SSI

(Computer systems security)

Threat modelling

Exercise sheet 2

João Azevedo & Paulo Araújo

University of Minho, Braga, PT
{a85227,a85729}@alunos.uminho.pt

Abstract. Este documento contém um modelo de ameaças detalhado para um Sistema de Agricultura de Precisão cujo objetivo passa por utilizar tecnologias digitais na automação do cultivo de campos agrícolas tendo por base a recolha e análise de dados de produção em tempo real. Estas tecnologias ajudam na aplicação de operações, de forma precisa, envolvidadas na produção, em larga escala, de campos agrícolas. Ao trabalhar com dados que estão diretamente ligados à reputação e gestão económica de uma empresa que utilize um sistema como este existem um conjunto de requisitos de segurança de informação que devem ser detalhados de modo a identificar ameaças e, se possível, mitigá-las, validando no final a eficácia do modelo desenvolvido.

Keywords: Security · Threat modelling · Precision Agriculture · STRIDE

1 Caso de estudo

Um sistema de agricultura de precisão (1) consiste na utilização de tecnologia e princípios científicos para analisar e gerir o cultivo de campos agrícolas baseados em dados recolhidos periodicamente da variação temporal e espacial de entidades envolvidas na produção agrícola, levando a estar perto de uma gestão em tempo real.

O sistema aplicacional está divido em diversas partes, desde os sensores que recolhem dados (temperatura e humidade, por exemplo) e atuadores que aplicam operações despoletadas pela análise desses mesmos dados (alterar temperatura, por exemplo) até aos diversos passos intermédios de agregação dos mesmos por entidades intermédias, o armazenamento e gestão em *cloud-based back-end*, chegando por fim ao utilizador final, o agricultor, através de uma interface *web* adaptada a diversos dispositivos.

Existem portanto diversos temas chave abordados na concretização de um sistema como este, trazendo muitos possíveis vetores de ataque em todas as entidades conectadas. Quando tratamos de assuntos como geração de grandes quantidades de dados, o tão conhecido *big data*, aliados com técnicas de análise dos mesmos e *machine learning*, que têm por vista introduzir uma melhor gestão das colheitas no que toca a como otimizar as plantações para aumentar a produção, podemos assim abordar este tema numa prespetiva de um atacante que queira diminuir a reputação de uma dada empresa ao introduzir dados maliciosos nos seus sistemas, destruir equipamento, ou até ganhar vantagem sobre o mesmo roubando os dados colecionados ao longo de anos, possivelmente.

Assim, é importante estar preparado para lidar com problemas de integridade dos seus dados, disponibilidade dos sistemas e privacidade nas informações transaccionadas, sendo estes os pilares da segurança da informação.

2 Modelação do sistema

Através do modelo de agricultura de precisão conseguimos verificar que o sistema se baseia em quatro grandes componentes: *Wireless sensor and actuators nodes* (WSN) (2), *Basestation/Gateway*, *Back-end* em *cloud* e uma *Dashboard/GUI* que comunicam entre si passando por várias pilhas protocolares, com vista a disponibilizarem informações fidedignas e atualizadas (em tempo aproximado ao real) ao utilizador final, o agricultor, e aos diversos aparelhos atuadores que executam as novas regras/operações nos campos de cultivo.

Em suma, o sistema aplicacional pode ser representado pelo seguinte diagrama (3) que descreve as diversas entidades envolvidas nas comunicações fim a fim:

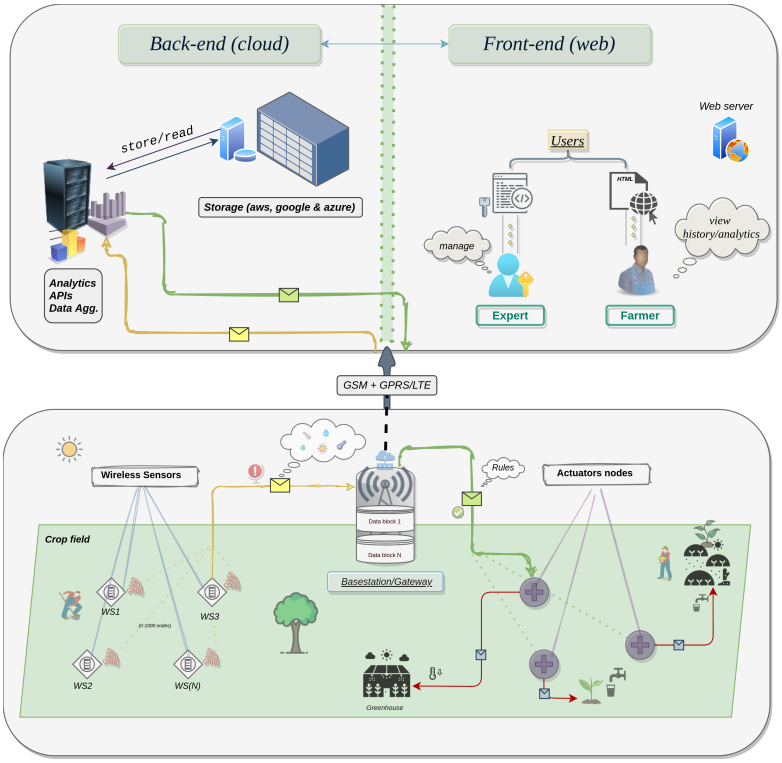

Fig. 1. Diagrama de representação do sistema de agricultura de precisão.

O desenvolvimento do diagrama final pressupõe uma análise detalhada de todos os componentes lá presentes, análise essa que pretende facilitar a construção de um modelo de ameaças mais completo.

2.1 *Wireless sensor and Actuators nodes* (WSN)

Estes dispositivos encontram-se por diversas partes do campo de cultivo e podem ser: sensores e atuadores.

Os primeiros tem por função a recolha de informações sobre o meio que os rodeia, de forma periódica, enunciando diversas características tais como temperatura, humidade e luz, enviando de seguida essas informações para uma única *Basestation/Gateway*.

Já os atuadores são também dispositivos que se encontram espalhados ao longo do terreno e em estufas, tendo como função modificar o estado de operação de diversos dispositivos agrícolas, consoante a informação que vão recebendo vinda dos *Gateways*

Um sistema destes pode ter na sua implementação até um total de 1000 nós. Mais se diz que a comunicação feita entre esses nós e os *Gateways* utiliza

um qualquer protocolo disponível para comunicações *wireless*, fator que será explorado mais à frente.

2.2 Basestation/gateway

Os *Gateways* funcionam como um ponto intermédio entre a informação recebida vinda dos sensores presentes nos campos, agregando posteriormente os dados em armazenamento temporário, e as novas regras aplicadas aos atuadores, vindas da análise e gestão pela camada lógica do sistema, presente no *Back-end*.

Para efetuar as comunicações com os sensores existem diversas interfaces de rádio presentes numa *Basestation*, assim como outras interfaces de rádio celular, como *Global System for Mobile Communications* (GSM) e *General Packet Radio Service/Long-Term Evolution* (GPRS/LTE) para comunicação com a *cloud*.

Assim, esta componente não faz qualquer tipo de precessamento de informação, servindo apenas como nó intermediário e de armazenamento volátil entre o *Back-end* e os sensores/atuadores.

Acrescentando que temporariamente, os dados recolhidos e agregados são enviados sob a forma de sumários para os analisadores no *Cloud-based Back-end*.

De salientar que pode haver um elevado número de *basestation/gateway* que efetuem comunicação com o *back-end*, mas um sensor/atuador comunica apenas com um único *basestation/gateway*. Eis uma representaçãm esquemática destes dois componenetes (4):

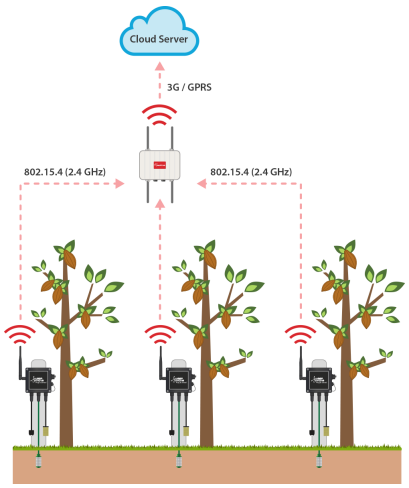

Fig. 2. Representação aproximada dos *Wireless nodes* e do *Gateway*.

2.3 *Cloud-based back-end*

O sistema *back-end* divide-se em duas camadas, uma de armazenamento de dados e outra com a lógica de negócio.

No que toca ao armazenamento em *cloud* de dados, temos que o mesmo é *multi-tenant* (que pode significar diferentes empresas envolvidas) e encontra-se hospedado em serviços como *AWS cloud*, *Google cloud* e *Microsoft Azure*.

No módulo lógico/analítico é onde se encontra todo o "cérebro" do sistema *Precision agriculture* e é nele onde ficam as funções e regras de todo o negócio.

É responsável por receber e agregar resumos de dados dos diferentes *gateways*, e em seguida realizar a análise dos mesmos, gerando, por fim, novas regras/operações para os atuadores nos campos.

É também importante referir que este sistema tem por fim a adaptação a diferentes cenários, isto é, cada empresa pode gerir um campo de cultivo diferente e, para isso, tem APIs fornecidas pelo *Back-end* para gestão e análise de dados e serviços.

2.4 *Dashboard/GUI*

Por fim, existe um módulo para, de forma visual e prática, os utilizadores (*experts* e os agricultores) poderem consultar, em tempo real, o histórico dos dados recolhidos e das decisões tomadas.

Esta secção da aplicação encontra-se destinada ao *front-end* e está desenvolvida em *web*, com vista a ser utilizada por um vasto leque de dispositivos, *smartphones*, *tablets* e computadores.

2.5 Definição de requisitos de segurança

Atualmente os requisitos de segurança são categorizados como requisitos não funcionais, que geralmente são definidos como atributos do software, podendo não ser integrados no software nem testados adequadamente.

Por isso é necessário utilizar modelos que permitam avaliar e encontrar *threats* que podem potenciar a vulnerabilidade do sistema criado, estando este sujeito a ataques de um agente malicioso.

É por isso necessário verificar se o sistema contém todos os pilares da segurança íntegros, para que o invasor seja incapaz de o prejudicar.

Em seguida neste documento iremos enunciar algumas vulnerabilidades, a que este sistema se encontra sujeito, percorrendo assim todos os tipos de falhas de segurança possíveis.

3 Definição das ameaças ao sistema

Na definição das diversas ameaças a um sistema desta natureza a abordagem pode seguir várias vertentes, podendo focar o desenvolvimento nos possivéis atacantes, nos dados envolvidos em diferentes vetores de ataque ou até mesmo

no *software* em si. Neste modelo de ameaças achamos por bem ter uma vista geral por vários destes pontos, pois achamos que só vendo as várias faces do sistema é que conseguimos perceber as várias ameaças.

3.1 *Integridade dos dados*

Numa primeira vertente, é importante perceber qual o "valor" hipotético dos dados recolhidos numa agricultura de precisão, estando portanto o seu conteúdo directamente relacionado com a eficácia individual de uma empresa que pretenda otimizar os seus lucros usando um sistema destes, ou até com a segurança alimentar de futuros clientes que consomem os produtos produzidos por sistemas automáticos baseados, por vezes, na previsão e aprendizagem de máquina, tendo como finalidade o comprometimento da reputação das marcas envolvidas e do setor agrícola.

Portanto, por onde começar na definição de possíveis vulnerabilidades que o sistema pode vir a ter? Comecemos por recordar o diagrama que modela o sistema:

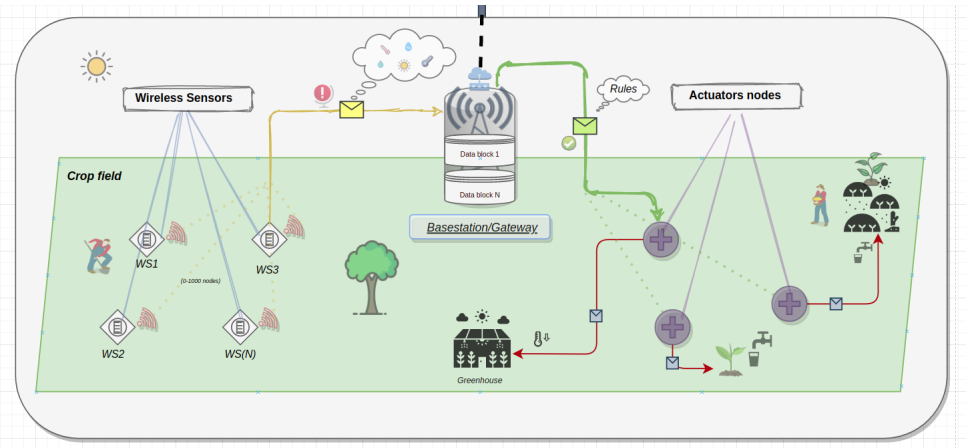

Fig. 3. Secção do diagrama que contém os dispositivos sensores e atuadores.

Os dados começam por ser recolhidos no campo de cultivo através de dispositivos *wireless*, WS1...WS(N), que podem ser *ZigBee sensors* (5), *TelosB motes* (6), *Arduino* ou *Raspberry*.

Na maior parte dos sensores *wireless* e, em particular, por exemplo, nos *ZigBee* e nos *TelosB*, estas são tecnologias vulneráveis a ataques de penetração através da rede devido à sua baixa complexidade, pouca memória e reduzida velocidade de processamento.

Mais se acrescenta que dispositivos como estes, numa situação de elevada congestão da rede, são impedidos de utilizar mecanismos custosos como crip-

tografia de chave pública no envio de dados para os *basestations*, com a finalidade de poderem aumentar a eficiência e eventual poupança de energia, no entanto, tornam-se imensamente vulneráveis a ataques através da rede, como por exemplo: *packet sniffing*.

Se tomarmos, em particular, o caso dos sensores *ZigBee*, sendo isto escalável também para muitos outros dispositivos como *Arduinos* ou *Raspberry*, conseguimos dividir as ameaças à integridade dos dados transacionados através do seguinte diagrama:

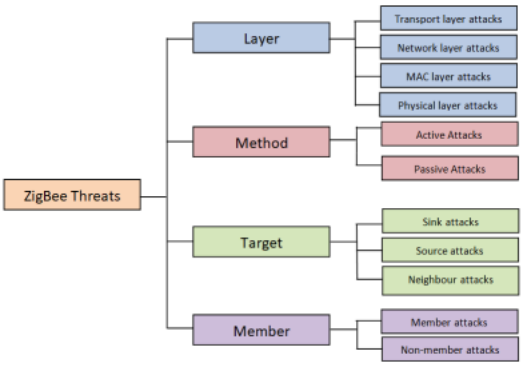

Fig. 4. Ameaças ao sistema de sensores *ZigBee*.

Relativamente à integridade dos dados e com o apoio da base de dados da CWE(7) e outras fontes, temos por exemplo, as seguintes ameaças:

1. *Verificação de integridade nas comunicações*: Quer isto dizer que, se não for garantido um mecanismo de verificação de integridade dos dados transacionados entre os sensores e os *gateways*, como por exemplo um simples *checksum*, não podemos considerar que os dados são íntegros ou válidos. Por isso deve existir um protocolo de comunicação que suporte, pelo menos, esta caraterística fundamental.

2. *Introdução de dados falsificados nas fontes:* Fugindo um pouco das camadas de rede e mesmo do *software* envolvido, podemos ter um tipo de ameaça onde o vetor de ataque está na alteração da flora presente nos campos de cultivo com a inserção de modificações genéticas (intencionais ou naturais) que provocam uma alteração massiva na interpretação e na tomada de decisões pelo sistema que pode levar imenso tempo a resolver e que tem consequências económicas e de segurança alimentar elevadíssimas.

É importante referir que estas verificações devem ser feitas não só na fase de recolha de dados, como também no envio das novas regras aos atuadores, visto

que não queremos correr o risco de, por exemplo, fornecer mais água a uma planta danificando o seu crescimento.

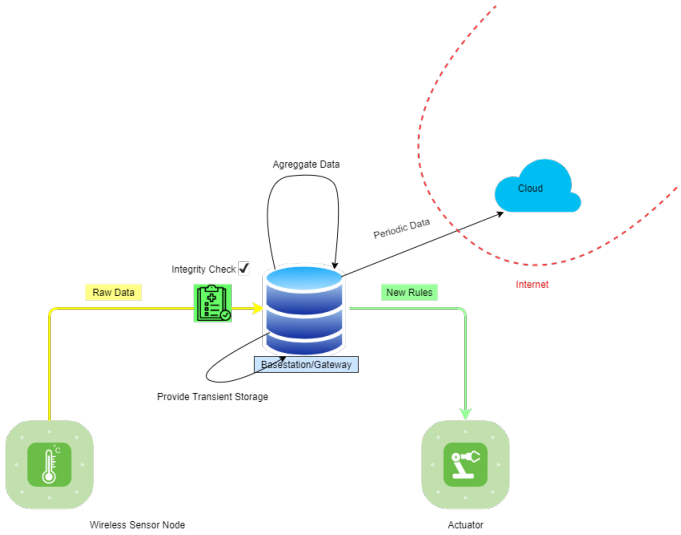

Fig. 5. Representação da verificação de integridade.

3.2 *Autenticação*

Numa atividade em que existe uma grande competitividade entre os diversos agricultores é necessário proteger os dados de acessos concorrentes indesejados.

Uma perda ou o uso indevido destes dados pode ter um grande impacto financeiro e emocional sobre os agricultores. É necessário então com relativa urgência verificar possíveis falhas no sistema e criar medidas que evitem estes acessos indesejados.

1. *Troca de dados sem autenticação:* A falta da existência de uma autenticação dos utilizadores que acedem à rede, nomeadamente nos canais rádio de comunicação, permite que uma entidade sem permissões possa ter acesso aos dados. Sem uma autenticação o invasor apenas necessita de perceber a estruturação dos protocolos recebidos/enviados para que em seguida possa inserir os seus de forma maliciosa.

2. *Autenticação sem verificação de destino*: Permite também que um invasor se faça passar por um ator, modificando o tráfego entre as duas entidades. Isto acontece quando um cliente/vítima comunica com um servidor malicioso que se está a fazer passar por um servidor confiável. Se o cliente avançar a autenticação ou ignorar uma falha da mesma, o servidor malicioso pode solicitar

informações de autenticação do usuário. Usando as mesmas em seguida para conseguir acessos a informação de forma indesejada.

3. *Utilizadores mal intencionados:* Existe ainda um problema que não está diretamente relacionado com o *software* e prende-se no facto de um interveniente deste sistema, por exemplo um agricultor com acesso aos dados, utilizar os mesmos de forma não intencionada. Ou seja o utilizador tem permissões de acesso aos dados mas utiliza-os de uma forma não permitida pelos princípios da empresa, por exemplo para ganhos próprios com a venda dos mesmos a terceiros ou apenas com o intuito de prejudicar a empresa.

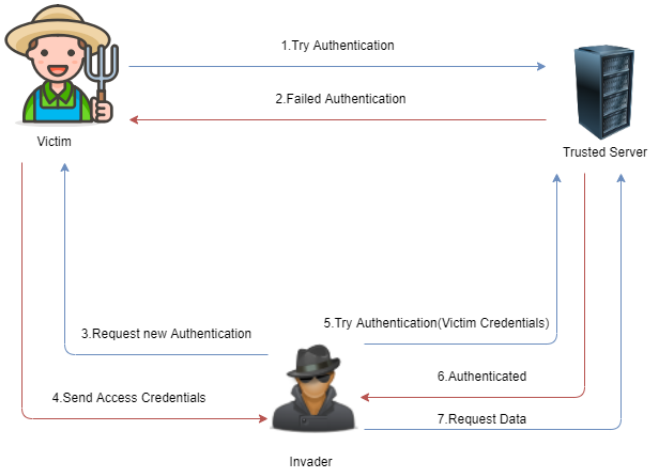

Fig. 6. Servidor não solicita autenticação

3.3 *Disponibilidade*

Como já havia sido referido, a agricultura de precisão pretende implementar várias plataformas comunicantes, em tempo aproximado ao real, de modo a

produzir respostas atempadas a situações adversas ou otimizar a produção dos campos de cultivo.

As plataformas envolvidas, isto é, os sensores, os *gateways*, a *cloud* e mesmo os servidores *web* que disponibilizam as aplicações de consulta de históricos devem ser acessíveis por utilizador fidedígnos quando e onde eles precisarem de usar.

São, portanto, estes os pontos principais que devem ser requeridos na manutenção da disponibilidade deste sistema, restando agora a fase de nomeação de ameaças à prontidade deste *software*:

1. *Falhas na conectividade nas instalações e equipamentos:* A proteção da estabilidade da rede e largura de banda em sistemas como estes, geridos em ambientes rurais (geralmente com cobertura de rede mais reduzida), que são incrementalmente complexos no número de nós, como vimos há pouco, com até 1000 sensores, falhas no *software* que podem levar a *restarts* e perdas de dados, ou sistemas de cultivo que precisam de atuar em certos *timmings* para garantir menor perdas de cultivo e dinheiro.

2. *Negação de serviço nos equipamentos:* Diversos equipamentos como os WSN, atuadores e *Gateways* precisam de atuar em *timmings* específicos podendo resultar num impacto grande nas produções agrícolas. Esta ameaça pode dar-se essencialmente através de um possível atacante que introduza *flooding* de pacotes nos *Gateways* impedindo-os de receber os dados reais devido à congestão/processamento de pacotes maliciosos, ou até, se não houver autenticação, levá-los a introduzir informação contaminada nas bases de dados.

3.4 *Auditing*

O processo de *auditing* de uma maneira geral servirá como uma forma de se poder testar e avaliar a postura geral de segurança de um sistema, sendo neste caso identificado pela postura de um *Gateway*, i.e., que respostas pode ele dar a eventuais anomalias na execução normal do sistema.

Então, será necessário perceber que a informação enviada por um certo sensor se encontra em conformidade com as informações enviadas pelos sensores em seu redor, ou que os dados se encontram dentro de um dado intervalo válido. Isto permite-nos perceber se um sensor se encontra danificado ou numa condição física (no local) não favorável à recolha íntegra de dados ou até se é, por exemplo, um sensor falso.

3.5 *Privacidade e Anonimato*

A agricultura de precisão é um tema adotado por muitos utilizadores que implementam este sistema nas suas instalações, possivelmente em locais estratégicos que não devem ser divulgados nem partilhados com terceiros.

Por outro lado lidamos com o problema destes sensores estarem expostos a ataques físicos de manipulação do seu funcionamento e mesmo a fase de instalação *outdoor* dos mesmos deve ter em conta questões ambientais.

De referir também que a partilha da localização é muito comum neste tipo de sistemas para detetar nós que falham ou saber o estado dos nós em volta dos mesmos. Resumindo, podemos definir dois tipos de ameaças nas informações trocadas:

1. *Hop-by-hop backtracking*: Se os atacantes conseguirem obter a *stream* de dados/pacotes partilhados na rede podem utilizar esta estratégia para detetar a localização original dos dispositivos envolvidos, o que representa um grande problema de segurança e privacidade;

2. *Privacidade dos dados recolhidos:* Perceber que cada empresa que implementa este sistema recolhe dados para o seu caso em específico e que é efetivamente o "dono" desses dados é um ponto fundamental na privacidade e nos direitos de uso dos mesmos, pelo que, todos os componenetes deste sistema podem estar comprometidos mas o *Back-end* deve ser, em especial, blindado a este tipo de ataques.

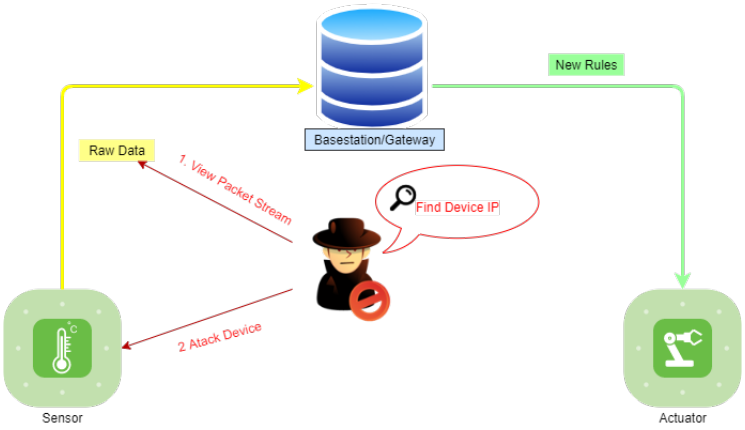

Fig. 7. Atacante vê os dados transacionados.

4 Medidas para combater/mitigar as ameaças

Como vimos ao longo deste documento, existem várias ameaças associadas principalmente com as comunicações nas redes ativas de sensores, atuadores e *gateways*, visto que são as principais origens dos dados e de aplicação de regras que afetam diretamente o sucesso do negócio em si, em termos de produção e consequente influência económica.

As medidas passam por essencialmente seguir padrões de segurança fornecidos por uma série de fontes como a CWE, já referenciada, e *papers* de outros *threat models* associados a aspetos adotados na modulação do sistema.

Destacam-se os seguintes pontos que devem ser tomados em conta:

1. **Integridade dos Dados**: Aqui será crucial que as comunicações feitas entre os sensores/atuadores e os *gateways* priorizem a utilização, não de um "protocolo qualquer" mas sim de um que suporte verificação de integridade, ignorando dados que não cheguem íntegros, visto que mantendo os dados corretos então conseguimos garantir que não envenenamos a base de dados com informação maliciosa e as decisões não são tomadas em vão.

   Por outro lado, periodicamente deve ser feita uma verificação dos dispositivos envolvidos no sistema, de modo a garantir integridade do *hardware* e o local onde se encontra instalado, bem como introduzir *software* de análise de dados que fogem muito do normal, sendo necessária uma análise manual por utilizadores fidedignos para resolver situação a situação, visto que isto tem influências económicas e de segurança alimentar elevadas.

2. **Autenticação**: Neste ponto devemos tomar medidas em relação a duas situações referidas acima. A troca de dados entre dispositivos nos campos de cultivo deve garantir que ambos sabem e validam a origem de cada um, determinando que o protocolo usado deve também garantir autenticação de ambos as entidades envolvidas. Isto previne por exemplo a introdução de *hardware* não autorizado nos campos, sendo uma alternativa a criação de inventário de *hardware* autorizado ao invés do costoso processo de autenticação.

   Falta apenas garantir que os sistemas de autenticação, *tokens*, se fazem de forma correta entre o *back-end* e o *front-end*, visto que os dados devem ser confinados ao utilizador que os gere, isto é, este mantém os direitos de uso confidencial e de gestão dos mesmos.

3. **Disponibilidade**: Neste tópico, e como em todos os sistemas, não nos podemos acreditar simplesmente que os sistemas estarão sempre funcionais e que o estado da rede será sempre favorável. Devemos portanto estabelecer mecanismos de controlo, monitorização, revisão e tolerância a faltas para manter a produção sempre constante (com operações *default*), ainda que nem sempre estejam atualizadas as operações.

A prevenção passa também por evitar *delays*/latências introduzidas por ataques de negação de serviço, onde os nós da rede devem funcionar num sistema mais distribuído com vários *gateways* e procurar alternativas, ou seja, não dependendo de um único *basestation* para enviar os dados.

4. **Auditing**: É importante também manter um sistema de verificação periódica da validade dos dados recebidos nos *gateways*, sendo estes os responsáveis por reportar todos os acontecimentos relevantes ao funcionamento do sistema. Desenvolver um sistema de *logs* permite a gestão do funcionamento dos vários dispositivos da rede.

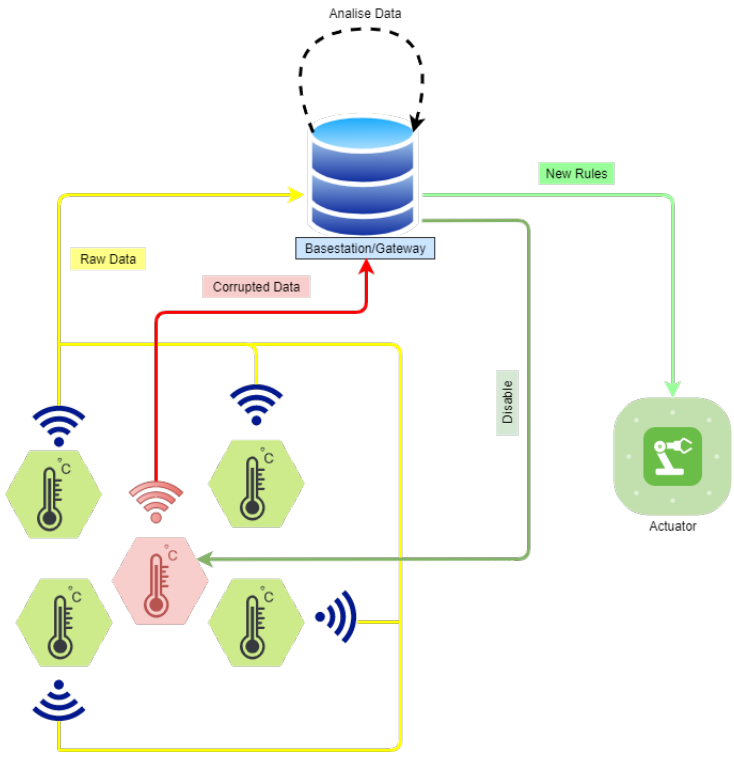

Fig. 8. Deteção de um dispositivo anómalo.

5. **Privacidade e Anonimato**: Corrigir ameaças relacionadas com privacidade resolve-se maioritariamente com as medidas adotadas anteriormente na proteção dos dados recolhidos da produção agrícola.
   Já é mais complicado proteger os sistemas de ataques como o *Hop-by-Hop backtracking*, não sendo tão crítico a sua resolução, a não ser que essa informação não seja partilhada através das mensagens trocadas e exista uma lista de dispositivos que podem estabelecer comunicações como forma de autenticação.

5 Validação do modelo

São muitos os cenários que podem por em causa um sistema como este podendo ameaçá-lo em várias vertentes.

Conseguimos verificar que, de forma geral, as situações mais críticas que podem comprometer os dados, a privacidade e integridade dos mesmos ocorrem quando falamos da utilização massiva de aparelhos de baixa capacidade de processamento e por vezes instáveis, mas cuja produção e tomada de decisões depende inteiramente da credibilidade introduzida pelos mesmos.

Adotar padrões de segurança de *hardware* e *software* nestes aparelhos e nos sistemas que comunicam com eles é um esforço coletivo que garante o direito e manutenção de dados a quem deve garantir, ou seja, aos donos dos campos de cultivo em questão.

O modelo aqui adotado segue isso mesmo e visa apresentar os principais pontos críticos e como contorná-los de modo a minimizar o trabalho de resolver problemas de segurança futuros e manter uma saúde pessoal dos futuros consumidores e do setor económico.

References

[1] "Precision Agriculture." Wikipedia, Wikimedia Foundation, 21 Oct. 2020, en.wikipedia.org/wiki/Precision_agriculture.

[2] "Wireless Sensor Network." Wikipedia, Wikimedia Foundation, 15 Oct. 2020, en.wikipedia.org/wiki/Wireless_sensor_network.

[3] Diagram made with a web tool. "Diagrams.net - Free Flowchart Maker and Diagrams Online." Flowchart Maker amp; Online Diagram Software, app. diagrams.net.

[4] "Sustainable Farming and the IoT: Cocoa Research Station in Indonesia." Libelium, 15 Dec. 2015, www.libelium.com/libeliumworld/success-stories/sustainable-farming-and-the-iot-cocoa-research-station-in-indonesia/.

[5] Research paper. https://www.researchgate.net/publication/334762096_ZigBee_Security_Vulnerabilities_Exploration_and_Evaluating

[6] Research paper. https://www.researchgate.net/publication/323999621_Performance_evaluation_on_TelosB_mote_of_a_secure_data_aggregation_protocol_using_ECC

[7] "Common Weakness Enumeration." CWE, cwe.mitre.org/.