Towards Operational Intrusion Detection Systems Dedicated to Agriculture: Challenges and Requirements

Laurent Bobelin, Usman Isah

Towards Operational Intrusion Detection Systems Dedicated to Agriculture: Challenges and Requirements

Laurent Bobelin[1][0000−0002−3268−4203] and Usman Isah[1]

INSA Centre Val de Loire, France
88 boulevard Lahitolle, 18000 Bourges, France
firstname.lastname@insa-cvl.fr

Abstract. The recent advances in technologies such as Artificial Intelligence, Internet of Things (IoT), automated drones and embedded systems has involved tremendous changes in many industrial systems architectures. The shift from non-interoperable simple systems to complex systems that involve hundreds of devices, gathered by various networks happened at a fast pace, leading to situations where the operators themselves do not have a clear idea of what their system is, how to secure them and how to recognize faulty behavior, understand the causes of such a behavior and how to correct it.
On the other hand, huge progress have occurred since the rise of Autonomic Computing twenty years ago. Indeed the initial promises of such system - complete autonomy, self healing properties to name a few - have been shown almost impossible to reach on real life large scale systems. However, a significant load of tasks may be offloaded to the operator by using some of those principles. Moreover, AI and machine learning recent advance greatly enhanced the capacity of a system to perceive and forecast its own state.
Intrusion Detection Systems (IDS) is one of services that is a the junction of all those advances. AI may help malicious traffic detection on highly heterogeneous systems involving IoT, embedded systems and more classic LAN. Human operators have to drive automatic actions against malicious patterns, while letting suspicious but honest traffic continue. Designing and implementing an efficient system in this case is an active research topic.
In this paper, we consider the specific case of IDS for networks dedicated to agriculture, from the operational point of view: while many work has focused on new techniques to efficiently implement IDS on those setup, this paper aims at identify constraints and possible solutions to perform an operational deployment of such IDS.

Keywords: IDS · Smart Farming · Operation.

1 Introduction

The last decades the rise of Internet of Things (IoT) involved tremendous changes in most industrial sectors. Nowadays most industrial systems are composed of

sensors and actuators, local gateways and servers coupled together into a common architecture. Local, small-scale networks may be of completely different kinds: ad-hoc vehicle networks, low-energy network of sensors and actuators, traditional computer networks, aggregation of networks composed by those elements, to name a few examples. For example, network dedicated to agriculture may encompass flying drones to detect diseases, human-guided tractors with the help of tracing systems, temperature or various hydrometry sensors, watering actuators, all of them gathering data to feed decision analysis systems (DA) dedicated to farmers. This fully-connected agriculture is often referred as agriculture 4.0 or smart agriculture.

On the infrastructure side, those industrial systems may be embodied by different kind of architecture, cloud, edge or fog-based system may be chosen. For example 5G systems offers network slicing to operate such system, where the network function layer gives the ability to deploy network services in any location of the network from the edge to the core, for a given price. While this architecture gives a lost of elasticity to the network services using Network Function Virtualization (NFV), it implies also to fully trust the infrastructure providers. The recent reluctance of Europe and US to deploy Chinese Huawei 5G equipment says a lot about the dangers of such approach.

Other actual infrastructure solution bypass these problems by employing most traditional Cloud technologies, also relying on NFV and Software Defined Networking (SDN) solutions. From a broad point of view, these architecture offers the same functionalities: aggregating networks, deploying services at various cost in different point of it, and some high level solution to orchestrate services (Management and Orchestration (MANO)) that may be fully automatic (Zero-Touch MANO).

While these infrastructures provides easy ways to aggregate network and orchestrate their services, it is still up to the logical network manager (the tenant) to monitor his network and enforce its security. Intrusion Detection Systems (IDS) is one of the means offered to the tenant to monitor its network, detect possible intrusion into the system and forestall future intrusions by changing low-level firewall rules tables. To do so, the different network entities have to collect some traffic traces, then some learning is done on those traces to help administrator decide whether a traffic is malicious or not. On many systems, collecting traces would be unfeasible: algorithms are employed to perform a fast estimation of how odd a network flow is compared to other normal, legitimate traffic, and only those strange traffic is collected. it is then queued in an alert system, and eventually a human expert estimates if the traffic is legitimate or malicious, how to stop it and how to efficiently mitigate risks of future similar intrusion or how to stop this traffic to be considered as potentially dangerous.

Design such a system in this highly heterogeneous context is actually an active research topic nowadays (see for example [17]). The use of Low Energy equipment adds an additional challenge, as the cost of gathering traffic on these equipment is higher compared to network core. More broadly, agriculture 4.0 is a specific setup where requirements for an IDS differs from traditional platforms.

While most of literature in this domain is focused on describing new solutions, mainly AI-based ones to implement IDS, our target is to identify challenges in this context when IDS is deployed and operating.

The remainder of this paper is organized as follows. First, we give an overview of the context and typical components of a network dedicated to agriculture in section 2, then give an overview of related work in section 3. We then give requirements and induced challenges in section 4 and conclude in section 5.

2 Context

2.1 Devices

Indeed many tools are now available to fully automatize agriculture, ranging from basic sensors to autonomous tractors.

Most common devices in used nowadays are sensors: widely deployed, sensors can monitor many parameters, rain, moisture, humidity, temperature, wind, just to give a few example. Data collected are usually used to forecast mandatory actions that farmers will have to perform in order to maintain production levels highs.

Other quite common fixed devices are more or less complex actuators dedicated to specific operations: automatic sprinklers, antifreeze towers [1], farmbots [2] to name a few.

Flying drones are also used for monitoring, detect anomalies, diseases and various problems on plots.

Finally tractors are a good examples of fully connected devices: usually modern tractors are usually guided by GPS systems, some of them are now fully autonomous and unmanned [13].

All devices are usually linked to a gateway, which may provides some computing resources to form an edge platform with other plots parts of the agricultural exploitation. the size of plots and their numbers may be quite different depending of the type of agricultural exploitation: for example in France vineyards producing protected designation of origin wines may group together tens of small-sized plots, while intensive farming producing cereals will group a few very large plots.

2.2 Architecture

Figure 1 gives an overview on how devices are usually coordinated using a edge/fog architecture. This is the architecture chosen for example by MERI-AVINO project [4].

All on-fields devices are usually communicating either with each other or most of the time with a gateway, that may include computing resources. Some devices may bypass this gateway by communicating using LPWAN protocols and dedicated gateways/antennas (LoRaWAN or SigFox for example) that does not include computing resources. Some may use wired communications (humidity and rain sensors for example) as sensors are deployed close to antennas while other may use Bluetooh or WiFi to exchange with base stations.

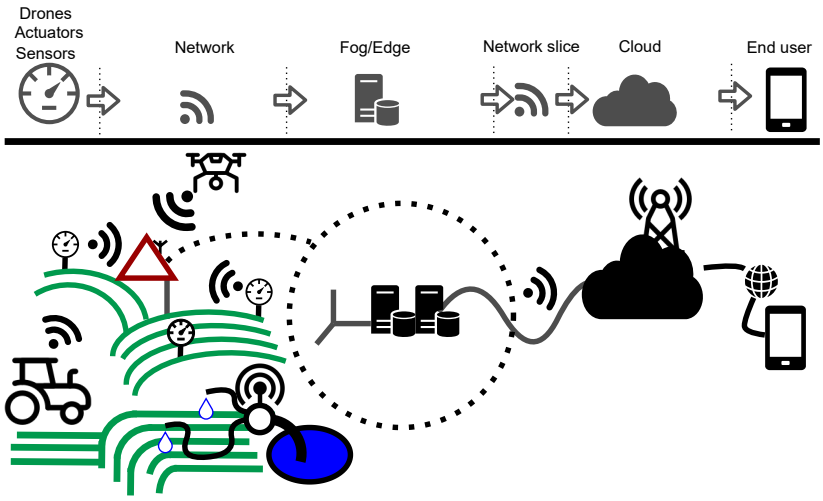

Fig. 1. Architecture of agriculture 4.0 solutions

Gateways communicates with each other by using networks, 5G dedicated networks slices, VLAN or encrypted communications to cloud resources gathering and analyzing data. Finally an interface is given to the end user to monitor this exploitation and decides if actions may be done on plots. Nowadays end user interface usually includes mobile applications and portals. Many vendors follow this architecture, as for example [3] or [6].

Usually those architecture are managed remotely by vendors. It implies that data coming from various exploitation may be gathered by the vendor, and used for various purposes. In our perspective, there is then an opportunity for the vendor to use those data to train DNN so as to efficiently protect the different networks of their platform. However, data sharing between clients or disclosure of clients data must be avoided: the different parameters measured, illness of some plots, are of critical interest for industrial competitors; it is as well a critical information to disclose a cyber attack occurred in the exploitation. Federated learning is a solution that allows to not disclose such sensitive information while taking benefits out of others' experience.

War in Ukraine showed how critical food production is an highly critical in case of conflicts: any part of the production chain, from fields to storage, is a potential target to cyber or physical attacks [5].

One of the main specificities of such platforms mainly rely on the fact that devices are deployed in-field, with little or no qualified persons being able to repair, fixe or mitigate risks when an attack or a failure happen. While this feature is shared with other networks (battlefield tactical networks for example [9]), criticity and deadline in case of problem may be different.

Sensors installation is usually done by vendors, while recalibration and maintenance is done by sending sensors back to the vendors. Actuators and tractors maintenance is usually up to the farmer. Usually farmer have little to no qualifications in computer science ; compromised devices are then unusable/untrustable until a technician can come if network connection is lost. Most of on field deployed devices having low energy consumptions requirements, it is usually not feasible to remotely stop intrusion on a local a system.

3 Related Work

Along with the rise of concerns about security and privacy worldwide, cybersecurity of smart farming has drawn a lot of attention in the last few years. There is actually a lot of prospective work, discussing about opportunities and challenges for that sector, as well as adapting techniques to this context (mostly AI-based, particularly Federated Learning that is fitting well with the requirements of smart farming, as discussed later in this paper).

Usually IDS can be considered in two different ways: by considering the targeted system it watchs, or by considering the techniques it uses. From the targeted systems point of vie, IDS are either Network-based IDS (NIDS, detecting intrusion based on network activities) or Host-based IDS (HIDS, detecting intrusion based on host behavior and/or activities). From the techniques the IDS uses, it may be (1) signature-Based, relying on pre-defined patterns, called signatures, to identify malicious activity, (2) anomaly-based, establishing a baseline of normal activity and flags any significant deviations as potential threats, or (3) hybrid combining both signature-based and anomaly-based detection. Those hybrid IDS It leverages pre-defined signatures for known threats while also monitoring for unusual activity.

Most of the paper are focused on NIDS and on anomaly-based IDS. One can find many different implementations based on the technologies it relies on. FELIDS for example is an FL-based NIDS for Smart Farming, focusing on detection for the most common protocols in this doemain [12]. [15] is similar, focusing on the deployment of CNN on fog resources. Authors may also only focus on the ML/AI methods themselves by exploring the different techniques possible and trying to determine which one suits the most to smart farming, such as the work of [16], or [14].

Many surveys can also be found on the literature on different aspects: some surveys deal with the cybersecurity of smart farming as a whole [11] [8], [18], [19] while other are focused on IDS, or on AI techniques used in IDS for smart farming and datasets to test those techniques [10]. [20] is a survey about FL in agriculture, with a section about IDS. Up to our knowledge, none of them however is focused on the operational aspects of IDS for smart farming.

4 Requirements and Challenges Induced by them

4.1 Remote SIEM

IDS data are gathered into SIEM, so as SOC analyst can investigate when alerts are raised. Remote SIEM and SOC are a de facto standard when its comes to smart farming: most of farmers does not have the ability, the skill and the human resources to maintain and operate their own SIEM and SOC, and thus, smart farming has to rely on remotely operated SIEM and SOC. However, such a remote operation induces some challenges to IDS.

One major obstacle is the issue of limited bandwidth. Many farms, especially those in remote locations, often struggle with limited or unreliable internet connectivity. Uploading the vast amounts of sensor data generated by smart farming systems to a remote SIEM can strain this already limited bandwidth, potentially disrupting critical agricultural operations. Additionally, data latency becomes a concern. Real-time monitoring of agricultural processes is crucial for timely decision-making. Delays in data transmission due to remote SIEM access can lead to slow response times for security incidents, potentially causing significant damage to crops or equipment.

Security concerns also arise when transmitting sensitive agricultural data over the internet. Data such as soil moisture levels or crop yields can be valuable to competitors or malicious actors. Implementing robust security measures, such as encryption, to secure communication channels and ensure data privacy adds complexity to the remote SIEM setup.

Furthermore, the effective utilization of a remote SIEM necessitates efficient data handling practices. Sensor data from smart farming systems is often diverse and unstructured. Pre-processing and filtering this data at the farm level before sending it to the SIEM is essential. This pre-processing reduces bandwidth consumption and allows the SIEM to focus on analyzing relevant security data. However, implementing such data pre-processing procedures requires expertise that may not be readily available on all farms. Sending experts in remote location is then a non-negligible additional cost.

Finally, the expertise required to manage and maintain a complex security solution like a remote SIEM can be a significant hurdle for many farms. Smaller farms in particular may not have dedicated IT staff with the necessary skillset to configure and utilize the system effectively. This lack of expertise can lead to vulnerabilities and a compromised security posture.

Some of those challenges may be mitigated by using some specific techniques. In particular, IDS may rely on Federated Learning to overcome the bandwidth and privacy concerns. The latter two challenges requires the integration of security solution

4.2 Dealing with Brownfield Devices

Securing the complex smart farming ecosystem presents unique challenges, particularly when incorporating brownfield devices into the security architecture.

A primary challenge lies in the inherent heterogeneity of brownfield devices. These devices, often deployed before cybersecurity considerations were paramount, frequently lack standardized communication protocols and security features. This heterogeneity makes it difficult to establish a consistent security posture across the entire smart farming infrastructure. Furthermore, the limited processing power and memory capabilities characteristic of brownfield devices can hinder the installation and operation of resource-intensive IDS agents. The additional processing overhead introduced by IDS software can potentially disrupt the core functionalities of these legacy devices, potentially impacting critical agricultural operations.

Another significant challenge is the issue of limited visibility and control. Brownfield devices often operate with outdated firmware and may not possess the necessary functionalities to integrate seamlessly with modern security solutions like IDS. This limited visibility into device activity and a lack of granular control over these devices make it difficult for IDS to effectively monitor for suspicious behavior and enforce security policies. Additionally, the potential incompatibility between legacy communication protocols and modern IDS solutions can further impede communication and data exchange, hindering the overall effectiveness of the intrusion detection system.

The challenge of vulnerability management is particularly concerning when dealing with brownfield devices. Due to their outdated nature, these devices may have known security vulnerabilities for which patches are no longer available or cannot be applied due to hardware or software limitations. This creates exploitable entry points for malicious actors seeking to disrupt agricultural operations or compromise sensitive data.

Despite these challenges, the complete exclusion of brownfield devices from a smart farming security strategy is often impractical or even impossible due to their continued role in critical agricultural processes. Potential solutions to address these challenges include segmentation strategies that isolate brownfield devices from more secure systems, risk assessments to prioritize critical devices for targeted security upgrades, and the exploration of lightweight IDS solutions specifically designed for resource-constrained environments. Another option is to use Azure Sphere approach [7], by physically deploying a security gateway on the targeted device. This may not be possible for any device, may come with a prohibitive cost, and may also be not resilient to the harsh in field conditions of smart farming.

4.3 Safety Concerns Integration

Smart farming necessitates an expanded scope for IDS functionality, encompassing not only cybersecurity concerns but also safety considerations.

Traditional IDS solutions effectively detect malicious activity aimed at disrupting or compromising agricultural operations, but they often overlook potential safety hazards. However, criticity of some alerts may not depend on IT considerations but on safety. Indeed, smart farming systems integrate a multitude of sensors and actuators that directly interact with the physical envi-

ronment. Malicious actors could exploit vulnerabilities within these systems to trigger actions that could have catastrophic consequences, such as over-irrigating crops, overheating greenhouses, or causing malfunctions in critical agricultural machinery.

The integration of safety level of criticity into IDS functionality may be a solution to mitigate these risks, but it is a challenge. By incorporating safety protocols and parameters alongside traditional cybersecurity measures, IDS can detect anomalous behavior that could lead to physical harm or equipment damage. For example, the system could be programmed to identify sudden spikes in temperature readings from greenhouses, potentially indicating a malfunction in the climate control system, or unusual fluctuations in water pressure that could signal a potential irrigation issue.

However, integrating safety alerts into IDS necessitates careful consideration of several challenges. The first hurdle lies in defining and establishing comprehensive safety protocols specific to the unique operational environment of each farm. These protocols should encompass a wide range of potential safety hazards associated with the specific sensors, actuators, and machinery deployed within the smart farming system. Furthermore, the development of accurate detection algorithms for safety-related anomalies requires collaboration between cybersecurity specialists and agricultural domain experts. These experts can provide in-depth insights into potential safety risks and the operational parameters that can be used to identify anomalous behavior.

Another challenge lies in the potential for an increase in false positives. Expanding the scope of IDS to include safety alerts can lead to an influx of alerts that may not represent actual threats. The development of sophisticated filtering and analysis mechanisms becomes essential to differentiate between genuine safety concerns and non-critical events.

4.4 Failure Alerts Integration

As stated before remotely managed SIEM is a de facto standard for smart farming, one of the causes of that fact being the prohibitive cost in human resource to maintain and manage SIEM and SOC in any farm.

As a matter of fact, this means that mitigation, when it implies to come physically on a device to reconfigure, initialize or recover it, may induce a very high cost, both in terms of time and money. Indeed the travel from the remote SOC to the farm may be long, and the activities of the farm may be stopped during that time, similar to the waste of time experienced by farmers when waiting for a device to be repaired.

Some compromission may even be mitigated by simply replacing the device by a new one. The integration into complex Cyber Physical System may require skills not related to the device itself but CPS experts, that may be able to physically access to the device.

There is then a need of convergence in between the mitigation of cybersecurity alerts and failure. This pledge for a SIEM and physical failure alert convergence.

5 Conclusion

Smart farming, with its intricate network of interconnected devices and sensors, presents unique challenges for cybersecurity. Intrusion Detection Systems (IDS) play a critical role in safeguarding these complex ecosystems, but their effectiveness hinges on addressing operational requirements and overcoming specific hurdles.

We identified key operational requirements for IDS in smart farming, yet unexplored by the literature, despite the numerous papers published so far on this topic. We pledge that those requirements may be the key requirements that future solutions developped must address.

If so, the potential benefits of utilizing IDS in smart farming are undeniable. By acknowledging these hurdles and implementing appropriate solutions, farms can leverage the power of IDS to enhance their security posture. The future of IDS in smart farming lies in continuous innovation. The integration of safety and failure alerts into IDS functionality would offer a significant cost reduction because of the significant delay in between detection of failure and possible mitigation of it. Smart farming should also integrate in its architecture robustness as a key requirement, to avoid loss of production due to the time before mitigation happen, may it be due to cybersecurity or failure.

Acknowledgments. This work has been partially funded by MERIAVINO. MERIAVINO is part of the ERA-NET Cofund ICT-AGRI-FOOD, with funding provided by national sources [ANR, UEFISCDI, GSRI] and co-funding by the European Union's Horizon 2020 research and innovation program, Grant Agreement number 862665

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Anti freeze towers from win-machines.com. https://www.wind-machine.com/
2. Farmbot. https://farm.bot/
3. Ict international. https://www.ictinternational.com/
4. Meriavino. https://ictagrifood.eu/sites/default/files/MERIAVINO\%20Leaflet.pdf
5. Russia is targeting wheat stocks in ukraine, worsening global food crisis, eu says. https://www.euronews.com/my-europe/2022/04/11/russia-is-targeting-wheat-stocks-in-ukraine-worsening-global-food-crisis-eu-says
6. Sencrop. https://sencrop.com/fr/
7. Azure, M.: Zero trust cybersecurity for the internet of things (2021-04-30 04:08:00 2021), https://azure.microsoft.com/mediahandler/files/resourcefiles/zero-trust-cybersecurity-for-the-internet-of-things/Zero%20Trust%20Security%20Whitepaper_4.30_3pm.pdf
8. Basharat, A., Mohamad, M.M.B.: Security challenges and solutions for internet of things based smart agriculture: A review. In: 2022 4th International Conference on Smart Sensors and Application (ICSSA). pp. 102–107 (2022). https://doi.org/10.1109/ICSSA54161.2022.9870979

9. Castanares, A., Tosh, D.K., Kamhoua, C.A.: Slice aware framework for intelligent and reconfigurable battlefield networks. In: MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM). pp. 489–494 (2021). https://doi.org/10.1109/MILCOM52596.2021.9653025
10. Ferrag, M.A., Shu, L., Friha, O., Yang, X.: Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. IEEE/CAA Journal of Automatica Sinica **9**(3), 407–436 (Mar 2022). https://doi.org/10.1109/jas.2021.1004344, http://dx.doi.org/10.1109/JAS.2021.1004344
11. Friha, O., Ferrag, M.A., Maglaras, L., Shu, L.: Digital agriculture security: Aspects, threats, mitigation strategies, and future trends. IEEE Internet of Things Magazine **5**(3), 82–90 (2022). https://doi.org/10.1109/IOTM.001.2100164
12. Friha, O., Ferrag, M.A., Shu, L., Maglaras, L., Choo, K.K.R., Nafaa, M.: Felids: Federated learning-based intrusion detection system for agricultural internet of things. Journal of Parallel and Distributed Computing **165**, 17–31 (2022). https://doi.org/https://doi.org/10.1016/j.jpdc.2022.03.003, https://www.sciencedirect.com/science/article/pii/S0743731522000570
13. Heikkilä, M., Suomalainen, J., Saukko, O., Kippola, T., Lähetkangas, K., Koskela, P., Kalliovaara, J., Hannu, H., Juho, P., Yastrebova, A., Posti, H.: Unmanned agricultural tractors in private mobile networks. Network **2**(1), 1–20 (Dec 2021). https://doi.org/10.3390/network2010001
14. Kethineni, K., Gera, P.: Iot-based privacy-preserving anomaly detection model for smart agriculture. Systems **11**(6) (2023). https://doi.org/10.3390/systems11060304, https://www.mdpi.com/2079-8954/11/6/304
15. Kethineni, K., Pradeepini, G.: Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. Cluster Computing **27**(2), 1719–1732 (Apr 2024). https://doi.org/10.1007/s10586-023-04052-4, https://doi.org/10.1007/s10586-023-04052-4
16. Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M.: Malicious detection model with artificial neural network in iot-based smart farming security. Cluster Computing (Mar 2024). https://doi.org/10.1007/s10586-024-04334-5, https://doi.org/10.1007/s10586-024-04334-5
17. Monir, M.F., Uddin, R., Pan, D.: Implementation of a click based ids on sdn-nfv architecture and performance evaluation. In: 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). pp. 1–6 (2021). https://doi.org/10.1109/BlackSeaCom52164.2021.9527751
18. Rettore de Araujo Zanella, A., da Silva, E., Pessoa Albini, L.C.: Security challenges to smart agriculture: Current state, key issues, and future directions. Array **8**, 100048 (2020). https://doi.org/https://doi.org/10.1016/j.array.2020.100048, https://www.sciencedirect.com/science/article/pii/S2590005620300333
19. Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A.G., Russell, C., Duncan, E.: A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. Applied Sciences **11**(16) (2021). https://doi.org/10.3390/app11167518, https://www.mdpi.com/2076-3417/11/16/7518
20. Žalik, K.R., Žalik, M.: A review of federated learning in agriculture. Sensors **23**(23) (2023). https://doi.org/10.3390/s23239566, https://www.mdpi.com/1424-8220/23/23/9566