Mechanism	Energy Efficiency	Cost	Implementation Complexity	Best Use Case in PA WSN
Symmetric Key (AES, RC4)	High	Low	Low to Moderate	Efficient for local encryption but key management is a challenge.
Asymmetric Key (RSA, ECC)	Low	High	High	Secure but energy-intensive. ECC is preferable.
Lightweight Cryptography	Very High	Low	Moderate	Good balance of security and energy use.
Hash-Based Authentication	Moderate	Low	Low to Moderate	Efficient for message integrity.
Digital Signatures (ECDSA)	Low	High	High	Ensures non-repudiation but is costly.
Lightweight Authentication (PUFs)	High	Moderate	Moderate	Energy-efficient and secure but requires hardware modifications.
Secure Routing Protocols	High	Low	Moderate	Useful for preventing eavesdropping and replay attacks.
Blockchain Security	Low	High	High	Very secure but not practical for PA WSN.
Signature-Based IDS	Low	High	High	Good for detecting known attacks but requires updates.
Anomaly-Based IDS (ML-Based)	Low	High	High	Adaptive to new threats but costly in terms of energy.

In Table 1, the comparison of various security mechanisms used in WSNs for PA, with trade-offs in energy efficiency, cost, and implementation complexity, is presented. The balance between energy efficiency, cost, and complexity of implementation will serve as the determinant for the best-suited security approach for reports on precision agriculture WSN.

- Lightweight cryptography is recommended for this purpose due to its efficiency and includes various encryption methodologies like PRESENT and SPECK, or symmetric key cryptography like AES-128.
- For message integrity, hash-based authentication: HMAC and SHA-3.
- Lightweight solutions based on physical unclonable functions (PUFs) can provide low-cost and energy-efficient authentication.
- Secure routing protocols (TinySec, LEACH) can introduce more security layers without excessive computational costs.
- While the anomaly-based intrusion detection systems (IDS) appear promising with ML-driven IDS based on supervised learning, this requires more optimisation for energy-constrained environments.

The choice of security approaches varies depending on the application scenario, network scale, and available computational capability in the agricultural setup. An optimal light-on combination of lightweight cryptography with efficient authentication and secure communication protocols strikes the right balance.

To protect wireless transmissions from various attacks, two fundamental security requirements must be met: Data Security and Network Survivability Security objectives in PA WSNs (Bhushan & Sahoo, 2017):

- Confidentiality: Preventing unauthorised access to critical data (e.g., cryptographic keys).

- Authentication: Ensuring that sensor nodes and base stations verify legitimate communication sources.
- Data Integrity: Preventing data modification or corruption during transmission.
- Security Management: Protecting base stations, as they are crucial control points in the network.

3. Prominent Attacks and Defence Mechanisms in WSN for Precision Agriculture

The following section describes characteristic attacks and detection, prevention, and protection mechanisms in wireless sensor networks (WSN), together with some significant case studies.

3.1. Node Capture Attack (NC)

Node Capture Attack (NC) is a critical threat in precision agriculture (PA), where attackers physically capture sensor nodes to extract sensitive data, such as cryptographic keys or sensor readings. Once compromised, attackers can manipulate data, disrupt communication, or mislead decision-making processes.

Wireless sensor networks (WSNs) are vulnerable to node capture (NC) attacks if nodes are not deployed in a way that enables proper monitoring. When an adversary captures a sensor node, they can exploit it to launch various attacks. By gaining access to the node's secret keys, the attacker can introduce numerous replicas (fake nodes) into the network, each possessing the same ID and secret key as the original node, compromising the integrity and security of the WSN. The NC attack can cause significant damage to the energy efficiency of neighbouring nodes, as well as to the distribution of incorrect information from the compromised node, which can lead to incorrect decision-making.

The protection mechanism, as shown in Figure 1, is based on the principle that in WSN for precision agriculture, the locations of sensor nodes do not change after implementation. Additionally, each sensor node can identify the sources of all messages from its neighbours.

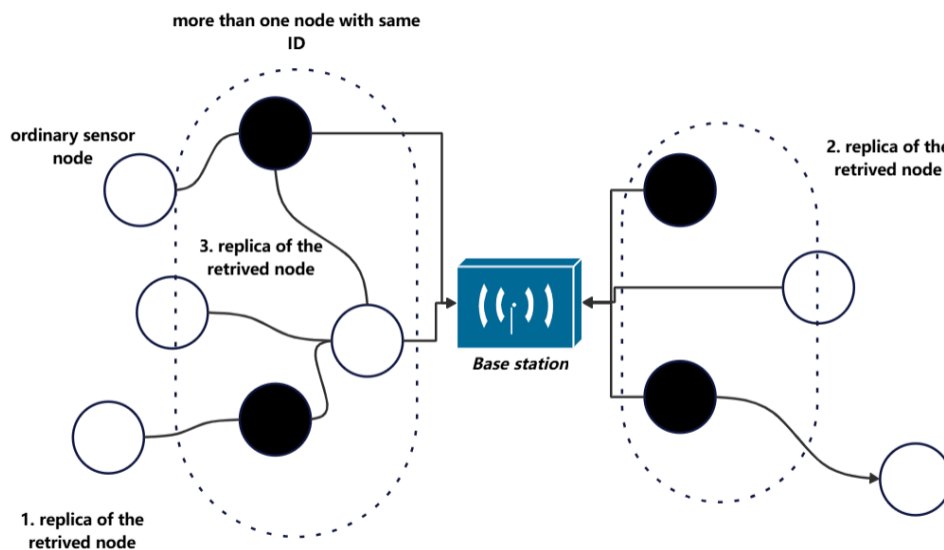


Figure 1. Schematic representation of a Node Capture Attack

The use of WSN in the architecture of precision agriculture in this study is based on the fact that we know the position and density of the deployed sensors. For this type of attack, the attacker must physically capture the sensor. This approach can be based on the number of sensor nodes that can be physically captured in a given region, as the higher the number of captured sensors, the greater the

probability of detecting the attacker. Furthermore, a certain amount of time is required to capture nodes and reintegrate them into the network. In static sensor networks like the one used here, a node is considered compromised if the same ID appears in more than one location.

3.2. Denial of Service (DoS) Attack

The main target of a Denial of Service (DoS) attack is the battery power and resource depletion of a sensor node, which are limited. This attack causes difficulties because replacing the sensor is often not straightforward, but rather complicated or costly, and the same applies to replacing or recharging the battery power. If a WSN (Wireless Sensor Network) succumbs to this attack and we fail to stop it, it automatically means a reduced lifespan of the network.

Nodes are vulnerable despite the fact that authenticity is ensured through the use of hash algorithms and symmetric keys. A malicious node that gains access to symmetric keys may also access information belonging to the base station. If the data concerning the base station is compromised, the entire WSN is compromised. The most critical point for the architecture of the wireless sensor network in a PP (Privacy Protection) is the base station, so all data belonging to it must be maximally protected, i.e., it must not be known to any other node in the network, as this is the only way to be sure that the base station has not been compromised.

In PP, the most common attack is the so-called permanent DoS (PDoS) attack, where an enemy remotely overwhelms the sensor nodes by sending fake packets or retransmitting packets that have already been transmitted through the network. (Raymond & Midkiff, 2008)

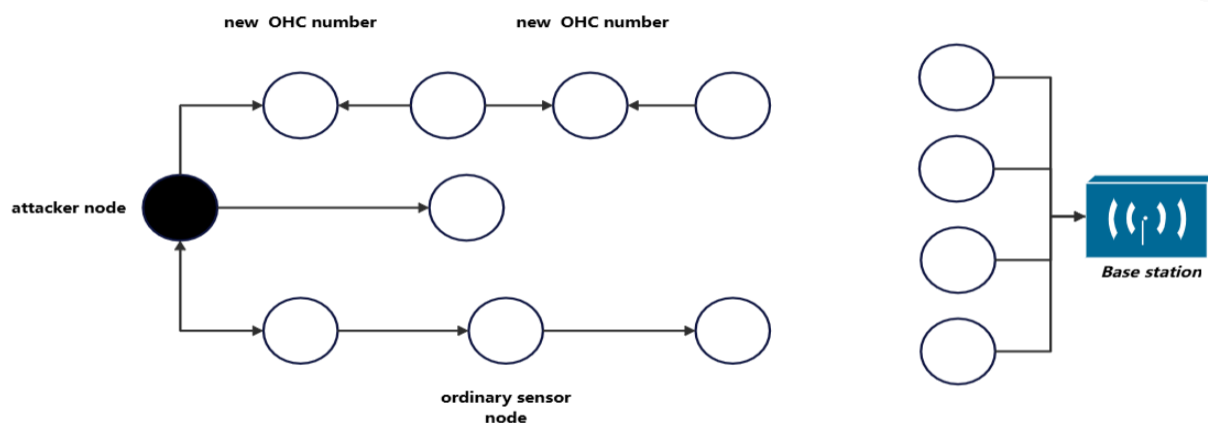


Figure 2. Schematic representation of a Denial of Service (DoS) attack

Figure 2 presents a solution utilising One-way Hash Chains (OHC) to safeguard end-to-end communication against PDoS attacks. Each node is configured with an OHC, enabling intermediate nodes to detect and mitigate PDoS by preventing the propagation of repeated or fake packets. In this approach, each packet contains a unique OHC number, and the intermediate node forwards it only if the number is new. This mechanism effectively prevents adversaries from flooding the communication path with duplicate packets.

Case Study 1: Denial of Service (DoS) Attack on AgroSense Platform (Serbia, 2023)(Biosens, n.d.)

In 2023, a botnet-driven DoS attack targeted AgroSense, a cloud-based precision agriculture platform developed by the BioSense Institute in Serbia, overwhelming the network and rendering it inaccessible for 48 hours.

Impact

1. *Disrupted Services:* Farmers were deprived of vital access to essential data on weather patterns, irrigation schedules, and soil moisture levels.
2. *Yield Reduction:* As the response to rapidly changing environmental conditions was stalled, this led to a concerning 10% drop in overall crop productivity.
3. *Economic Loss:* Many farmers faced significant financial repercussions due to incorrect pesticide applications and ineffective irrigation methods.

Mitigation Measures

- Implemented advanced traffic filtering mechanisms to skillfully distinguish between legitimate traffic and malicious requests.
- Established collaborations with leading cybersecurity firms to deploy robust DDoS protection services.
- Conducted security awareness training for farmers and system operators.

3.3. Hello Flooding Attack

The Hello flooding attack is a threat of flooding messages used for neighbour discovery. The attacker sends or responds to HELLO packets with high transmission power, so a large number of nodes in the network perceive it as a neighbouring node. The attacker transmits packets with such high power that a large number of nodes in the network select it as their parent node. This increases the delay because all messages are routed through the attacker's node. In this way, the part of the network under attack gets the impression that the attacker is the base station, and it can take full control over the nodes and completely isolate that part of the network from the rest of the WSN (Zhang et al., 2013).

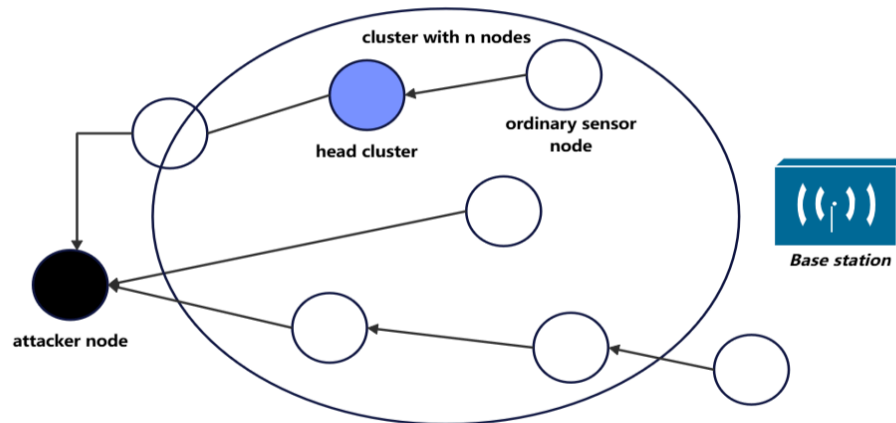


Figure 3. Schematic representation of the Hello flooding attack

One of the best protection mechanisms against this attack, as shown in Figure 3, is based on high energy efficiency – the Low Energy Adaptive Clustering Hierarchy (LEACH). According to data found in the literature (Zhang et al., 2013), this protection mechanism is based on dividing the WSN into clusters. By determining a threshold for the number of nodes belonging to each cluster, a head (head node) is assigned to each cluster, thus triggering the protection mechanism against this type of attack in the WSN in a Privacy Protection (PP) system. The protection algorithm works by detecting the cluster head whose number of members exceeds the threshold set for each cluster, thus detecting if there is an intruder in the network. However, confirmation that a malicious node is present in the network is based on the strength of the received signal and distance.

Case Study 2: Hello Flooding Attack on Smart Farming Networks (Serbia, 2024) (Biosens, n.d.)

In February 2024, a Hello Flooding Attack targeted IoT-enabled precision agriculture networks managed by the BioSense Institute in Serbia, where attackers sent false Hello packets to sensor nodes, causing excessive energy consumption, network congestion, and a breakdown of data transmission.

Impact

1. *Network Congestion:* The excessive burden on nodes within the sensor network resulted in setbacks in transmitting data.
2. *Energy Depletion:* The sensor nodes drained their battery by reacting to Hello packets. Ended up shortening the network's lifespan.
3. *Loss of Data Integrity:* Agricultural systems have been using inaccurate information, which has resulted in decisions about irrigation and fertilisation being made without all the necessary facts.

Mitigation Measures

- Implemented secure authentication protocols to verify legitimate sensor nodes.
- Implemented energy-saving intrusion detection systems (IDSs) to identify and address traffic patterns.
- Enhanced the network firmware by adding security measures to block nodes from accessing the network.
- Implemented time-based packet filtering to reduce the frequency of Hello packet transmissions.

3.4. Jamming Attack

In this type of attack, a jamming device emits radio frequency signals containing useless or unwanted data, interfering with sensor nodes. These signals may mimic network traffic or appear as white noise. Jamming is the intentional act of directing electromagnetic energy toward a communication system to disrupt signal transmission (Shen, Liu, & Zhang, 2015). Attacks on wireless sensor networks that "play" with the radio frequencies of nodes are referred to as jamming (Curiac et al., 2007).

Three types of jamming attacks can be distinguished:

- **Spot Jamming:** The attacker targets a single frequency that the victim uses, expending significant power to overpower the original signal.
- **Sweep Jamming:** The attacker rapidly switches between different frequencies, briefly jamming each one with a full-power signal.
- **Barrage Jamming:** The attacker simultaneously jams multiple frequencies. As the range of jammed frequencies increases, the jamming power on previous frequencies decreases.

Several countermeasures can be used to prevent jamming, such as Frequency Hopping Spread Spectrum (FHSS) (Pickholtz, Schilling, & Milstein, 1982), Direct Sequence Spread Spectrum (DSSS), Ultra-Wide Band Spectrum (UWB), Antenna Polarisation, and Directional Transmission, as described in the paper referenced in the literature (Bhushan & Sahoo, 2017). Some of these methods are computationally demanding, such as DSSS, or not energy-efficient, such as FHSS, as it requires constant frequency changes. Similarly, Antenna Polarisation and Directional Transmission require overly complex antennas for implementation in Privacy Protection (PP) systems.

The protection mechanism that draws our attention is shown in Figure 4, which is the use of the Ultra-Wide Band (UWB) modulation technique. This technique is based on emitting short pulses over a very large frequency range (Nekoogar, 2005). This makes the signal transmission or interception difficult and renders it resistant to effects caused by signal scattering and reflection.

There are studies presenting sensor node arrangements that require minimal energy (Wang et al., 2024). UWB also ensures extended battery life and precise localisation.

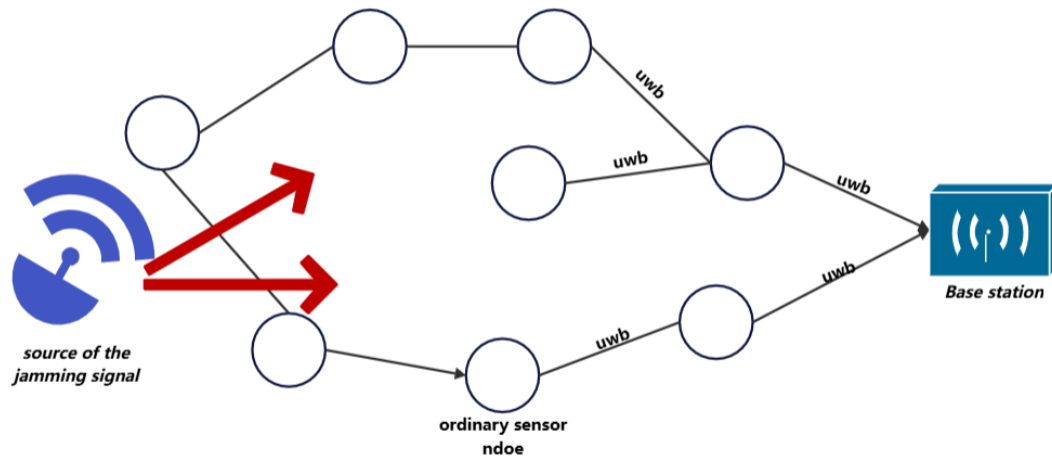


Figure 4. Schematic representation of a jamming attack

Case Study 3: Jamming Attack on Smart Agriculture Networks (Serbia, 2024) (Biosens, n.d.)

In March 2024, a jamming attack targeted IoT-enabled precision agriculture systems monitored by the BioSense Institute in Serbia, where attackers used high-power radio frequency signals to interfere with wireless communications between IoT sensors and control systems, disrupting real-time data transmission.

Impact

1. *Sensor Communication Failure:* There was a breakdown in sensor communication where the WSN devices couldn't send information about soil moisture levels, temperature readings, and the health of crops.
2. *Disrupted Irrigation and Fertilisation:* The malfunction of automated irrigation and fertilisation systems caused disruptions in operations, resulting in the distribution of resources and lower crop yields.
3. *Increased Operational Costs:* Farmers needed to gather data by hand and modify irrigation schedules themselves, which led to labour and operational costs.

Mitigation Measures

- The use of Frequency hopping spread spectrum (FHSS) to reduce the impact of interference caused by jamming.
- The use of anti-jamming detection algorithms to pinpoint and counteract sources of interference.
- Enhanced network resilience was achieved by using antennas and optimising transmission power.
- Implementation of communication channels, as a backup, for wireless networks.

3.5. Message Replay Attack

The message replay attack is a subtype of the denial-of-sleep attack. The application of WSN (Wireless Sensor Networks) in Privacy Protection (PP) are particularly vulnerable to this type of attack, which is based on eavesdropping on network traffic and resending it through the network. If no defence mechanism is employed against this type of attack, the traffic generated by the attacker will be considered regular traffic for this network, and the nodes will attempt to deliver it to its destination.

This generates an excessive amount of traffic in the network that does not contribute to any value and wastes the battery energy of every single node. The attack works on the principle that an adversary can intercept and retransmit the data (Jesudoss & Subramaniam, 2014).

Good results in protecting against this attack were achieved by a protection mechanism applied in a network measuring 100x100 meters with 100 randomly distributed nodes (Jesudoss & Subramaniam, 2014). The implementation of this model in PP can be easily scaled to larger areas, as well as areas of different proportions, without compromising the protection mechanism.

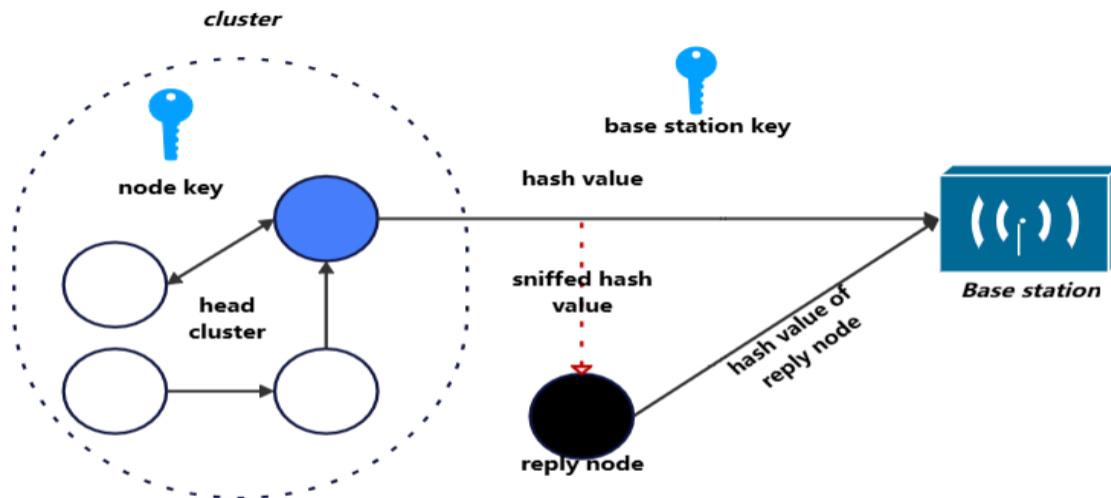


Figure 5. Schematic representation of the message replay attack

It is assumed that clusters are not predefined, the network conditions are heterogeneous, and not all nodes have the same initial energy. Each node has two secret (private) keys. One key is used for communication between nodes, while the other is reserved for communication with the base station. The second key is only utilised when a node assumes the role of a cluster head.

To deter the attacker from accessing the network, authentication must be performed between the cluster head and the nodes that wish to join the network, as shown in Figure 5.

3.6. Selective Forwarding Attack

This attack targets the data transmission layer, where a malicious node selectively drops legitimate packets instead of forwarding them. Selective forwarding can occur in two ways: first, by discarding packets of a specific type, and second, by dropping packets based on their origin or destination, targeting particular nodes (Bhushan & Sahoo, 2017).

The protection mechanism suitable for application in Privacy Protection (PP) is Detection Using Acknowledgments (DUA) due to its relatively low resource overhead for the nodes, as shown in Figure 6, in contrast to other mechanisms that provide equally good results but are demanding in terms of battery power consumption for the nodes.

DUA is a multihop acknowledgement scheme that triggers an alarm based on responses from other nodes. Nodes on the forwarding route can detect a malicious node within the network. Intermediate nodes, upon detecting a malicious node through multihop, send an alarm message to the base station.

DUA consists of three attack detection packets named the acknowledgement packet, the report packet, and the alarm packet. There are two detection procedures:

i) *downstream*, which indicates data transmission from the source node to the base station;

ii) *upstream*, which indicates data transmission from the base station to the source node (Yu & Xiao, 2006).

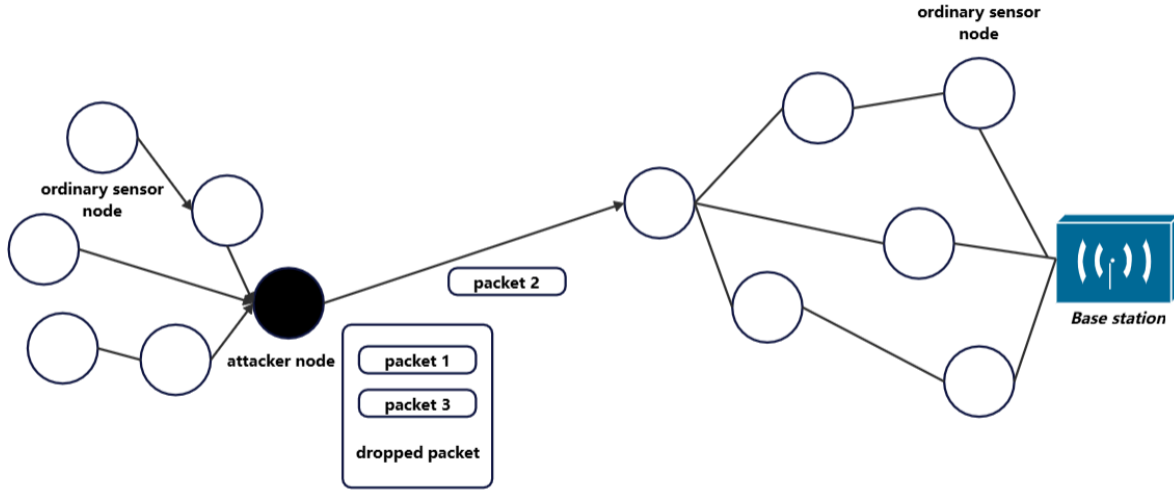


Figure 6. Schematic representation of the selective forwarding attack

A wormhole attack in precision agriculture involves malicious nodes creating a "tunnel" by forwarding packets between them, disrupting the wireless sensor network (WSN) used for monitoring and managing agricultural systems (see Figure 7).

Malicious nodes can mislead data paths, causing false routing, data loss, increased energy consumption, and privacy breaches by intercepting or altering critical agricultural data. Protection measures include secure routing protocols with encryption, time synchronisation to detect anomalies, and location-based security to prevent virtual tunnel attacks.

This attack can hinder effective resource management and compromise the operational efficiency of precision agriculture operations.

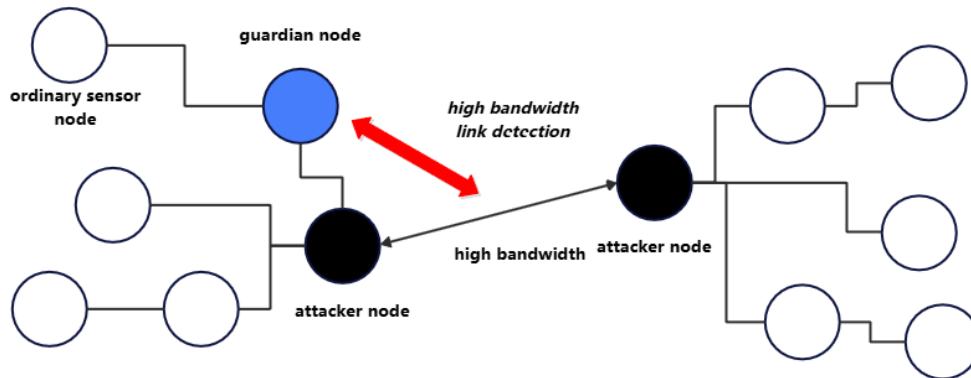


Figure 7. Schematic representation of a wormhole attack

3.7. Spoofing Attack

This attack is based on compromising the authenticity of the source node. It cannot be carried out if two nodes that communicate are not within each other's range. For them to communicate, the communication must be indirect, using other nodes between them.

Spoofing attacks, which are critical for outdoor applications, are carried out either by the malicious node taking the source node's ID from the packets it forwards in relay data packets, or by the

malicious node sending fake data to the destination node, which contains the previously stolen source node's ID (Gavrić & Simić, 2018).

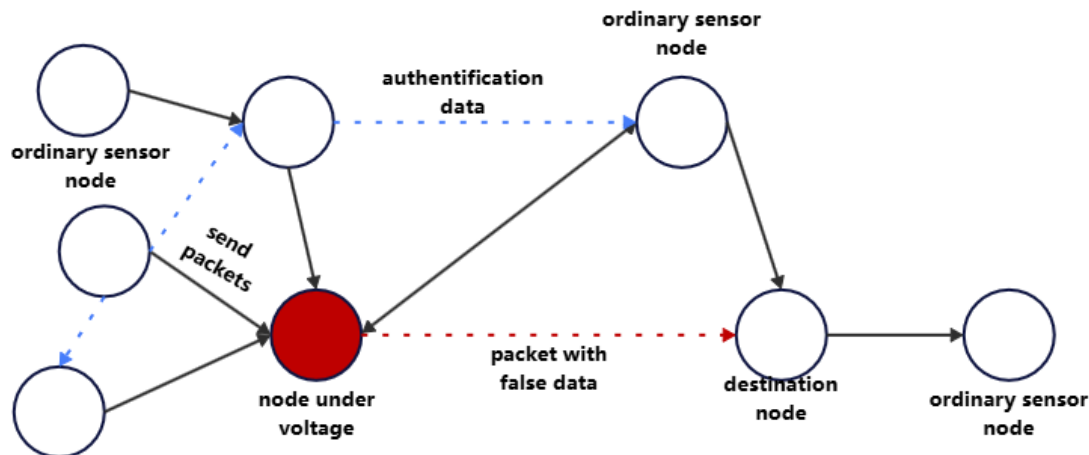


Figure 8. Schematic representation of a spoofing attack

To defend against this attack, all nodes in the WSN must be convinced that the packets are authentic. The method shown in Figure 8 yields good results and satisfies all the criteria on which the system architecture in this work is based. The method relies on multiple routes. A Bloom filter is used for registering the hash values of the IDs of neighbouring nodes at the source node. This method is called the Authentic Identity Bloom Filter (AIBF) and ensures scattered data transmission for packet authentication from the legitimate source node.

Additionally, the proposed method uses Source-initiated Tree-based Routing (SRIDR). SRIDR is based on routing methods that use an ID-based tree, and a routing table is created for each node. This method consists of three procedures: authentic identity transmission, using the authentic identity to detect falsifications, and detecting spoofing attacks.

Case Study 4: GPS Spoofing Attack on Autonomous Tractors (Serbia, 2023) (Biosens, n.d.)

In September 2023, a spoofing attack targeted John Deere 8R autonomous tractors using RTK-GPS for precise navigation in Serbia. Attackers deployed a GPS spoofing device within a 5 km radius, transmitting counterfeit signals that altered positioning data and caused the tractors to deviate from their programmed paths. These signals countermanded RTK-GPS corrections, making the system accept a fake location data as legitimate.

The attacks caused significant operational disruptions and economic losses, including the following:

- a) *Crop damage and resource wastage*: two tractors deviated by 15 metres, damaging crop rows and wasting fertiliser, and automated pesticide spraying drones sprayed incorrect areas, leading to overuse of chemicals.
- b) *Economic losses*: an estimated €30,000 in damages due to crop loss and wasted resources, and additional costs for manual correction and realignment of GPS-guided tractors.
- c) *Supply chain delays*: Continuous disruption of the harvest schedule by machinery misalignment, and disruption to logistics and distribution, blocking export contracts.
- d) *Safety and environmental threats*: Failure to notice pesticides resulted in overapplication, which also posed a further threat to soil contamination, and a real and serious threat to workers and nearby farms.

4. Conclusion

This paper provides an overview of security threats in Wireless Sensor Networks (WSNs) applied to precision agriculture. Particular emphasis is placed on securing data transmission, along with the algorithms and mechanisms that offer protection against common attacks in WSNs. The study concludes that the summarised mechanisms, which are thoroughly explained and visually represented, can comprehensively ensure key security aspects, including confidentiality, authentication, and integrity. Future research should focus on the integration of machine learning techniques for real-time anomaly detection and adaptive security measures tailored to evolving attack patterns. Additionally, the implementation of blockchain-based authentication methods could enhance data integrity and trust within sensor networks.

The case studies highlight the growing threat of cyberattacks in precision agriculture, particularly within WSN infrastructures. While Serbia's BioSense Institute has made strides in digitising agriculture, robust security frameworks are essential to prevent disruptions. Future agricultural systems must integrate AI-driven threat detection, blockchain security, and continuous network monitoring to safeguard precision farming technologies. Another future direction is the evaluation of energy-efficient security protocols, as resource constraints in WSNs remain a critical challenge, and experimental validations in real-world agricultural environments to assess the effectiveness and scalability of the proposed security mechanisms. Finally, the development of hybrid security frameworks that combine cryptographic, AI-driven, and lightweight authentication methods may offer a more robust approach to safeguarding WSNs in precision agriculture.

Acknowledgement

The publication of this article was supported by the 2024 Development Fund of the Babeş-Bolyai University.

References

- Bhushan, B., & Sahoo, G. (2017). Recent advances in attacks, technical challenges, vulnerabilities, and their countermeasures in wireless sensor networks. *Wireless Personal Communications*. <https://doi.org/10.1007/s11277-017-4962-0>
- Biosens. (n.d.). *BioSense Institute*. Retrieved from <https://www.biosens.rs/en>
- Curiac, D.-I., Baniias, O., Dragan, F., Volosencu, C., & Dranga, O. (2007). Malicious node detection in wireless sensor networks using an autoregression technique. In *Proceedings of the 3rd International Conference on Networking and Services (ICNS 2007)*. <https://doi.org/10.1109/ICNS.2007.79>
- Gavrić, Ž., & Simić, D. (2018). Overview of DoS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ingeniería e Investigación*, 38(1), 130–138. <https://doi.org/10.15446/ing.investig.v38n1.65453>
- Jackson, E. (2016). The value of big data in agriculture: Inputs, farming and processing. *International Food and Agribusiness Management Review*, 19(Special Issue), 5–6.
- Jawhar, I., Mohamed, N., Al-Jaroodi, J. & Zhang, S., (2014). A framework for using unmanned aerial vehicles for data collection in linear wireless sensor networks. *Journal of Intelligent & Robotic Systems*, 74(1-2), 437–453. <https://doi.org/10.1007/s10846-013-9965-9>
- Jesudoss, A., & Subramaniam, N. (2014). A survey on authentication attacks and countermeasures in a distributed environment. *Indian Journal of Computer Science and Engineering*, 5(2), 71–77.
- Nekoogar, N. (2005). *Introduction to ultra-wideband communications*. Prentice Hall.
- Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture*, 118, 66–84. <https://doi.org/10.1016/j.compag.2015.08.011>

- Pickholtz, R. L., Schilling, D. L., & Milstein, L. B. (1982). Theory of spread-spectrum communications—a tutorial. *IEEE Transactions on Communications*, 30(5), 855–884. <https://doi.org/10.1109/TCOM.1982.1095533>
- Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1), 74–81. <https://doi.org/10.1109/MPRV.2008.6>
- Shen, Y., Liu, S., & Zhang, Z. (2015). Detection of Hello Flood attack caused by malicious cluster heads on LEACH protocol. *International Journal of Advancements in Computing Technology*, 7(2).
- Wang, Y., Jiang, M., Wang, D., & Ning, G. (2024). Antenna delay calibration in an IR-UWB radar simulated by vector network analyzer. *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–7. <https://doi.org/10.1109/ICECET61485.2024.10698730>
- Yu, B., & Xiao, B. (2006). Detecting selective forwarding attacks in wireless sensor networks. In *Proceedings of the 20th International Parallel and Distributed Processing Symposium* (pp. 1–8). IEEE. <https://doi.org/10.1109/IPDPS.2006.1639675>
- Zhang, M., Li, M., Wang, W., Liu, C., & Gao, H. (2013). Temporal and spatial variability of soil moisture based on WSN. *Mathematical and Computer Modelling*, 58, 826–833.