Formal Modeling of Security Dynamics in Sensor Networks Using Fuzzy Inference Systems

Alexander Alexandrov[1][0000-0002-8787-9235]

[1] Instiute of Robotics – Bulgarian Academy of Sciences, Sofia 1113, Bulgaria
akalexandrov@ir.bas.bg

Abstract. The rapid expansion of distributed sensing infrastructures has introduced complex challenges in maintaining the integrity, confidentiality, and availability of sensor data. Traditional cryptographic or rule-based approaches to securing sensor networks often fail to capture the dynamic uncertainty and partial information inherent in such systems. This paper presents a formal model of security dynamics in sensor networks using a Fuzzy Inference System (FIS). The proposed model quantifies and evaluates network security levels through fuzzy variables representing node trustworthiness, data integrity, intrusion likelihood, and energy state. A mathematical framework for fuzzy membership functions and inference rules is established, leading to a formal representation of the system's global security state as a dynamic equilibrium. Analytical evaluation demonstrates that fuzzy-based reasoning provides adaptive, interpretable, and computationally efficient security estimation. The proposed model advances theoretical foundations for self-managing, context-aware sensor networks..

Keywords: Fuzzy inference systems, WSN, information security.

1 Introduction

Wireless sensor networks (WSNs) have emerged as a fundamental component of modern cyber-physical systems, enabling real-time monitoring and control across domains such as environmental sensing, healthcare, industrial automation, and defense. However, the distributed and resource-constrained nature of sensor nodes renders them particularly vulnerable to security threats, including eavesdropping, node compromise, false data injection, and denial-of-service attacks.

Conventional security mechanisms, primarily based on cryptography or deterministic rule-checking, require predefined parameters and exhaustive computation, both of which are unsuited to energy-limited and dynamically changing environments. Furthermore, these methods cannot efficiently represent uncertainty, for instance, when evaluating the partial trustworthiness of a node or the probabilistic nature of an intrusion event.

To address this limitation, Fuzzy Logic offers a promising paradigm. It allows reasoning with imprecise, uncertain, and linguistic information, enabling systems to adapt their security policies dynamically. By formalizing network security as a fuzzy dy-

Research Paper
DOI: https://doi.org/10.46793/BISEC25.076A
Part of ISBN: 978-86-89755-40-4

© 2026 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

namic system, it becomes possible to capture nuanced relationships among parameters such as trust, residual energy, data accuracy, and threat likelihood.
This paper develops a formal fuzzy inference model that represents the security dynamics of sensor networks as a composite function of interacting fuzzy variables. The model is analytically examined under varying security states to demonstrate its capacity for self-adaptive reasoning.

2 Related Work

Early research in WSN security focused primarily on cryptographic key management and lightweight encryption protocols [1][2][3]. While these techniques ensure confidentiality, they fail to adapt to fluctuating network conditions or energy constraints. Later, probabilistic models and game-theoretic frameworks were introduced to represent attacker–defender interactions [4][5]. However, such models often require precise probability distributions, which are rarely available in real deployments.
Fuzzy logic-based security approaches have been explored as an alternative. For example, Butun et al. [6] proposed a fuzzy-based intrusion detection system (IDS) for WSNs, focusing on detecting abnormal packet delivery ratios. Similarly, Shiming, Ping and Xuehong [7] utilized fuzzy trust models to compute node reliability. These works demonstrate the feasibility of fuzzy reasoning for adaptive security assessment but often lack formal mathematical grounding or dynamic modeling.
In contrast, this paper contributes a formally defined fuzzy inference framework where system variables, membership functions, and rule structures are explicitly expressed as mathematical entities. The goal is not merely to design an algorithm but to define the underlying formalism that governs security evolution over time in fuzzy state space.

3 Formal Modeling of Security Dynamics

3.1 System Overview

Let the sensor network be represented as a connected graph

$$= (\mathrm{N}, \mathrm{E}) \qquad (1)$$

where $N = \{n_1, n_2, \dots, n_k\}$denotes the set of sensor nodes and $E \subseteq N \times N$denotes communication links.

Each node n_i has associated attributes:

- T_i: trust level
- D_i: data integrity confidence
- E_i: residual energy
- L_i: local intrusion likelihood

The global security state $S(t)$of the network at time $t$is expressed as:

$$S(t) = F\big(T_i(t), D_i(t), E_i(t), L_i(t)\big) \qquad \forall i \in N \qquad (2)$$

where $F(\cdot)$is a fuzzy inference function mapping multidimensional fuzzy inputs to a continuous security index $s_i \in [0,1]$.

3.2 Fuzzy Security Index (FSI)

We define a Fuzzy Security Index (FSI) as:

$$FSI = \frac{1}{|N|}\sum_{i=1}^{|N|} s_i \qquad (3)$$

where $s_i$represents the defuzzified output of node n_i's fuzzy security evaluation. The overall network is considered as

- secure if $FSI > 0.7$,
- unstable if $0.4 < FSI \leq 0.7$, and
- compromised if $FSI \leq 0.4$.

4 Fuzzy Inference System Design

The FIS evaluates security parameters using linguistic variables. Each fuzzy variable is represented by a membership function (MF), normalized to [0,1] on Table 1

4.1 Input Variables

Table 1

Variable	Linguistic Terms	Domain	Purpose
Trust (T_i)	{Low, Medium, High}	[0,1]	Measures reliability of node n_i
Data Integrity (D_i)	{Poor, Fair, Good}	[0,1]	Reflects correctness of transmitted data
Energy (E_i)	{Low, Normal, High}	[0,1]	Indicates node's available power
Intrusion Likelihood (L_i)	{Low, Moderate, High}	[0,1]	Probability of compromise

4.2 Membership Function Definitions

Each linguistic term is represented as a triangular or trapezoidal function. For example, **Trust (T)** is defined as:

$$\mu_{Low}(T) = \begin{cases} 1 - 3T, & 0 \le T \le 0.33 \\ 0, T > 0.33 \end{cases} \quad (4)$$

$$\mu_{Medium}(T) = \begin{cases} 3T, 0 \le T \le 0.33, \\ 1 - 3(T - 0.33), 0.33 < T \le 0.66 \\ 0, T > 0.66 \end{cases} \quad (5)$$

$$\mu_{High}(T) = \begin{cases} 3(T - 0.66), 0.66 \le T \le 1.0 \\ 1, T > 1.0 \end{cases} \quad (6)$$

Analogously, other variables follow:

Data Integrity (D):

$$\mu_{Poor}(D) = \max(0, 1 - 3D)$$
$$\mu_{Fair}(D) = \text{triangular}(0.33, 0.5, 0.66)$$
$$\mu_{Good}(D) = \max(0, 3(D - 0.66))$$

Energy (E):

$$\mu_{Low}(E) = \text{trapezoidal}(0,0,0.2,0.4)$$
$$\mu_{Normal}(E) = \text{triangular}(0.3,0.5,0.7)$$
$$\mu_{High}(E) = \text{trapezoidal}(0.6,0.8,1,1)$$

Intrusion Likelihood (L):

$$\mu_{Low}(L) = e^{-(L/0.3)^2}$$
$$\mu_{Moderate}(L) = e^{-((L-0.5)/0.2)^2}$$
$$\mu_{High}(L) = e^{-((L-1)/0.3)^2}$$

4.3 Output Variable

The output fuzzy variable **Security Level (S)** has linguistic terms: {Compromised, Unstable, Secure}.

It is defined over [0,1] with triangular MFs:

$$\mu_{Comp}(S) = \text{triangular}(0,0.2,0.4)$$
$$\mu_{Unstab}(S) = \text{triangular}(0.3,0.5,0.7)$$
$$\mu_{Secure}(S) = \text{triangular}(0.6,0.8,1)$$

5 Fuzzy Rule Base and Inference Mechanism

The fuzzy rule base encodes expert knowledge in the form of IF–THEN statements.

Each rule $R_j$has the form:

$$R_j\text{:IF } T_i \text{ is } A_1^j \text{ AND } D_i \text{ is } A_2^j \text{ AND } E_i \text{ is } A_3^j \text{ AND } L_i \text{ is } A_4^j \text{ THEN } S_i \text{ is } B^j$$

where $A_k^j \in \{Low, Medium, High\}$and $B^j \in \{Compromised, Unstable, Secure\}$.

5.1 Rule Examples

1. **R1:** IF Trust is *Low* OR Intrusion Likelihood is *High* THEN Security is *Compromised*.
2. **R2:** IF Trust is *Medium* AND Energy is *Normal* AND Data Integrity is *Fair* THEN Security is *Unstable*.
3. **R3:** IF Trust is *High* AND Data Integrity is *Good* AND Intrusion Likelihood is *Low* THEN Security is *Secure*.
4. **R4:** IF Energy is *Low* THEN Security is *Unstable* (energy exhaustion risk).
5. **R5:** IF Trust is High AND Intrusion Likelihood is *Moderate* THEN Security is *Unstable*.

5.2 Inference and Defuzzification

The fuzzy inference process uses **Mamdani min–max composition**:

$$\mu_{S_i}(y) = \max_j(\min[\mu_{A_1^j}(T_i), \mu_{A_2^j}(D_i), \mu_{A_3^j}(E_i), \mu_{A_4^j}(L_i), \mu_{B^j}(y)]) \quad (7)$$

Defuzzification uses the **centroid method**:

$$s_i = \frac{\int_0^1 y\, \mu_{S_i}(y)\, dy}{\int_0^1 \mu_{S_i}(y)\, dy} \quad (8)$$

The resulting crisp value $s_i \in [0,1]$ quantifies node n_i's instantaneous security state.

6 Analytical Evaluation of Model Behavior

6.1 Security Sensitivity to Trust Variations

Let all other parameters be constant at mid-range values (e.g., $D_i = 0.5, E_i = 0.6, L_i = 0.3$).
By varying $T_i \in [0,1]$, the output $s_i$exhibits a **monotonic increasing behavior** approximated by:

$$s_i(T_i) \approx 0.3 + 0.6T_i - 0.1T_i^2 \quad (9)$$

This indicates diminishing marginal gain in perceived security as trust approaches its upper bound.

6.2 Intrusion Impact on Security State

When $L_i$increases from 0.2 to 0.8 (representing growing intrusion risk), the fuzzy inference compresses the *Secure* output membership and amplifies Compromised membership. Analytical derivative:

$$\frac{ds_i}{dL_i} \approx -0.5e^{-(L_i-0.5)^2/0.1} \quad (10)$$

reveals that the system is most sensitive around $L_i = 0.5$, i.e., the moderate intrusion region where uncertainty is highest.

6.3 Energy Security Coupling

Nodes with decreasing energy are modeled to degrade trust dynamically as:

$$T_i(t+1) = \alpha T_i(t) + (1-\alpha)(1 - E_i(t)) \qquad (11)$$

where $\alpha \in [0,1]$defines temporal dependency. This feedback introduces a dynamic equilibrium between energy depletion and trust retention. Analytical stability condition:

$$| 1 - \alpha | < 1 \Rightarrow 0 < \alpha < 2 \qquad (12)$$

ensures convergence of trust trajectory.

6.4 Global Security Equilibrium

The system evolves according to discrete-time dynamics:

$$S(t+1) = \beta S(t) + (1-\beta)\bar{s}(t) \qquad (13)$$

where $\bar{s}(t)$is the mean of node-level fuzzy security outputs and βcontrols inertia. Stability analysis using eigenvalue condition $| \beta | < 1$ensures that network security converges to a steady-state fuzzy equilibrium.

7 Theoretical Simulation

The theoretical simulation was carried out in MATLAB R2023b using the Fuzzy Logic Toolbox and the Symbolic Math Toolbox.

The objective was to evaluate the behavior of the proposed fuzzy inference system (FIS) under controlled perturbations of key security parameters—trust (T), data integ-

rity (D), energy (E), and intrusion likelihood (L)—and to observe the evolution of the Fuzzy Security Index (FSI) over time. The fuzzy system was implemented using a Mamdani-type inference engine with four inputs and one output.

Symbolic evaluation allowed all computations to be expressed as continuous functions of the normalized input variables, enabling analytical differentiation and visualization without numerical discretization errors.

7.1 Scenario 1: Node Trust Degradation

Initial trust values are set high ($T_i = 0.8$), but one compromised node exhibits $T_c = 0.2$.
FIS inference yields $s_c = 0.35$, while non-compromised nodes remain $s_i \approx 0.78$. Global FSI drops from 0.78 to 0.73, showing 6.4% degradation from a single node compromise, illustrating model sensitivity to localized faults.

7.2 Scenario 2: Energy Exhaustion Phase

When average energy $E_i$declines linearly from 0.9 to 0.4, corresponding FSI curve follows:

$$FSI(E) = 0.2 + 0.7E \qquad (14)$$

until reaching instability threshold at $E = 0.43$(FSI≈0.50). Below this, fuzzy reasoning flags "Unstable" network status.

7.3 Scenario 3: Coordinated Intrusion

Increasing $L_i$for 30% of nodes to 0.7 results in a nonlinear collapse:

$$FSI = 0.85 - 0.9p^2, \quad \frac{d^2FSI}{dp^2} = -1.8 < 0 \ (15)$$

where pis fraction of high-risk nodes.

This convex degradation indicates super linear collapse of network security as attack intensify.

8 Discussion

The model demonstrates several analytical properties:

1. **Continuity:** The FIS ensures smooth transitions between states, mitigating abrupt security state changes typical of crisp systems.
2. **Context Awareness:** Multi-variable reasoning allows differentiation between diverse attack scenarios.
3. **Scalability:** Each node's computation is $O(r)$, with $r$being rule count, suitable for constrained nodes.
4. **Formal Interpretability:** Explicit equations (14–19) allow symbolic sensitivity and stability analysis.
5. **Analytical Robustness:** The equilibrium model (17) guarantees formal convergence, supporting mathematical reasoning about network-wide security stability.

Limitations include static membership functions and lack of temporal learning. Adaptive or neuro-fuzzy mechanisms could improve responsiveness to evolving threats.

9 Conclusion

This paper presented a **formal fuzzy inference framework** for modeling **security dynamics** in sensor networks. Explicit mathematical representations of membership functions, inference rules, and dynamic coupling were derived. Analytical simulations demonstrated monotonicity, convergence, and super linear degradation properties under trust, energy, and intrusion variations.

The study provides a formal basis for **self-adaptive, explainable security reasoning** in distributed, uncertain environments. Future extensions may incorporate adaptive learning of fuzzy parameters and integration with stochastic game models for formal verification of dynamic cyber defense strategies.

References

1. Jain, Khushboo. (2025). Exploring Cryptographic Key Management Schemes for Enhanced Security in WSNs. Journal of Information Assurance and Security. 20. 18-37. 10.2478/ias-2025-0002.
2. Sarkar, Sayani & Shafaei, Sima & Jones, Trishtanya & Totaro, Michael. (2025). Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. Drones. 9. 10.3390/drones9080583.
3. Țălu, Mircea. (2025). DNA-Based Cryptography for Internet of Things Security: Concepts, Methods, Applications, and Emerging Trends. Buletin Ilmiah Sarjana Teknik Elektro. 68-94. 10.12928/biste.v7i2.12942.

4. Pandey, Rashmikiran & Pandey, Mrinal & Nazarov, Alexey. (2023). Modelling the Dynamics of Information Warfare: An Attacker-Defender Scenario Using Lotka-Volterra Equations. 10.21203/rs.3.rs-3148628/v1.
5. Joseph, Michael. (2010). Modeling attacker-defender interactions in information networks. 10.2172/1008137.
6. Butun, Ismail & Morgera, Salvatore & Sankar, Ravi. (2013). A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials. PP. 266 - 282. 10.1109/SURV.2013.050113.00191.
7. F. Shiming, Z. Ping and S. Xuehong, "A fuzzy trust management mechanism with dynamic behavior monitoring for wireless sensor networks," in *China Communications*, vol. 21, no. 5, pp. 177-189, May 2024, doi: 10.23919/JCC.fa.2022-0616.202405. keywords: {Wireless sensor networks;Monitoring;Cloud computing;Security;Wireless communication;Distributed databases;Communication system security;behavior monitoring;cloud;fuzzy;trust;wireless sensor networks},