Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Fractional Cyber–Biological Model for Energy-Aware Trust-Based Mobile-Agent Wireless Sensor Networks: Secure Plant-Disease Surveillance

Taylan Demir

1996.matematik.1996@gmail.com

Ankara University https://orcid.org/0000-0001-7402-4468

Shkelqim Hajrulla

Epoka University

Loubna Ali

Faculty of Computer Science and Informatics (BSBI)

Research Article

Keywords: Caputo fractional derivative; wireless sensor networks; plant-disease surveillance; leaf wetness; trust management; secure sensor fusion; mobile agents; selective forwarding; cyber–biological modeling.

Posted Date: September 22nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11103886/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

A Fractional Cyber–Biological Model for Energy-Aware Trust-Based Mobile-Agent Wireless Sensor Networks: Secure Plant-Disease Surveillance

Taylan Demir[1,*], Shkelqim Hajrulla[2], Loubna Ali[3]

[1]Department of Mathematics, Faculty of Science, Ankara University, Ankara, Turkiye

[2]Department of Computer Engineering, Epoka University, Tirana, Albania

[3]Faculty of Computer Science and Informatics (BSBI), Berlin, Germany

[*]Corresponding author: demir.taylan96@gmail.com

Abstract

Low-power wireless sensor networks increasingly act as the measurement layer of biological decision systems, so a communication-security failure can propagate beyond the network and distort downstream biological inference. We formulate this interaction in two coupled layers. The cyber layer is a three-state Caputo fractional differential system for normalized residual energy, trust, and compromise probability under bounded selective-forwarding or on–off attack evidence. A mobile-agent utility rule converts these states into an energy-aware routing decision. The model is well posed on finite horizons, the physical cube $[0,1]^3$ is positively invariant, and the constant-attack trust–compromise equilibrium satisfies the Matignon sector condition for every $0 < \alpha \leq 1$. Thus the fractional order changes transient memory without moving the constant-attack equilibrium. The biological layer is a plant-disease biosurveillance module: relative humidity, leaf wetness, and thermal suitability are combined into a normalized microclimate infection-suitability index, while cyber reliability states generate time-dependent fusion weights for competing sensor nodes. The fused signal drives a bounded disease-pressure equation used as a disease-generic biological decision state. A synthetic five-node greenhouse experiment couples an internal selective-forwarding episode to falsified microclimate data. For $\alpha = 0.85$, trust-aware fusion reduces the attack-window root-mean-square error of the environmental suitability estimate from 0.07162 to 0.02818. The corresponding error in the downstream disease-pressure state decreases from 0.02059 to 0.00645. The improvement is not instantaneous: at attack onset, the previously trusted compromised node can transiently receive excessive weight before its trust state reacts. This delay exposes a genuine security–biology trade-off rather than an artificial claim that fractionalization is intrinsically beneficial. The resulting framework connects packet evidence, fractional cyber memory, secure sensor fusion, and biological risk estimation in a single reproducible model.

Keywords: Caputo fractional derivative; wireless sensor networks; plant-disease surveillance; leaf wetness; trust management; secure sensor fusion; mobile agents; selective forwarding; cyber–biological modeling.

2020 Mathematics Subject Classification: 26A33; 34A08; 34D20; 68M12; 92C47; 92C80; 92D30.

1 Introduction

Wireless sensor networks (WSNs) combine low-power sensing, local computation, and wireless communication in environments where battery capacity and security exposure are both severe design constraints. The classical architectural difficulties identified in early WSN studies—limited energy, bandwidth, memory, and computation—remain relevant in current Internet-of-Things deployments [1]. Security mechanisms cannot therefore be evaluated independently of their energetic cost. A trust rule that detects compromised nodes reliably but requires excessive message exchange may reduce network lifetime enough to defeat its operational purpose.

Agricultural and biological monitoring sharpen this requirement because network data can directly influence disease-warning or intervention decisions. Wireless sensor networks have long been used to collect spatially distributed agricultural measurements [16, 17]. In plant-disease management, microclimatic variables such as leaf wetness, relative humidity, and temperature are especially important because many foliar infection processes depend on the persistence of free water under suitable thermal conditions [18, 20]. IoT-enabled leaf-wetness sensors have consequently been developed for in-situ disease monitoring [19]. A compromised relay in such a system is therefore not merely a networking problem: packet suppression or falsified sensing can bias a biological risk estimate and alter the timing of disease-management decisions.

Trust and reputation mechanisms were introduced precisely because cryptographic protection alone does not resolve the problem of an authenticated node that later behaves maliciously. Reputation-based frameworks such as RFSN [2] and subsequent surveys [3, 4, 5] formalized the use of behavioral evidence for secure node selection, routing, and data aggregation. Internal attacks are particularly difficult because the adversary may possess legitimate credentials. Selective forwarding is a representative example: a compromised relay forwards some packets but discards others, making malicious loss difficult to separate from channel-induced loss. On–off attacks exploit the same weakness temporally by alternating cooperative and malicious phases so that a reputation score partially recovers between attacks [6, 7].

Energy awareness introduces a second layer of feedback. Trust-based cluster-head selection and secure routing protocols explicitly combine residual energy with trust indicators [8, 9, 10, 11]. Recent work continues to emphasize that security and energy efficiency must be treated jointly rather than as separable objectives [12]. Mobile agents provide a natural implementation mechanism for this coupling. Instead of transferring all raw measurements repeatedly to a sink, executable software entities can migrate through selected nodes, aggregate data locally, and return compressed information. This paradigm has been studied for energy-aware data collection and itinerary planning [13, 14, 15]. Yet mobile-agent selection remains vulnerable if node trust is treated as a memoryless scalar updated only from the most recent observation.

The mathematical issue is therefore not simply how to compute a trust score. The more basic question is how past forwarding behavior, present compromise risk, and energy depletion should interact over time. Fractional differential equations offer one possible low-dimensional representation of such history dependence. For the Caputo derivative, the present rate depends on a power-law weighted history of the state. This feature has been used broadly to model hereditary and nonlocal processes [21, 22, 23, 24]. In the present setting, the fractional order is

not introduced as an automatic performance-improvement parameter. It is used as an explicit memory scale whose dynamical consequences can be analyzed.

The contribution of this paper is fivefold.

(i) We introduce a coupled fractional model for normalized residual energy $E(t)$, trust $T(t)$, and compromise probability $C(t)$ under a bounded attack intensity $A(t)$. The three state variables enter the same dynamical system rather than being combined only after independent estimation.

(ii) We define an energy-aware mobile-agent utility functional and a threshold decision rule. The rule exposes the trade-off between retaining a high-energy node and excluding a node whose trust has degraded or whose compromise probability has increased.

(iii) We establish basic mathematical properties of the model: finite-horizon existence and uniqueness, positive invariance of the physical state region, the unique constant-attack equilibrium of the trust–compromise subsystem, and local fractional-order stability via the Matignon sector criterion [27].

(iv) We perform reproducible synthetic experiments using a fractional Adams–Bashforth–Moulton predictor–corrector scheme [25, 26]. Persistent selective-forwarding and bursty on–off attacks are compared across $\alpha \in \{1, 0.95, 0.85, 0.75\}$. A step-refinement test is included to separate dynamical conclusions from numerical discretization effects.

(v) We add an applied packet-to-decision layer for a five-node mobile-agent routing problem. Packet forwarding counts, estimated benign link loss, battery telemetry, communication load, and hop cost are mapped into the fractional state equations and a guarded next-host selection rule. This case study makes the deployment interpretation explicit and exposes the price of memory as a finite detection delay.

(vi) We couple the network model to a disease-generic plant biosurveillance layer. Microclimate observations are fused with state-dependent reliability weights and drive a bounded biological disease-pressure variable. This extension quantifies how a cyber compromise propagates into biological inference and how trust-aware fusion limits that propagation after the detection transient.

A central conclusion is deliberately restrained: for constant attack intensity, the equilibrium does not depend on α. Fractional memory changes how rapidly the system approaches that equilibrium and how strongly it retains past attack episodes. Consequently, a smaller fractional order can attenuate short attack bursts over a finite observation horizon, but the same memory can prolong the influence of earlier events and delay recovery. This distinction is important if fractional models are to be used as mechanisms rather than as purely curve-fitting devices.

2 Background and related work

2.1 Trust management and internal attacks

A trust-management system typically collects direct or indirect evidence, converts it into a reputation or trust value, and uses that value in a decision layer. The literature contains Bayesian, beta-distribution, fuzzy, Dempster–Shafer, machine-learning, and hybrid approaches; comprehensive reviews are given in [3, 4, 5]. A common design difficulty is temporal manipulation. If old cooperative behavior is weighted too strongly, an on–off attacker can accumulate enough reputation to survive subsequent malicious intervals. If old behavior is forgotten too rapidly, normal nodes can be penalized by transient channel failures. Time-window and trend-based mechanisms have therefore been proposed specifically against time-varying reputation attacks [6, 7].

The present model does not replace packet-level trust estimation. Instead, it provides a continuous-time state layer into which packet-level observations can be mapped through $A(t)$ and parameter calibration. This separation is useful: the trust evidence mechanism may vary across protocols, while the resulting state dynamics can still be studied in a common analytic framework.

2.2 Energy-aware trust and mobile agents

Residual energy is routinely used in cluster-head selection and routing because repeated selection of a highly trusted but nearly depleted node can create an energy hole. LEACH-TM, for example, combines trust management with energy-aware hierarchical routing [8]. More recent schemes similarly mix trust, residual energy, cryptographic protection, or optimization-based weighting [9, 10, 11, 12]. Such approaches motivate a state model in which energy and trust are dynamically coupled rather than ranked independently.

Mobile agents offer a complementary way to reduce communication overhead. Energy-aware itinerary design, local aggregation, and multiple-agent strategies have been reported in [13, 14, 15]. In a security-sensitive deployment, however, an itinerary planner should avoid nodes that are energetic but behaviorally suspicious. This motivates the utility rule introduced in Section 7.

2.3 Wireless sensing for plant-disease biosurveillance

Wireless sensing is now a standard component of precision-agriculture architectures, where distributed nodes collect environmental and crop-related variables under strict energy and communication constraints [16, 17]. For foliar disease-warning systems, leaf wetness is particularly informative because the presence and duration of free water, together with favorable temperature, can control pathogen germination and infection opportunities [18]. This has motivated both dedicated leaf-wetness instrumentation and IoT-connected sensing platforms [19].

The biological use of these measurements changes the meaning of network trust. If a compromised node only degrades throughput, the loss is primarily computational or energetic. If the same node reports environmental variables used in disease prediction, its data can also distort an epidemiological or plant-protection decision. The study of plant epidemics emphasizes that disease intensity is a dynamic quantity and that sampling and environmental observations connect

biological theory to practical decision making [20]. We therefore treat secure data fusion as an explicit interface between the network state and a downstream biological state rather than as a post-processing detail.

2.4 Why a Caputo state model?

For $0 < \alpha < 1$, the Caputo derivative is

$$ {}^{C}D_t^{\alpha} x(t) = \frac{1}{\Gamma(1-\alpha)} \int_0^t \frac{x'(s)}{(t-s)^{\alpha}}\, ds. \tag{1} $$

Unlike an ordinary derivative, (1) weights the complete state history. The kernel has a slow algebraic tail, so an attack episode can influence the subsequent state even after the external attack intensity has changed. The Caputo form is convenient for initial-value problems because classical initial conditions can be used [22, 23, 24]. Stability of commensurate linear fractional systems is governed by an angular condition on eigenvalues rather than by the sign of the real part alone [27].

We stress a modeling limitation at the outset. A Caputo law is a phenomenological representation of memory; it is not derived here from a microscopic packet-arrival process. The value of α must therefore be estimated or justified from data in an eventual deployment. The current paper studies the mathematical consequences of such a memory law and provides a reproducible synthetic benchmark.

3 Network assumptions and attack representation

Consider a WSN with a sink, stationary sensor nodes, and one or more mobile software agents. A mobile agent visits selected nodes, performs local data collection or aggregation, and transfers a reduced payload along its itinerary. We study the state of a representative candidate node. The network-level policy can apply the same local state model to every candidate and rank nodes by the utility introduced below.

Let

$$ E(t) \in [0,1], \qquad T(t) \in [0,1], \qquad C(t) \in [0,1] $$

denote normalized residual energy, trust, and compromise probability. The exogenous communication load is denoted by $\rho \in [0,1]$. The attack signal

$$ A : [0,\infty) \longrightarrow [0,1] $$

is assumed piecewise continuous. It is not a binary label: intermediate values can represent partial packet dropping, uncertain evidence, or a posterior attack score obtained from a detector.

Two attack profiles are used in the experiments.

Persistent selective forwarding. A constant level

$$ A(t) = a_s, \qquad 0 < a_s < 1, \tag{2} $$

represents a compromised relay that continuously drops or manipulates a fixed fraction of traffic.

On–off attack. For low and high intensities $0 \le a_L < a_H \le 1$,

$$A(t) = a_L + (a_H - a_L) \sum_{k=1}^{m} \mathbf{1}_{I_k}(t), \tag{3}$$

where the intervals I_k are disjoint. This profile alternates between nearly cooperative behavior and aggressive attack phases.

The abstraction in (2)–(3) deliberately separates attack detection from state evolution. A packet-level detector can be changed without altering the analysis as long as its output is normalized to $[0, 1]$.

4 Fractional energy–trust–compromise model

We propose the commensurate Caputo system

$$^{C}D_t^{\alpha} E = -E\big(\varepsilon_0 + \varepsilon_1 \rho + \varepsilon_2 C + \varepsilon_3 A(t)\big), \tag{4a}$$

$$^{C}D_t^{\alpha} T = \lambda(1 - T) - \mu C T - \xi A(t) T, \tag{4b}$$

$$^{C}D_t^{\alpha} C = \kappa A(t)(1 - C) - \delta T C, \tag{4c}$$

with

$$0 < \alpha \le 1, \qquad E(0) = E_0, \quad T(0) = T_0, \quad C(0) = C_0 \in [0, 1].$$

All coefficients are nonnegative, with

$$\varepsilon_0, \lambda, \kappa, \delta > 0.$$

The terms in (4) have direct interpretations. The baseline term ε_0 represents unavoidable node activity; $\varepsilon_1 \rho$ represents communication load; $\varepsilon_2 C$ penalizes processing, retransmission, or defensive overhead associated with a compromised state; and $\varepsilon_3 A$ represents attack-induced expenditure. Trust relaxes toward one at rate λ in the absence of evidence against the node. The terms $\mu C T$ and $\xi A T$ decrease trust when compromise risk or direct attack evidence is present. Compromise probability grows with attack exposure through $\kappa A(1-C)$ and is reduced by trustworthy behavior through $\delta T C$.

For dimensional consistency, the coefficients multiplying the right-hand side have units of time$^{-\alpha}$ when physical time is dimensional. In normalized simulations below, time is scaled and the coefficients are dimensionless in the corresponding fractional time unit.

5 Well-posedness and state constraints

Let

$$x(t) = (E(t), T(t), C(t))^{\mathsf{T}}, \qquad \Omega = [0, 1]^3,$$

and write (4) as $^{C}D_t^{\alpha} x = f(t, x)$.

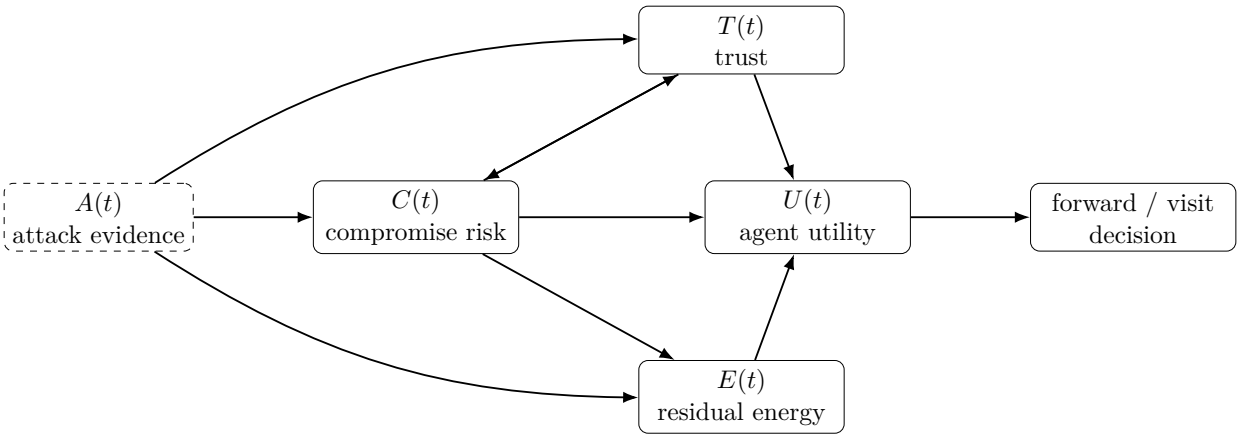


Figure 1: State coupling in the proposed model. The external attack signal changes compromise risk, trust, and attack-induced energy consumption; the mobile-agent decision uses all three states.

Theorem 5.1 (Finite-horizon existence and uniqueness)**.** *Let $A(t)$ be piecewise continuous and bounded in $[0,1]$, and let $x_0 \in \Omega$. For every finite $t_f > 0$, system (4) admits a unique continuous solution on $[0, t_f]$.*

Proof. For fixed t, the map $x \mapsto f(t,x)$ is polynomial in (E,T,C) and is therefore locally Lipschitz on $\mathbb{R}^3$. Since A is bounded and piecewise continuous, f is measurable in t and continuous on every interval not containing a switching point. The Caputo initial-value problem is equivalent to the Volterra equation

$$x(t) = x_0 + \frac{1}{\Gamma(\alpha)} \int_0^t (t-s)^{\alpha-1} f(s, x(s))\, ds. \tag{5}$$

Standard local existence and uniqueness for Caputo equations follows from the local Lipschitz property [22, 24]. The invariant-region result below prevents finite-time escape from the compact physical region, so the solution extends to every finite horizon. □

Theorem 5.2 (Positive invariance)**.** *Assume $x_0 \in \Omega$ and $A(t) \in [0,1]$. Under the standard Caputo comparison principle, $\Omega = [0,1]^3$ is positively invariant for (4).*

Proof. It is enough to inspect the vector field on the six faces of the cube. At $E = 0$,

$$f_E(t, 0, T, C) = 0,$$

whereas at $E = 1$,

$$f_E(t, 1, T, C) = -\big(\varepsilon_0 + \varepsilon_1 \rho + \varepsilon_2 C + \varepsilon_3 A\big) \le 0.$$

At the trust boundaries,

$$f_T(t, E, 0, C) = \lambda > 0, \qquad f_T(t, E, 1, C) = -(\mu C + \xi A) \le 0.$$

Finally,

$$f_C(t, E, T, 0) = \kappa A \ge 0, \qquad f_C(t, E, T, 1) = -\delta T \le 0.$$

Thus the field is inward-pointing or tangent on each boundary face. The fractional comparison principle prevents a first exit through any face; see, for example, the comparison framework in

[28, 24]. Hence trajectories initiated in Ω remain in Ω. □

Remark 5.3. The boundary calculation is simple, but the fractional setting matters: one should not replace the comparison argument by an ordinary-derivative "first crossing" proof without justification. The statement above explicitly invokes the Caputo comparison principle.

Proposition 5.4 (Energy comparison bound)**.** *Let*

$$g_{\min} = \varepsilon_0 + \varepsilon_1\rho, \qquad g_{\max} = \varepsilon_0 + \varepsilon_1\rho + \varepsilon_2 + \varepsilon_3.$$

Then, for $E_0 \geq 0$*,*

$$E_0 E_\alpha(-g_{\max} t^\alpha) \;\leq\; E(t) \;\leq\; E_0 E_\alpha(-g_{\min} t^\alpha), \tag{6}$$

whenever the scalar Caputo comparison theorem is applied to (4a)*.*

Proof. Because $C, A \in [0,1]$,

$$g_{\min} \leq \varepsilon_0 + \varepsilon_1\rho + \varepsilon_2 C + \varepsilon_3 A \leq g_{\max}.$$

Compare (4a) with the scalar equations

$${}^C D_t^\alpha z_\pm = -g_{\min\,/\,\max} z_\pm, \qquad z_\pm(0) = E_0,$$

whose solutions are Mittag–Leffler functions. The comparison principle gives (6). □

6 Constant-attack equilibria and fractional stability

Suppose $A(t) \equiv a \in [0,1]$ and ρ is constant. Because there is no harvesting term in (4a), the full long-time equilibrium has $E^* = 0$. This should not be interpreted as a network failure prediction at a specific physical time: E is a normalized depletion variable and the model is intended for finite-horizon policy analysis unless an energy-harvesting term is added.

The nontrivial equilibrium structure lies in the trust–compromise subsystem.

Theorem 6.1 (Unique admissible trust–compromise equilibrium)**.** *For* $a > 0$*, the subsystem* (4b)–(4c) *has a unique equilibrium* $(T^*, C^*) \in (0,1)^2$*. It satisfies*

$$T^* = \frac{\lambda}{\lambda + \mu C^* + \xi a}, \tag{7}$$

$$C^* = \frac{\kappa a}{\kappa a + \delta T^*}, \tag{8}$$

where T^* *is the unique positive root of*

$$\delta(\lambda + \xi a)(T^*)^2 + \Big[\kappa a(\lambda + \mu + \xi a) - \lambda\delta\Big] T^* - \lambda\kappa a = 0. \tag{9}$$

For $a = 0$*,* $(T^*, C^*) = (1, 0)$*.*

Proof. At equilibrium, (4b) and (4c) give (7) and (8). Substituting (8) into (7) yields (9). For $a > 0$, the leading coefficient is positive and the constant term is negative. Therefore the two

roots of (9) have opposite signs, so there is exactly one positive root. From (7), this root satisfies $T^* < 1$. Equation (8) then gives $0 < C^* < 1$. When $a = 0$, the equations reduce immediately to $T^* = 1$ and $C^* = 0$. □

Theorem 6.2 (Local asymptotic stability for all $0 < \alpha \leq 1$)**.** *Let $a \in [0, 1]$ be constant. The admissible equilibrium of the trust–compromise subsystem is locally asymptotically stable for every commensurate order $0 < \alpha \leq 1$.*

Proof. The Jacobian of the (T, C) subsystem at (T^*, C^*) is

$$J_{TC} = \begin{pmatrix} -\lambda - \mu C^* - \xi a & -\mu T^* \\ -\delta C^* & -\kappa a - \delta T^* \end{pmatrix}. \tag{10}$$

Its trace is strictly negative. Its determinant can be rewritten as

$$\det J_{TC} = (\lambda + \mu C^* + \xi a)(\kappa a + \delta T^*) - \mu \delta T^* C^* \tag{11}$$

$$= (\lambda + \xi a)(\kappa a + \delta T^*) + \mu \kappa a C^* > 0. \tag{12}$$

Hence both eigenvalues have negative real part. If they are real, they lie on the negative real axis and have argument π. If they are complex, their negative real part implies

$$|\arg(\lambda_j)| > \frac{\pi}{2}.$$

Since $0 < \alpha \leq 1$,

$$\frac{\alpha\pi}{2} \leq \frac{\pi}{2},$$

and therefore every eigenvalue satisfies Matignon's sector condition

$$|\arg(\lambda_j)| > \frac{\alpha\pi}{2}.$$

The equilibrium is thus locally asymptotically stable [27]. □

Corollary 6.3 (Equilibrium is independent of fractional order)**.** *For constant attack intensity a, the coordinates (T^*, C^*) do not depend on α. The fractional order changes the transient approach to equilibrium, not the equilibrium itself.*

This corollary is central to the interpretation of the numerical results. Any finite-time advantage observed at smaller α must be described as a transient memory effect; it cannot be advertised as a different constant-attack steady state.

7 Energy-aware mobile-agent decision rule

We combine the three state variables through

$$U(t) = w_E E(t) + w_T T(t) - w_C C(t), \qquad w_E, w_T, w_C \geq 0, \qquad w_E + w_T + w_C = 1. \tag{13}$$

A candidate node is eligible for the mobile-agent itinerary when

$$U(t) \geq \Theta. \tag{14}$$

In safety-critical applications, (14) can be supplemented by hard guards

$$T(t) \geq T_{\min}, \qquad C(t) \leq C_{\max},$$

so that a large energy reserve cannot compensate for an unacceptable security state.

The utility is intentionally linear. Its purpose here is not to solve a multiobjective optimization problem but to expose the dynamic trade-off explicitly. Nonlinear utilities, learned weights, or context-dependent thresholds can be inserted without changing the state equations. The weights should ultimately be selected from deployment requirements rather than tuned to improve a single simulation metric.

8 Numerical method and reproducibility

8.1 Fractional predictor–corrector scheme

For a Caputo system

$${}^{C}D_t^{\alpha} x(t) = f(t, x(t)), \qquad x(0) = x_0,$$

we use the Adams-type predictor–corrector method of Diethelm, Ford, and Freed [25, 26]. On the uniform grid $t_n = nh$, the predictor is

$$x_{n+1}^{P} = x_0 + \frac{h^{\alpha}}{\Gamma(\alpha+1)} \sum_{j=0}^{n} b_{j,n+1} f(t_j, x_j), \tag{15}$$

where

$$b_{j,n+1} = (n+1-j)^{\alpha} - (n-j)^{\alpha}.$$

The corrector is

$$x_{n+1} = x_0 + \frac{h^{\alpha}}{\Gamma(\alpha+2)} \left[f(t_{n+1}, x_{n+1}^{P}) + \sum_{j=0}^{n} a_{j,n+1} f(t_j, x_j) \right], \tag{16}$$

with

$$a_{0,n+1} = n^{\alpha+1} - (n-\alpha)(n+1)^{\alpha}$$

and, for $1 \leq j \leq n$,

$$a_{j,n+1} = (n-j+2)^{\alpha+1} + (n-j)^{\alpha+1} - 2(n-j+1)^{\alpha+1}.$$

The future-node coefficient is one and is represented by the first term in brackets in (16).

Table 1: Baseline normalized parameters used in the numerical experiments.

Parameter	Value	Interpretation
ε_0	0.004	baseline energy expenditure
ε_1	0.006	communication-load coefficient
ε_2	0.012	compromise-related energy cost
ε_3	0.004	attack-related energy cost
ρ	0.45	normalized communication load
λ	0.08	trust recovery coefficient
μ	0.45	compromise-to-trust penalty
ξ	0.30	direct attack-to-trust penalty
κ	0.32	attack-to-compromise coefficient
δ	0.28	trust-mediated compromise removal
(E_0, T_0, C_0)	$(1, 0.92, 0.05)$	initial state
(w_E, w_T, w_C)	$(0.35, 0.45, 0.20)$	utility weights
Θ	0.30	eligibility threshold
h	0.25	time step
t_f	120	final normalized time

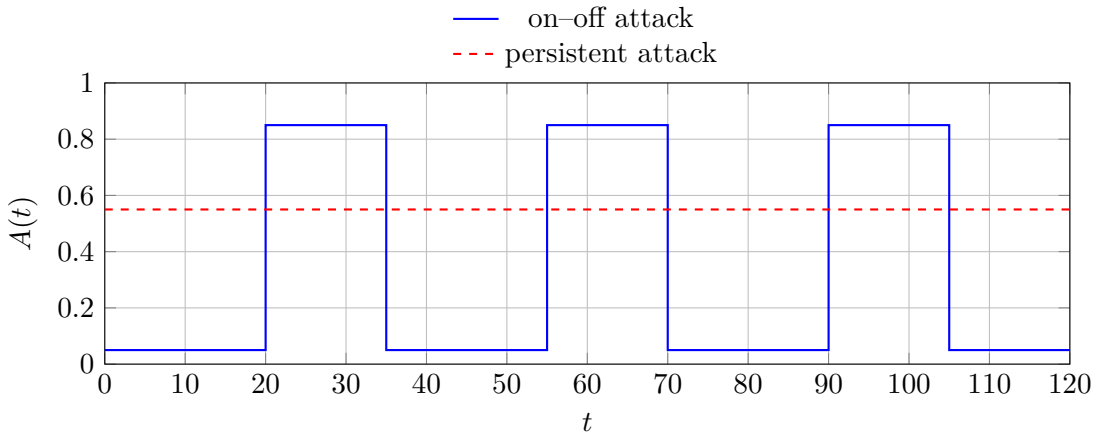


Figure 2: Attack profiles used in the numerical study.

8.2 Parameter set

The experiments are synthetic and are not claimed as calibration to a particular hardware platform. Their purpose is to test the mathematical mechanism under transparent, reproducible conditions. The baseline parameters are given in Table 1.

For the on–off scenario,

$$A(t) = \begin{cases} 0.85, & t \in [20, 35] \cup [55, 70] \cup [90, 105], \\ 0.05, & \text{otherwise.} \end{cases} \tag{17}$$

The persistent selective-forwarding benchmark uses $A(t) = 0.55$.

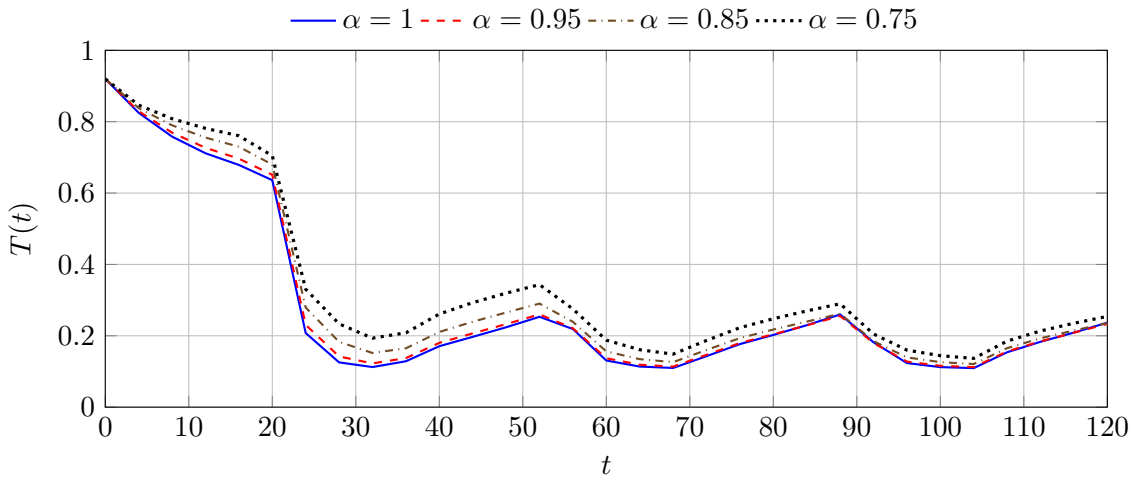


Figure 3: Trust trajectories under the on–off attack (17). Lower fractional order attenuates the finite-time depth of the attack response but retains past attack influence for longer.

9 Numerical results

9.1 Persistent attack: equilibrium check

For $a = 0.55$, Theorem 6.1 gives

$$T^* \approx 0.12941, \qquad C^* \approx 0.82927.$$

The integer-order trajectory at $t = 120$ reaches these values to the reported precision. Fractional trajectories with $\alpha < 1$ remain farther from the same equilibrium because their relaxation is slower. This is consistent with Corollary 6.3: the order modifies the transient, not the constant-attack fixed point.

For comparison, at the low background level $a = 0.05$,

$$T^* \approx 0.59514, \qquad C^* \approx 0.08760.$$

The large separation between these two equilibria explains the pronounced response to the high attack intervals in (17).

9.2 On–off trust dynamics

Figure 3 shows the trust state for four fractional orders. Each high-attack interval produces an abrupt directional change. The ordinary model ($\alpha = 1$) reacts most rapidly and reaches the lowest trust minimum. Smaller orders spread the effect of each attack over a longer history and reduce the instantaneous depth of the trust collapse. The price is slower recovery after the attack is removed.

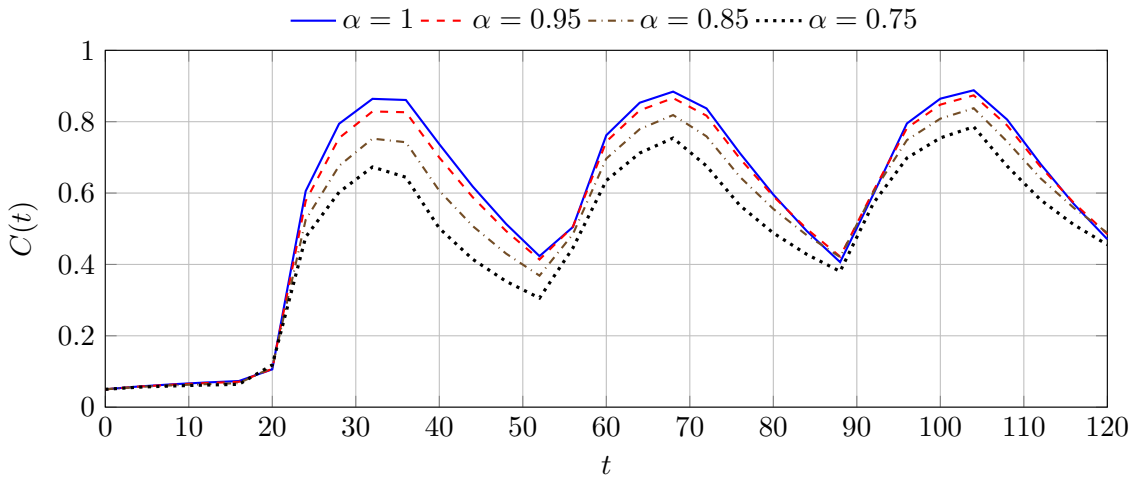


Figure 4: Compromise probability under repeated on–off attack intervals.

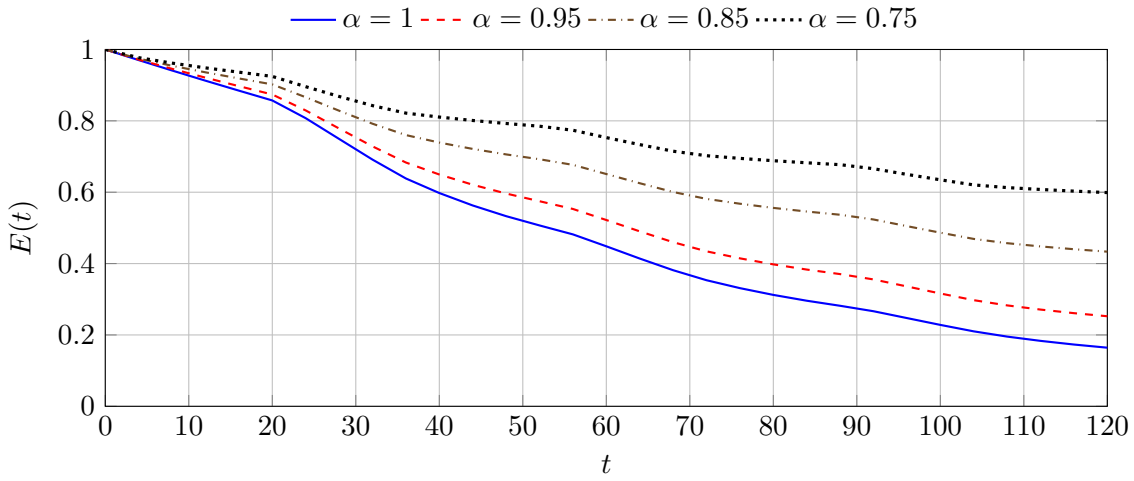


Figure 5: Normalized residual energy under the on–off attack.

9.3 Compromise probability

The same memory trade-off appears in $C(t)$; see Figure 4. The maximum compromise probability decreases from approximately 0.891 at $\alpha = 1$ to 0.791 at $\alpha = 0.75$ over the simulated horizon. This reduction should not be read as a universal security gain. Under a sufficiently long persistent attack, every order approaches the same equilibrium C^*.

9.4 Energy and decision utility

The energy equation reacts to both compromise risk and direct attack intensity. Figure 5 shows that the lower-order trajectories retain more normalized energy over the finite horizon. Again, this is a slower-transient effect: the fractional equation responds more gradually to cumulative expenditure.

The combined utility in (13) is shown in Figure 6. The horizontal line marks the baseline eligibility threshold $\Theta = 0.30$. Lower α keeps the utility above the threshold for a larger proportion of the finite simulation window because energy and security states move more slowly. Such retention can be useful when attack evidence is noisy, but it can also make exclusion of a genuinely malicious

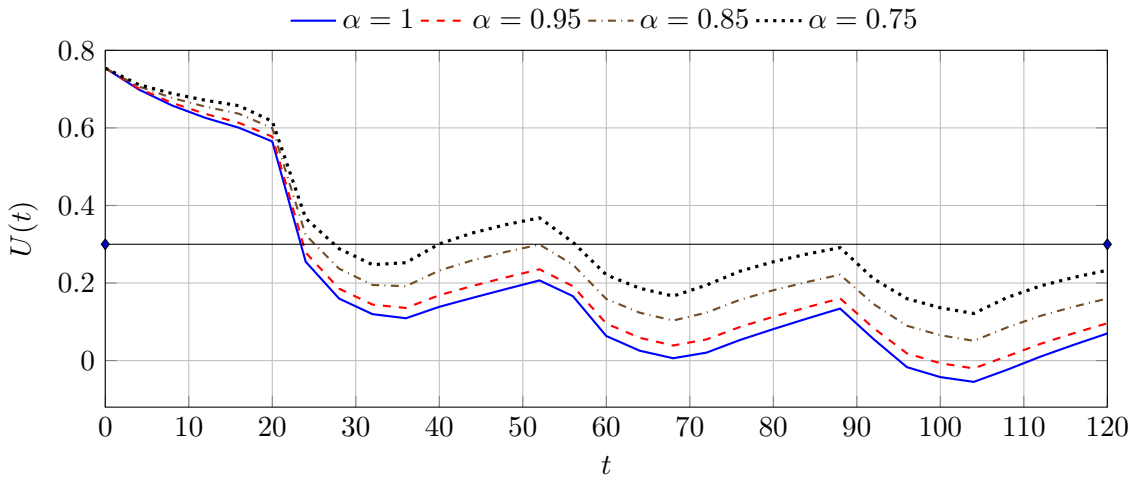


Figure 6: Energy–trust–compromise utility under the on–off attack. The thin horizontal line is $\Theta = 0.30$.

Table 2: Finite-horizon metrics for the on–off attack. These values describe the stated synthetic parameter set and are not hardware-calibrated performance claims.

α	$E(120)$	$\min T$	$\max C$	Eligible fraction
1.00	0.1643	0.1091	0.8909	0.1933
0.95	0.2524	0.1117	0.8775	0.1954
0.85	0.4334	0.1199	0.8427	0.2308
0.75	0.5990	0.1354	0.7915	0.3617

node less immediate. This is a policy trade-off rather than a monotone "smaller is better" effect.

9.5 Summary metrics

Table 2 reports finite-horizon metrics for the on–off scenario. The eligible-time fraction is the fraction of grid points satisfying $U(t) \geq \Theta$.

For persistent $A = 0.55$, the corresponding values are given in Table 3. The difference among orders is again substantial at $t = 120$, but Theorem 6.1 shows that this difference is transient.

9.6 Phase-plane memory signature

Figure 7 plots the trust–compromise trajectories for the on–off experiment. Each attack pulse drives the state toward the persistent high-attack region; the low-attack intervals then pull it back toward the background equilibrium. Fractional memory changes the geometry and speed of these excursions. The loops are not periodic orbits: they are forced transient paths created by the switching attack signal.

9.7 Step refinement

To check that the principal observations are not artifacts of the baseline step, the $\alpha = 0.85$ on–off simulation was repeated with $h = 0.125$ and $h = 0.0625$. Table 4 reports differences at common

Table 3: Finite-horizon metrics for persistent selective-forwarding intensity $A(t) = 0.55$.

α	$E(120)$	$\min T$	$\max C$	Eligible fraction
1.00	0.1104	0.1294	0.8293	0.0603
0.95	0.1906	0.1305	0.8258	0.0686
0.85	0.3659	0.1350	0.8111	0.0956
0.75	0.5362	0.1453	0.7791	0.1414

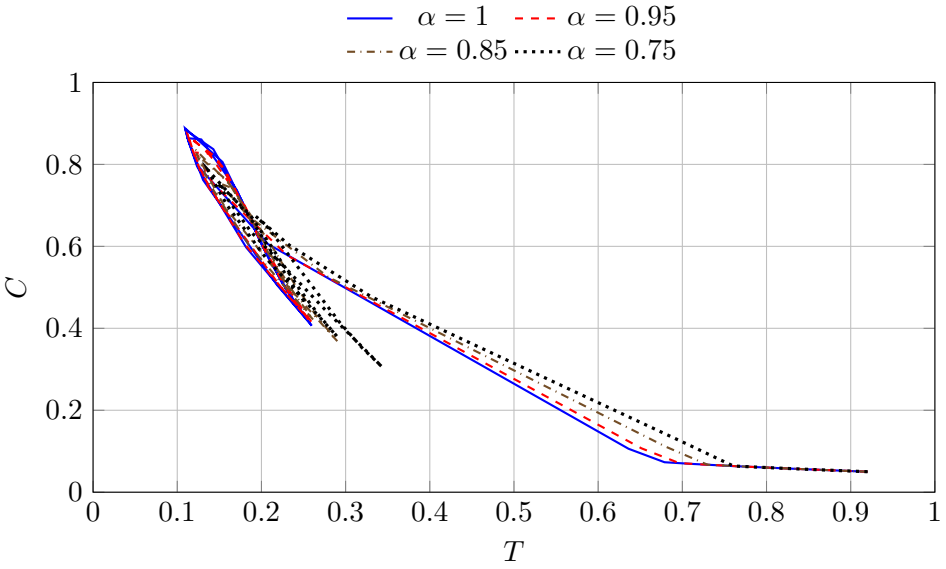


Figure 7: Trust–compromise trajectories under the same on–off attack profile.

grid points.

The largest errors occur near attack switching times, where $A(t)$ is discontinuous. The reduction under step refinement is consistent with numerical convergence of the reported trajectories. A deployment-oriented implementation should align switching events with the temporal grid or use event-aware quadrature.

10 Applied modeling: packet-informed mobile-agent itinerary selection

The state model becomes operational only after measurable network quantities are connected to $A(t)$, $E(t)$, and $\rho(t)$. This section gives one concrete realization for a mobile-agent WSN. The example is deliberately synthetic: it is not presented as a hardware calibration. Its purpose is to show how packet-level evidence can be converted into the continuous state model and how that state then changes an itinerary decision.

10.1 Measurement-to-state interface

Consider candidate node i during decision epoch k. Let $R_i[k]$ be the number of packets that should have been forwarded according to the routing schedule, and let $F_i[k]$ be the number verified as forwarded by watchdog acknowledgments or sink-side sequence information. The observed drop

Table 4: Step-refinement differences for $\alpha = 0.85$ under the on–off attack.

Comparison	E	T	C
max $\lvert x_{0.25} - x_{0.125}\rvert$	9.21×10^{-4}	1.33×10^{-2}	1.87×10^{-2}
RMS $\lvert x_{0.25} - x_{0.125}\rvert$	6.54×10^{-4}	1.71×10^{-3}	3.07×10^{-3}
max $\lvert x_{0.125} - x_{0.0625}\rvert$	4.65×10^{-4}	7.39×10^{-3}	1.04×10^{-2}
RMS $\lvert x_{0.125} - x_{0.0625}\rvert$	3.29×10^{-4}	8.51×10^{-4}	1.54×10^{-3}

ratio is

$$\widehat{d}_i[k] = 1 - \frac{F_i[k]}{R_i[k]}, \qquad R_i[k] > 0. \tag{18}$$

A nonzero drop ratio is not automatically malicious because wireless links also lose packets. Let $q_i \in [0, 1)$ denote an estimated benign loss baseline. We therefore define the normalized attack evidence

$$A_i[k] = \mathrm{clip}_{[0,1]}\left(\frac{\widehat{d}_i[k] - q_i}{1 - q_i}\right), \tag{19}$$

where $\mathrm{clip}_{[0,1]}(z) = \min\{1, \max\{0, z\}\}$. This normalization has a useful interpretation: $A_i = 0$ corresponds to loss explainable by the benign baseline, while $A_i = 1$ corresponds to essentially complete forwarding failure after the baseline has been removed.

Residual energy is obtained directly from battery telemetry,

$$E_i[k] = \frac{B_i[k]}{B_i[0]}, \tag{20}$$

with $B_i[k]$ the available battery energy. Communication load can be normalized from packet activity, for example

$$\rho_i[k] = \min\left\{1, \frac{N_i^{\mathrm{tx}}[k] + N_i^{\mathrm{rx}}[k]}{N_{\max}}\right\}. \tag{21}$$

Equations (19)–(21) provide the interface between network measurements and the continuous-time model. Between decision epochs the measured inputs are held piecewise constant.

For M candidate nodes, the local dynamics are replicated nodewise:

$${}^{C}D_t^{\alpha} x_i(t) = f_i(t, x_i(t); A_i(t), \rho_i(t)), \qquad x_i = (E_i, T_i, C_i)^{\mathsf{T}}, \quad i = 1, \ldots, M. \tag{22}$$

No coupling between different nodes is required at the state-estimation level. The coupling enters through the itinerary decision because the mobile agent chooses one candidate from the admissible set.

10.2 Guarded itinerary score

A practical mobile-agent itinerary should account not only for security state but also for the communication effort needed to reach the candidate. Let $H_i \in [0, 1]$ denote a normalized hop or migration cost from the current agent host to node i. We use

$$S_i(t) = 0.30E_i(t) + 0.40T_i(t) - 0.20C_i(t) - 0.10H_i. \tag{23}$$

The coefficients in (23) are illustrative policy weights rather than fitted constants. Security is protected by hard guards:

$$E_i(t) \geq 0.20, \qquad T_i(t) \geq 0.22, \qquad C_i(t) \leq 0.65. \tag{24}$$

If $\mathcal{A}(t)$ is the set of nodes satisfying (24), the next host is

$$i^*(t) = \arg\max_{i \in \mathcal{A}(t)} S_i(t). \tag{25}$$

Thus a high-energy node cannot remain eligible solely because of its battery level if its trust or compromise state violates a security guard.

10.3 Five-node greenhouse biosurveillance case study

To make the decision layer concrete, consider a small environmental-monitoring cluster in which a mobile software agent leaves its current host G, visits one of five candidate relay/aggregation nodes, and then continues toward the sink. Such an itinerary is consistent with the mobile-agent data-aggregation paradigm discussed in [13, 14, 15]. Figure 8 is a schematic representation; the geometry is illustrative and is not used as a radio-propagation model.

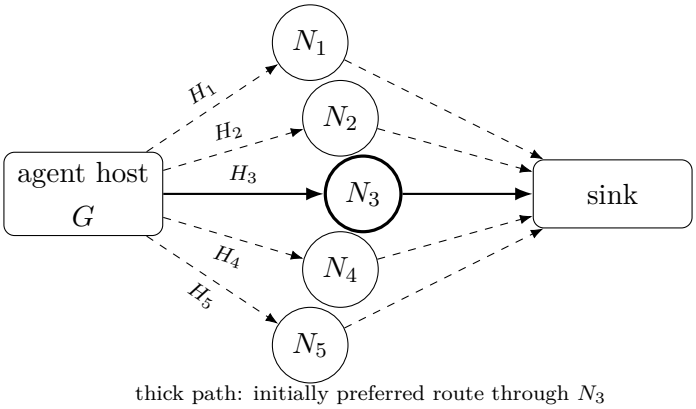


Figure 8: Illustrative five-node greenhouse biosurveillance network. Node N_3 initially has the best combined energy, trust, and hop-cost profile but later performs selective forwarding; the same compromised node is used below to stress-test biological data fusion.

The node-specific initial conditions are listed in Table 5. All rate coefficients are retained from Table 1. The normalized hop cost H_i is fixed over the experiment, while ρ_i reflects a different communication burden for each candidate.

Table 5: Node-specific quantities for the applied routing case study.

Node	$E_i(0)$	$T_i(0)$	$C_i(0)$	ρ_i	H_i
N_1	0.82	0.82	0.08	0.40	0.50
N_2	0.80	0.84	0.07	0.50	0.35
N_3	1.00	0.99	0.01	0.30	0.15
N_4	0.78	0.80	0.08	0.30	0.55
N_5	0.85	0.83	0.10	0.65	0.40

Nodes N_1, N_2, and N_4 experience only low background evidence, with $A_1 = 0.03$, $A_2 = 0.04$, and $A_4 = 0.02$. Node N_5 has persistent suspicious behavior, $A_5 = 0.16$. Node N_3 is initially the preferred relay but launches one aggressive selective-forwarding episode,

$$A_3(t) = \begin{cases} 0.85, & 20 \le t \le 35, \\ 0.03, & \text{otherwise.} \end{cases} \tag{26}$$

For an illustrative benign loss estimate $q_3 = 0.02$ and $R_3 = 100$ expected forwarding events, (19) shows that $A_3 = 0.85$ corresponds to roughly fifteen successfully forwarded packets during an epoch, whereas the background value $A_3 = 0.03$ corresponds to about ninety-five. This translation is included only to give the normalized attack signal an observable packet-level meaning.

10.4 Applied routing outcome

The case study was simulated with the same PECE implementation as the single-node experiments. Table 6 compares the integer-order baseline with the fractional case $\alpha = 0.85$. Because N_3 has a strong initial score advantage, neither model removes it exactly at the attack onset. The integer-order model changes route at $t = 20.75$; the fractional model changes at $t = 21.00$. Hence memory introduces one additional $h = 0.25$ integration step of exposure in this particular configuration.

Table 6: Packet-informed itinerary response to the attack on N_3. "Attack decisions on N_3" counts grid decision times within $20 \le t \le 35$ for which N_3 is still selected.

α	route-change time	attack decisions on N_3	$E_3(35)$	$T_3(35)$	$C_3(35)$	$S_3(35)$
1.00	20.75	3	0.679	0.110	0.883	0.056
0.85	21.00	4	0.786	0.145	0.778	0.123

The state values at $t = 35$ illustrate the central trade-off. For $\alpha = 0.85$, the attacked node retains more energy and a higher trust value, and its compromise probability has grown less than in the ordinary model. The same slower response, however, delays route exclusion. This is precisely why the fractional order should not be interpreted as a monotone "security improvement" parameter. It reshapes the temporal weighting of evidence.

Figure 9 shows the applied score for the attacked node and the node that becomes the preferred safe alternative, N_4, when $\alpha = 0.85$. The crossing shortly after $t = 20$ triggers the route change.

After the attack is removed at $t = 35$, $S_3(t)$ recovers gradually but remains slightly below $S_4(t)$ through $t = 120$; numerically, $S_3(120) = 0.4220$ and $S_4(120) = 0.4237$. Thus the combined trust–compromise–energy state produces a natural hysteresis against immediate re-entry of a recently attacked relay.

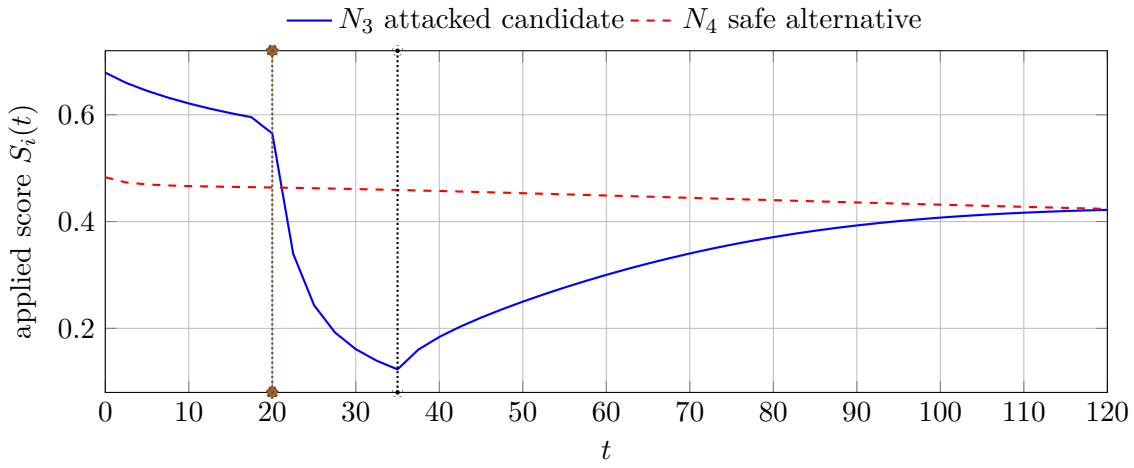


Figure 9: Applied itinerary scores for $\alpha = 0.85$. The vertical dotted lines delimit the selective-forwarding interval. The N_3–N_4 score crossing triggers migration away from the attacked relay.

This example supplies an explicit application chain,

$$\text{packet observations} \longrightarrow A_i(t) \longrightarrow (E_i, T_i, C_i) \longrightarrow S_i(t) \longrightarrow i^*(t),$$

which is absent from a purely phenomenological state model. In a field deployment, the same equations can be driven by measured forwarding counts and battery telemetry, while the policy weights and guards can be chosen from application-level risk tolerances.

11 Biological integration: secure plant-disease surveillance

The network model becomes biologically consequential when sensor values are used to drive a disease-warning state. We consider a greenhouse crop canopy as a concrete but disease-generic application. The purpose is not to calibrate a particular pathogen. Instead, the biological layer is constructed to answer a narrower question: if a compromised sensor node distorts microclimate data, how much of that distortion reaches a downstream disease-risk variable, and how much can the cyber trust state suppress it?

11.1 Microclimate infection-suitability index

Let $R_i(t) \in [0, 1]$ denote normalized relative humidity, $W_i(t) \in [0, 1]$ normalized leaf wetness, and $\vartheta_i(t)$ canopy temperature measured by node i. Leaf wetness and temperature are established inputs to many plant-disease warning systems because free water under favorable thermal conditions controls infection opportunities for numerous foliar pathogens [18, 20]. We introduce the

bounded thermal suitability function

$$G_\vartheta(\vartheta) = \exp\left[-\frac{(\vartheta - \vartheta^\star)^2}{2\sigma_\vartheta^2}\right] \in (0, 1], \tag{27}$$

and define a disease-generic local microclimate suitability score

$$Z_i(t) = 0.35R_i(t) + 0.45W_i(t) + 0.20G_\vartheta(\vartheta_i(t)). \tag{28}$$

The weights in (28) are illustrative and sum to one. They are not claimed as species-specific biological constants. In a field study they should be replaced by weights or a mechanistic infection function estimated for the host–pathogen system under consideration. The role of (28) is to provide a transparent map from sensor variables to a bounded quantity that can be corrupted by a compromised node.

11.2 Trust-aware biological data fusion

A simple arithmetic mean treats every node as equally reliable. The cyber state provides a natural alternative. For nodes satisfying the hard guards in (24), define

$$q_i(t) = E_i(t)T_i(t)\big[1 - C_i(t)\big], \qquad \omega_i(t) = \frac{q_i(t)}{\sum_{j\in\mathcal{A}(t)} q_j(t)}. \tag{29}$$

Nodes outside $\mathcal{A}(t)$ receive zero weight. The secure fused suitability is

$$\widehat{Z}_{\mathrm{sec}}(t) = \sum_{i\in\mathcal{A}(t)} \omega_i(t) Z_i^{\mathrm{obs}}(t), \tag{30}$$

whereas the unprotected baseline is

$$\widehat{Z}_{\mathrm{avg}}(t) = \frac{1}{M}\sum_{i=1}^{M} Z_i^{\mathrm{obs}}(t). \tag{31}$$

Equation (30) gives the network states a direct biological meaning. A node loses influence not because its environmental value is numerically unusual, but because independent forwarding evidence has reduced its trust or increased its compromise probability.

11.3 Bounded disease-pressure state

To isolate the effect of cyber memory, the biological layer is kept integer-order in the present paper. Let $P(t) \in [0, 1]$ denote normalized disease pressure rather than literal disease prevalence. We use

$$\frac{dP}{dt} = r_b\widehat{Z}(t)\big(1 - P(t)\big) - \gamma_b P(t), \qquad P(0) = P_0, \tag{32}$$

where $r_b > 0$ controls accumulation of environmentally supported infection pressure and $\gamma_b > 0$ represents decay when conditions become less favorable. This one-state equation is intentionally modest: it is a decision variable, not a mechanistic replacement for a pathogen-specific epidemic model.

Proposition 11.1 (Biological admissibility)**.** *If* $0 \le \widehat{Z}(t) \le 1$ *and* $P_0 \in [0,1]$*, then every solution of* (32) *remains in* $[0,1]$*. For constant* $\widehat{Z}(t) = z$*, the unique equilibrium is*

$$P^*(z) = \frac{r_b z}{r_b z + \gamma_b}. \tag{33}$$

Proof. At $P = 0$, the vector field equals $r_b \widehat{Z}(t) \ge 0$; at $P = 1$, it equals $-\gamma_b < 0$. Hence the interval $[0,1]$ is forward invariant. Setting the right-hand side of (32) to zero for constant z gives (33) directly. □

11.4 Synthetic greenhouse stress test

We reuse the five-node cyber trajectories from Section 10 with $\alpha = 0.85$ and introduce a latent, uncorrupted suitability field

$$Z^\star(t) = \mathrm{clip}_{[0,1]}\left[0.46 + 0.12\sin\left(\frac{2\pi t}{48}\right) + 0.06\sin\left(\frac{2\pi t}{19}\right)\right]. \tag{34}$$

The deterministic oscillations mimic changing greenhouse microclimate without being tied to a particular crop. Sensor observations are generated by

$$Z_i^{\mathrm{obs}}(t) = \mathrm{clip}_{[0,1]}\left[Z^\star(t) + b_i + 0.008\sin\left(\frac{2\pi t}{p_i} + \varphi_i\right) + u_i(t)\right], \tag{35}$$

with the deterministic settings in Table 7. During the selective-forwarding interval, compromised node N_3 also injects a positive falsification $u_3(t) = 0.36$ for $20 \le t \le 35$. All other u_i are zero. This compound scenario represents an internal node that both degrades forwarding and reports an artificially elevated disease-conducive microclimate. It is a stress test rather than an assertion that these two behaviors must occur together in practice.

Table 7: Deterministic sensor offsets used in the biological stress test.

Node	b_i	p_i	φ_i	falsification $u_i(t)$
N_1	-0.015	13	0	0
N_2	$+0.010$	15	1	0
N_3	$+0.005$	17	2	$0.36\,\mathbf{1}_{[20,35]}(t)$
N_4	-0.005	19	3	0
N_5	$+0.005$	21	4	0

For (32) we set $r_b = 0.10$, $\gamma_b = 0.06$, and $P_0 = 0.15$ in the same normalized time unit used by the cyber simulation. Three biological trajectories are then computed: the reference $P^\star$ driven by $Z^\star$, the unprotected trajectory P_{avg} driven by (31), and the trust-aware trajectory P_{sec} driven by (30).

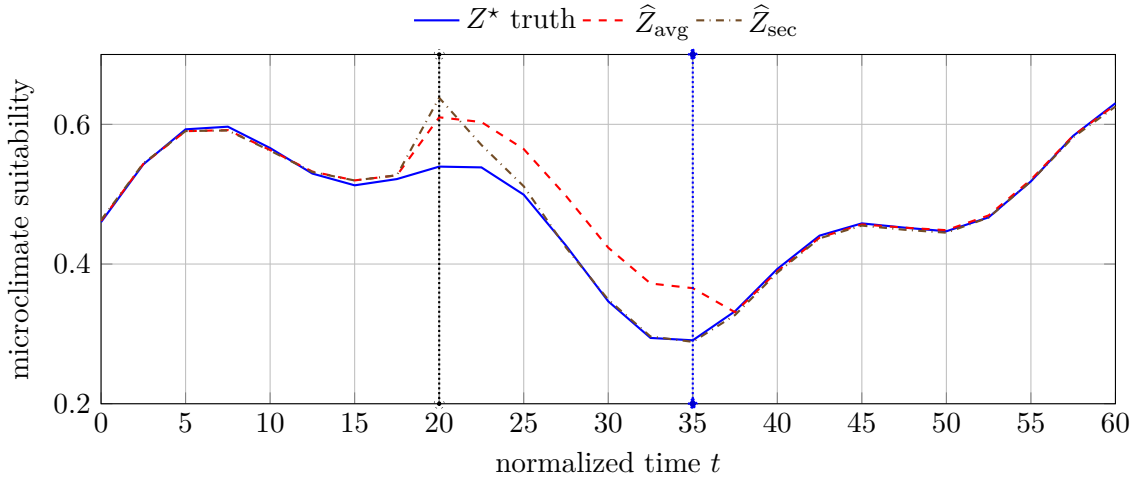


Figure 10: Microclimate suitability during the biological stress test. The compromised node begins with high cyber credibility, so trust-aware fusion initially overshoots more strongly at $t = 20$. As trust falls and compromise probability rises, its weight collapses and the secure estimate rapidly returns toward the latent field.

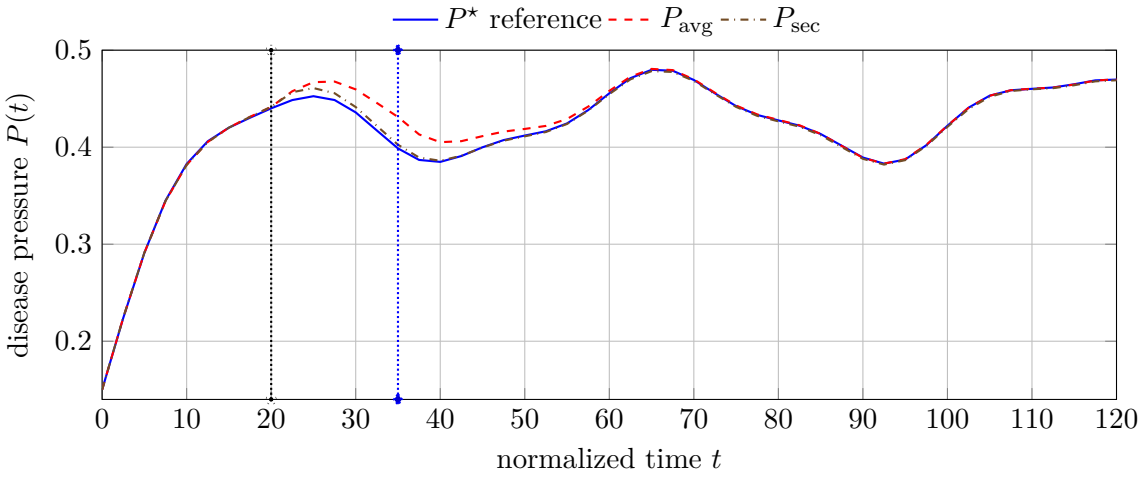


Figure 11: Propagation of sensor corruption into the downstream biological state. Naive averaging retains the false high-risk signal throughout the attack interval and leaves a visible post-attack bias. Trust-aware fusion substantially limits the integrated distortion after the cyber state has reacted.

11.5 Cyber-to-biological error propagation

Table 8 quantifies the biological effect. Over the attack interval, trust-aware fusion lowers the suitability RMSE from 0.07162 to 0.02818, a 60.7% reduction. The downstream disease-pressure RMSE decreases from 0.02059 to 0.00645, a 68.7% reduction. The benefit persists after the packet attack ends: over $35 \leq t \leq 60$, the disease-pressure RMSE is 0.01480 under naive averaging and 0.00130 under trust-aware fusion.

Table 8: Error propagation from compromised sensing to biological disease pressure for $\alpha = 0.85$. RMSE values are computed against the latent reference signals.

Quantity and interval	naive average	trust-aware fusion	reduction
Z, full horizon	0.02560	0.01047	59.1%
Z, attack interval $[20, 35]$	0.07162	0.02818	60.7%
P, full horizon	0.00989	0.00249	74.8%
P, attack interval $[20, 35]$	0.02059	0.00645	68.7%
P, post-attack $[35, 60]$	0.01480	0.00130	91.2%

A subtle point is visible in Figure 10. At exactly $t = 20$, the secure estimator has larger instantaneous error than the arithmetic mean because N_3 has accumulated a favorable trust history and therefore receives a comparatively large reliability weight. The security layer needs evidence before it can suppress the node. This behavior is not a defect of the numerical experiment; it is the expected price of history-dependent trust. The principal benefit appears in the integrated error once the cyber state responds. In a biological deployment where a short false alarm is costly, the weights in (29) should therefore be combined with anomaly gating or a faster direct-evidence channel rather than interpreted as a complete detector.

The complete cross-domain chain is now

$$\text{packet and sensor observations} \longrightarrow A_i(t),\ (E_i, T_i, C_i) \longrightarrow \omega_i(t) \longrightarrow \widehat{Z}_{\text{sec}}(t) \longrightarrow P_{\text{sec}}(t).$$

This is the point at which the network model becomes genuinely biological: cyber reliability affects the estimated environmental conditions, which in turn alter a dynamic disease-pressure state used for plant-health decision support.

12 Interpretation and design implications

The simulations reveal three effects that are easy to conflate.

First, the fractional order acts on *response speed and memory*, not on the location of the constant-attack equilibrium. This follows analytically from Corollary 6.3. Consequently, a smaller α can keep $T(t)$ higher and $C(t)$ lower during a finite burst simply because the state reacts more slowly. The same mechanism may be undesirable when a rapid exclusion decision is required.

Second, energy and trust cannot be optimized independently. A node with high trust but little remaining energy may be a poor mobile-agent destination; a node with abundant energy but a large compromise probability is unsafe. The utility (13) makes this trade-off visible. In practice, the weights should be set from application loss functions, and hard security constraints should be imposed when compromise risk exceeds an unacceptable level.

Third, an on–off attacker explicitly exploits memory. Memoryless or very short-window schemes can overreact to noise, whereas excessively long memory can allow historical cooperation to mask recent attacks. The Caputo order provides a continuous parameter controlling this balance. It does not eliminate the need for an attack detector; rather, it determines how the detector output

is accumulated dynamically.

Fourth, cyber uncertainty propagates into the biological layer nonlinearly in time. The greenhouse stress test shows that trust-aware fusion can greatly reduce accumulated disease-pressure error, but the protection is delayed because a previously reliable node remains influential at the beginning of the compromise. Biological decision support should therefore distinguish between long-memory reliability and rapid anomaly evidence. The former stabilizes decisions against noisy links; the latter is needed when a sudden corrupted measurement could trigger an expensive intervention.

These observations suggest a calibration strategy. Given packet traces, one can estimate $A(t)$ from forwarding failures or anomaly scores, infer $E(t)$ from battery telemetry, and fit α together with the rate parameters by minimizing a multi-state loss. Model selection should compare the fractional system against the $\alpha = 1$ baseline using out-of-sample data. Without such a comparison, the extra memory parameter is not justified merely because it yields a visually smoother trajectory.

13 Limitations

The present work is a mathematical and synthetic computational study. Several limitations should be kept explicit.

(i) The attack signal is exogenous. A complete cyber-physical model would couple packet-level observations, detector uncertainty, and attacker adaptation to $A(t)$.

(ii) The model describes a representative node. Network-wide congestion, interference, topology changes, and correlated compromise events are not represented explicitly.

(iii) The energy equation is normalized and does not include harvesting, sleep scheduling, or radio-specific transmit/receive costs. Those mechanisms can be added as additional terms once a hardware platform is fixed.

(iv) The fractional order is not estimated from field data in this study. The numerical results therefore establish dynamical consequences, not empirical superiority.

(v) The utility weights and threshold are illustrative. A real deployment requires sensitivity analysis against mission-specific costs and false-exclusion risk.

(vi) The biological suitability index and disease-pressure equation are disease-generic and are not calibrated to a specific crop–pathogen pair. They demonstrate cyber-to-biological error propagation, not a validated epidemiological forecast.

(vii) The greenhouse data are deterministic synthetic signals. Field validation would require synchronized leaf-wetness, humidity, temperature, packet, battery, and plant-disease observations, together with an independently established disease outcome.

These restrictions are intentional. They keep the first model analytically tractable while identifying exactly which claims are supported by the current mathematics.

14 Conclusion

We developed a fractional cyber–biological framework in which residual energy, trust, and compromise probability evolve through a Caputo state model and directly influence both mobile-agent routing and biological sensor fusion. The cyber state cube is positively invariant, the finite-horizon initial-value problem is well posed, and the constant-attack trust–compromise subsystem has a unique admissible equilibrium. Its Jacobian satisfies the Matignon sector condition for every $0 < \alpha \leq 1$. The analysis therefore separates equilibrium security from transient memory: changing α changes the temporal weighting of attack history but does not relocate the constant-attack equilibrium.

The plant-disease extension shows why this distinction matters outside communications. In the synthetic greenhouse experiment, a compromised high-trust node simultaneously performs selective forwarding and reports an artificially high disease-suitability signal. Naive sensor averaging transfers this corruption directly into the biological pressure state. State-dependent trust fusion reduces the attack-window suitability RMSE by 60.7% and the corresponding disease-pressure RMSE by 68.7%. The protection is not instantaneous; the compromised node briefly retains excessive influence because its prior trust is high. This transient exposes the operational cost of memory and argues for hybrid designs that combine long-horizon trust with fast anomaly gating.

The present study is deliberately a mechanism paper rather than a field-validation paper. A natural next step is joint calibration from greenhouse or field data containing packet traces, battery telemetry, leaf wetness, relative humidity, temperature, and independently measured disease outcomes. Such data would allow statistical estimation of α, replacement of the generic suitability map by a pathogen-specific infection function, and comparison of the proposed fusion rule with integer-order, sliding-window, robust-statistical, and learning-based alternatives. The same architecture can then be extended to heterogeneous crop zones, multiple mobile agents, spatial epidemic states, and energy-harvesting sensor platforms.

Data and computational reproducibility

No external dataset is used in the present numerical study. The experiments are synthetic and are fully specified by Table 1, the attack profiles, the applied-routing specification in Table 5, and the PECE scheme (15)–(16). The applied packet-to-attack mapping is given by (19). The biological stress test is completely defined by (34)–(35), Table 7, and the parameters $r_b = 0.10$, $\gamma_b = 0.06$, $P_0 = 0.15$. The plotting coordinates used in all figures are embedded directly in this `main.tex` source.

Declarations

Funding. *To be completed by the authors before journal submission.*

Competing interests. *To be completed and approved by all authors before journal submission.*

Author contributions. *To be finalized according to the target journal's CRediT requirements.*

Prior dissemination. An abstract version of the study was presented at the 2nd International

Conference on Mathematics and Computers with Applications (MCWA 2026), Istanbul, Turkiye, 21–23 July 2026. The present manuscript develops the full mathematical model, proofs, stability analysis, packet-informed routing study, and the new plant-disease biosurveillance extension.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks: a survey, *Computer Networks* 38(4) (2002), 393–422. doi:10.1016/S1389-1286(01)00302-4.

[2] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, Reputation-based framework for high integrity sensor networks, *ACM Transactions on Sensor Networks* 4(3) (2008), Article 15, 1–37. doi:10.1145/1362542.1362546.

[3] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, Management and applications of trust in wireless sensor networks: A survey, *Journal of Computer and System Sciences* 80(3) (2014), 602–617. doi:10.1016/j.jcss.2013.06.014.

[4] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, Trust management system in wireless sensor networks: design considerations and research challenges, *Transactions on Emerging Telecommunications Technologies* 26 (2015), 107–130. doi:10.1002/ett.2674.

[5] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, Trust-based attack and defense in wireless sensor networks: A survey, *Wireless Communications and Mobile Computing* 2020 (2020), Article ID 2643546. doi:10.1155/2020/2643546.

[6] W. Fang, Z. Shi, L. Shan, F. Li, and X. Wang, Trusted scheme for defending on-off attack based on BETA distribution, *Journal of System Simulation* 27(11) (2015), 2722–2728.

[7] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution, *Science China Information Sciences* 60 (2017), 040305. doi:10.1007/s11432-016-9028-0.

[8] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks, *Digital Communications and Networks* 7(4) (2021), 470–478. doi:10.1016/j.dcan.2021.03.005.

[9] B. S. Venkatesh Prasad and H. R. Roopashree, Energy aware and secure routing for hierarchical cluster through trust evaluation, *Measurement: Sensors* 33 (2024), 101132. doi:10.1016/j.measen.2024.101132.

[10] S. Sharma, M. Yahya, A. Jain, A. I. Alutaibi, A. Baihan, P. Dutta, and A. Abugabah, Evaluation of legitimacy of IoT devices based on an energy-efficient trust management scheme in information-centric networking, *International Journal of Communication Systems* 38(9) (2025), e70085. doi:10.1002/dac.70085.

[11] M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and H. Abdul Gaffar, Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks, *Scientific Reports* 15 (2025), 19724. doi:10.1038/s41598-025-03558-8.

[12] J. Alotaibi, Energy-efficient trust management for secure IoT devices in information-centric wireless sensor networks, *Peer-to-Peer Networking and Applications* 19 (2026), Article 43. doi:10.1007/s12083-025-02194-3.

[13] M. Dong, K. Ota, L. T. Yang, S. Chang, H. Zhu, and Z. Zhou, Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks, *Computer Networks* 74 (2014), 58–70. doi:10.1016/j.comnet.2014.06.019.

[14] M. El Fissaoui, A. Beni-Hssane, and M. Saadi, Mobile Agent Protocol based energy aware data aggregation for wireless sensor networks, *Procedia Computer Science* 113 (2017), 25–32. doi:10.1016/j.procs.2017.08.279.

[15] S. Karthik, M. Karthick, N. Karthikeyan, and S. Kannan, A multi-Mobile Agent and optimal itinerary planning-based data aggregation in wireless sensor networks, *Computer Communications* 184 (2022), 24–35. doi:10.1016/j.comcom.2021.11.019.

[16] Aqeel-ur-Rehman, A. Z. Abbasi, N. Islam, and Z. A. Shaikh, A review of wireless sensors and networks' applications in agriculture, *Computer Standards & Interfaces* 36(2) (2014), 263–270. doi:10.1016/j.csi.2011.03.004.

[17] T. Ojha, S. Misra, and N. S. Raghuwanshi, Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges, *Computers and Electronics in Agriculture* 118 (2015), 66–84. doi:10.1016/j.compag.2015.08.011.

[18] T. Rowlandson, M. Gleason, P. Sentelhas, T. Gillespie, C. Thomas, and B. Hornbuckle, Reconsidering leaf wetness duration determination for plant disease management, *Plant Disease* 99(3) (2015), 310–319. doi:10.1094/PDIS-05-14-0529-FE.

[19] K. S. Patle, R. Saini, A. Kumar, S. G. Surya, V. S. Palaparthy, and K. N. Salama, IoT enabled, leaf wetness sensor on the flexible substrates for in-situ plant disease management, *IEEE Sensors Journal* 21(17) (2021), 19481–19491. doi:10.1109/JSEN.2021.3089722.

[20] L. V. Madden, G. Hughes, and F. van den Bosch, *The Study of Plant Disease Epidemics*, American Phytopathological Society, St. Paul, MN, 2007.

[21] M. Caputo, Linear models of dissipation whose Q is almost frequency independent–II, *Geophysical Journal of the Royal Astronomical Society* 13 (1967), 529–539. doi:10.1111/j.1365-246X.1967.tb02303.x.

[22] I. Podlubny, *Fractional Differential Equations*, Mathematics in Science and Engineering, Vol. 198, Academic Press, San Diego, 1999.

[23] A. A. Kilbas, H. M. Srivastava, and J. J. Trujillo, *Theory and Applications of Fractional Differential Equations*, North-Holland Mathematics Studies, Vol. 204, Elsevier, Amsterdam, 2006.

[24] K. Diethelm, *The Analysis of Fractional Differential Equations*, Lecture Notes in Mathematics, Vol. 2004, Springer, Berlin, 2010.

[25] K. Diethelm, N. J. Ford, and A. D. Freed, A predictor-corrector approach for the numerical solution of fractional differential equations, *Nonlinear Dynamics* 29 (2002), 3–22. doi:10.1023/A:1016592219341.

[26] K. Diethelm, N. J. Ford, and A. D. Freed, Detailed error analysis for a fractional Adams method, *Numerical Algorithms* 36(1) (2004), 31–52. doi:10.1023/B:NUMA.0000027736.85078.be.

[27] D. Matignon, Stability results for fractional differential equations with applications to control processing, in *Computational Engineering in Systems Applications*, Vol. 2, IMACS, Lille, France, 1996, pp. 963–968.

[28] Y. Li, Y. Chen, and I. Podlubny, Mittag–Leffler stability of fractional order nonlinear dynamic systems, *Automatica* 45(8) (2009), 1965–1969. doi:10.1016/j.automatica.2009.04.003.