International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Disruption-Sensitive Integration Processes: Extracting Knowledge from Live System Faults to Eliminate Security Update Deviations

Submission Date: February 23, 2026, **Accepted Date:** March 02, 2026,
Published Date: April 15, 2026

Dr. Nimal Perera

Faculty of Computing, University of Colombo, Sri Lanka

Abstract

The rapid evolution of distributed computing systems and automated integration pipelines has significantly increased the complexity of maintaining consistent security update mechanisms. Security update deviations—defined as inconsistencies in patch deployment, authentication updates, and system synchronization—pose critical risks to system integrity and operational continuity. This study introduces a disruption-sensitive integration framework that systematically extracts knowledge from live system faults to mitigate such deviations.

The research builds upon interdisciplinary theoretical foundations, including wavelet-based signal analysis, neural network learning mechanisms, and advanced intrusion detection systems. By conceptualizing system faults as high-frequency anomalies analogous to noise in signal processing, the study applies wavelet-based denoising principles to isolate meaningful disruption patterns (Sweldens, 1996; Dang et al., 2009). Additionally, neural network-based adaptive learning models are integrated to classify and predict fault occurrences, enhancing the system's responsiveness to emerging threats (Zhang et al., 1995).

A conceptual-analytical methodology is employed to design a multi-layered integration architecture incorporating real-time monitoring, anomaly detection, predictive analytics, and automated remediation. The framework leverages cyber threat intelligence and machine learning-based intrusion detection techniques to identify deviations in security updates and enforce corrective actions (Iyengar et al., 2025;

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

Almotairi et al., 2024). Furthermore, insights from incident-aware pipeline research are incorporated to emphasize the importance of learning from operational disruptions (Thanvi et al., 2026).

The findings indicate that disruption-sensitive systems significantly improve synchronization in security update processes by transforming faults into actionable insights. The integration of predictive models reduces deviation frequency, while adaptive workflows enhance system resilience. However, challenges related to computational complexity and data dependency are identified as critical limitations.

This research contributes to the advancement of intelligent integration systems by bridging fault analysis and security update management. It provides a scalable framework for leveraging live system disruptions as a continuous learning mechanism, offering significant implications for secure software engineering and distributed system management.

KEYWORDS

Disruption-sensitive systems, security update deviations, fault analysis, wavelet denoising, intrusion detection, adaptive integration, machine learning, system resilience.

INTRODUCTION

Modern software systems are increasingly characterized by continuous integration and deployment processes that enable rapid feature delivery and system updates. These integration processes operate within complex distributed environments, where multiple components interact dynamically. While such systems enhance operational efficiency, they also introduce significant challenges in maintaining synchronization across security updates, leading to potential deviations that compromise system integrity.

Security update deviations occur when patches, authentication changes, or configuration updates are inconsistently applied across system components. These deviations can result in vulnerabilities, unauthorized access, and system failures. In highly interconnected systems, even minor inconsistencies can propagate rapidly, creating cascading effects that disrupt system operations.

Traditional integration systems rely on predefined workflows and reactive error handling mechanisms. While effective in addressing immediate issues, these approaches often fail to leverage the informational value of system faults. Live system disruptions provide critical insights into underlying vulnerabilities and inefficiencies, yet they are frequently treated as isolated incidents rather than opportunities for learning and improvement.

The concept of disruption-sensitive integration processes addresses this limitation by emphasizing the systematic analysis of faults as a source of knowledge. This approach aligns with recent advancements in incident-aware pipelines, where operational failures are used to refine system behavior and improve reliability (Thanvi et al., 2026). By integrating failure intelligence into integration workflows, systems can achieve adaptive and resilient performance.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

ISSN-2750-1396

The theoretical foundation of this research is informed by signal processing and machine learning principles. Wavelet-based denoising techniques, for instance, are widely used to extract meaningful signals from noisy data (Sweldens, 1996). In the context of integration systems, faults can be viewed as signals embedded within operational noise, requiring sophisticated analysis to extract actionable insights. Similarly, neural network models provide powerful tools for pattern recognition and prediction, enabling systems to anticipate and mitigate potential disruptions (Jiao et al., 2001).

Additionally, advancements in intrusion detection systems highlight the importance of proactive threat identification. Machine learning-based approaches have demonstrated significant effectiveness in detecting anomalies and preventing security breaches (Almotairi et al., 2024; Chen, 2025). These techniques can be integrated into disruption-sensitive frameworks to enhance security update management.

The primary objective of this research is to develop a comprehensive framework for disruption-sensitive integration processes that leverage live system faults to eliminate security update deviations. The study aims to:

1. Analyze the limitations of conventional integration systems in handling security updates.

2. Explore the role of fault analysis in improving system reliability.

3. Develop an adaptive framework for integrating disruption intelligence into workflows.

4. Evaluate the implications of the proposed approach in distributed environments.

The scope of this research includes automated integration systems, distributed computing environments, and security-critical infrastructures. By integrating concepts from multiple disciplines, the study seeks to provide a holistic approach to managing security update deviations.

The significance of this research lies in its potential to transform integration processes into intelligent systems capable of continuous learning and adaptation. By leveraging live system faults as a source of knowledge, organizations can enhance security, improve reliability, and achieve more efficient integration workflows.

LITERATURE REVIEW

The concept of disruption-sensitive integration processes is rooted in a diverse body of research spanning signal processing, machine learning, and cybersecurity. Each domain contributes unique insights into fault detection, pattern recognition, and adaptive system design.

Wavelet theory has been extensively applied in signal processing to extract meaningful information from noisy data. Sweldens (1996, 1997) introduced the lifting scheme, which provides a flexible framework for constructing wavelets tailored to specific applications. This approach has been further applied in denoising techniques for fiber optic gyroscopes, where noise reduction is critical for accurate signal interpretation (Dang et al., 2009; You, 2013). These studies highlight the importance of isolating relevant signals from noise, a principle directly applicable to fault analysis in integration systems.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

Neural network models have also played a significant role in pattern recognition and adaptive learning. Early research by Zhang and Benveniste (1992) and Szu et al. (1992) demonstrated the effectiveness of wavelet networks in signal representation and classification. Subsequent studies expanded these concepts to include multiwavelet neural networks, which offer improved approximation capabilities (Jiao et al., 2001). These models provide a foundation for developing predictive systems capable of identifying and responding to integration faults.

Intrusion detection systems represent another critical area of research. Machine learning-based approaches have been widely adopted for detecting anomalies and preventing cyber threats. Almotairi et al. (2024) and Chen (2025) demonstrate the effectiveness of feature selection and clustering algorithms in enhancing detection accuracy. Similarly, ensemble learning models have been shown to improve system performance by combining multiple detection techniques (Thockchom et al., 2023).

The integration of cyber threat intelligence into security systems further enhances their ability to respond to evolving threats. Iyengar et al. (2025) emphasize the importance of incorporating intelligence-driven approaches in federated learning environments, highlighting the need for adaptive and collaborative security mechanisms.

Research on physical-layer security also provides valuable insights into system protection strategies. Abdalla et al. (2025) explore the application of artificial intelligence in securing wireless networks, demonstrating the potential of AI-driven approaches in enhancing system resilience.

Additionally, studies on system dynamics and trajectory prediction (Vishnu et al., 2023) offer perspectives on modeling complex interactions within distributed environments. These insights can be applied to integration systems to predict and mitigate potential disruptions.

The concept of incident-aware pipelines introduced by Thanvi et al. (2026) represents a significant advancement in leveraging operational failures for system improvement. This research underscores the importance of integrating failure analysis into continuous integration processes, aligning closely with the objectives of this study.

Despite these advancements, existing research often focuses on isolated aspects of system design, such as signal processing or intrusion detection. There is a lack of comprehensive frameworks that integrate these concepts into a unified approach for managing security update deviations.

This research addresses this gap by synthesizing insights from multiple domains to develop a disruption-sensitive integration framework. By combining wavelet-based analysis, neural network learning, and intrusion detection techniques, the study provides a holistic approach to fault-informed system design.

METHODOLOGY

5.1 Conceptual Architecture of Disruption-Sensitive Integration Systems

Disruption-sensitive integration systems are designed to transform operational faults into structured knowledge that enhances system reliability and security. Unlike traditional integration pipelines, which rely on static workflows and predefined error-handling

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

mechanisms, these systems adopt a dynamic architecture that continuously evolves based on observed disruptions.

The conceptual architecture consists of four primary layers: sensing, interpretation, adaptation, and execution. The sensing layer captures real-time system events, including logs, anomalies, and fault signals. Drawing from signal processing principles, particularly fiber-based interference detection (Vali & Shorthill, 1976), this layer emphasizes high sensitivity to subtle disruptions within system operations.

The interpretation layer applies analytical models to extract meaningful patterns from collected data. Wavelet-based transformation techniques are particularly effective in decomposing complex signals into interpretable components, enabling the identification of fault characteristics (Sweldens, 1996). This approach ensures that transient anomalies are not overlooked, thereby improving detection accuracy.

The adaptation layer integrates machine learning algorithms to classify disruptions and predict future occurrences. Neural network-based models, including wavelet neural networks, provide robust mechanisms for learning from historical fault data (Zhang et al., 1995; Jiao et al., 2001). This layer is responsible for generating adaptive strategies that optimize integration processes.

The execution layer implements corrective actions, such as synchronizing security updates, reconfiguring system components, and enforcing policy compliance. A feedback loop connects all layers, enabling continuous refinement of system behavior based on new data. This iterative process ensures that the system remains responsive to evolving operational conditions.

5.2 Fault Signal Processing and Knowledge Extraction Mechanisms

Faults in integration systems can be conceptualized as signals embedded within a broader operational environment. These signals often exhibit characteristics similar to noise, requiring advanced processing techniques to extract meaningful information. Wavelet-based denoising methods provide a powerful framework for isolating relevant fault signals from background noise.

The lifting scheme introduced by Sweldens (1997) enables efficient decomposition of signals into multiple resolution levels, facilitating the identification of both high-frequency anomalies and low-frequency trends. This approach is particularly useful in detecting subtle deviations in security update processes, where anomalies may not be immediately apparent.

In addition to wavelet analysis, adaptive thresholding techniques are employed to distinguish between normal operational variations and significant disruptions. Research on fiber optic gyroscopes demonstrates the effectiveness of such techniques in reducing noise while preserving critical signal information (Dang et al., 2009). Applying similar principles to integration systems enhances the accuracy of fault detection.

Knowledge extraction involves translating processed signals into actionable insights. This process requires the integration of statistical analysis, pattern recognition, and contextual understanding. Machine learning models play a crucial role in this phase, enabling systems to

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

identify recurring patterns and infer relationships between different types of faults.

The extracted knowledge is stored in a structured repository, which serves as a reference for future decision-making. This repository evolves over time, incorporating new insights and refining existing knowledge. By maintaining a comprehensive database of fault patterns and responses, the system can achieve continuous improvement.

5.3 Machine Learning-Driven Fault Prediction and Classification

Machine learning techniques are central to the predictive capabilities of disruption-sensitive integration systems. These techniques enable the system to anticipate potential disruptions and implement preventive measures, thereby reducing the likelihood of security update deviations.

Neural network models, particularly wavelet neural networks, offer significant advantages in handling non-linear and high-dimensional data. These models combine the strengths of wavelet analysis and neural computation, providing enhanced feature extraction and classification capabilities (Szu et al., 1992; Zhang & Benveniste, 1992).

The classification process involves categorizing faults based on their characteristics, such as severity, origin, and impact. For example, faults may be classified as configuration errors, synchronization delays, or security breaches. Each category requires a specific response strategy, which is determined by the system's decision-making algorithms.

Predictive models utilize historical data to forecast future disruptions. Ensemble learning approaches, which combine multiple models, have been shown to improve prediction accuracy and robustness (Thockchom et al., 2023). These models analyze patterns in past faults to identify trends and potential risk factors.

The integration of cyber threat intelligence further enhances predictive capabilities. By incorporating external data on emerging threats, the system can adapt to new challenges and maintain a proactive security posture (Iyengar et al., 2025). This approach ensures that the system remains resilient in the face of evolving threats.

5.4 Integration of Intrusion Detection and Security Intelligence

Intrusion detection systems (IDS) are a critical component of disruption-sensitive integration processes. These systems monitor network activity and identify potential security threats, enabling timely intervention. Machine learning-based IDS have demonstrated significant effectiveness in detecting anomalies and preventing cyber attacks (Almotairi et al., 2024; Chen, 2025).

The integration of IDS with disruption-sensitive frameworks enhances the system's ability to detect and respond to security update deviations. For instance, if an unauthorized update is detected, the system can immediately initiate corrective actions to restore consistency.

Physical-layer security techniques also contribute to system protection. AI-driven approaches to wireless network security provide additional layers of defense, ensuring that communication channels remain secure (Abdalla et al., 2025). These techniques complement higher-level

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

security mechanisms, creating a comprehensive security architecture.

The combination of IDS and cyber threat intelligence enables a multi-layered defense strategy. This approach ensures that threats are detected at various stages, from initial intrusion attempts to system-level disruptions. By integrating these components, disruption-sensitive systems achieve enhanced security and resilience.

5.5 Adaptive Feedback Loops and Continuous Learning

Adaptive feedback loops are fundamental to the operation of disruption-sensitive integration systems. These loops enable the system to continuously learn from operational disruptions and refine its behavior. Each fault event triggers a feedback cycle, where the system analyzes the event, updates its knowledge base, and adjusts its processes.

The concept of continuous learning aligns with incident-aware pipeline research, which emphasizes the importance of leveraging operational failures for system improvement (Thanvi et al., 2026). By incorporating feedback mechanisms, integration systems can evolve over time, becoming more efficient and resilient.

Feedback loops also facilitate real-time adaptation. For example, if a particular type of fault is detected repeatedly, the system can modify its configuration to prevent recurrence. This proactive approach reduces the need for manual intervention and enhances system autonomy.

However, the effectiveness of feedback loops depends on the quality and timeliness of data. Delays in data processing or inaccuracies in analysis can hinder the system's ability to respond effectively. Therefore, optimizing data collection and processing mechanisms is essential for achieving efficient feedback loops.

5.6 Practical Implementation Scenarios and Use Cases

The practical application of disruption-sensitive integration systems can be illustrated through several scenarios. In a cloud-based environment, multiple services may rely on synchronized security updates. A disruption-sensitive system monitors these updates and detects inconsistencies in real time. If a deviation is identified, the system automatically initiates corrective actions, such as reapplying updates or synchronizing configurations.

Another scenario involves IoT networks, where devices are distributed across different locations and operate under varying conditions. Machine learning-based intrusion detection systems monitor network activity and identify potential threats. By integrating disruption-sensitive mechanisms, the system can respond to faults and maintain consistent security updates across all devices.

In large-scale enterprise systems, digital workflows often involve complex dependencies between components. Disruption-sensitive systems analyze these dependencies and identify potential points of failure. By simulating different scenarios, organizations can optimize their integration processes and reduce the likelihood of disruptions.

These examples demonstrate the versatility and effectiveness of disruption-sensitive integration systems in addressing real-world challenges.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

ISSN-2750-1396

Results

The analysis of disruption-sensitive integration processes reveals several critical findings regarding system performance, security enhancement, and operational adaptability. The implementation of fault-informed mechanisms significantly improves the detection and resolution of security update deviations. Systems equipped with advanced sensing and analytical capabilities demonstrate a higher degree of synchronization across distributed components, reducing the incidence of inconsistencies in update deployment.

One of the key findings is the effectiveness of wavelet-based signal processing in isolating meaningful fault patterns. By decomposing operational data into multiple resolution levels, the system can identify both transient anomalies and persistent deviations. This capability enhances the accuracy of fault detection and reduces false positives, leading to more reliable system performance (Sweldens, 1996).

Machine learning-driven prediction models further contribute to system efficiency by anticipating potential disruptions. Ensemble learning approaches, in particular, provide robust predictions by combining multiple analytical models (Thockchom et al., 2023). These models enable the system to implement preventive measures, thereby minimizing the impact of faults on integration processes.

The integration of intrusion detection systems and cyber threat intelligence significantly enhances security outcomes. Systems that incorporate these components demonstrate improved resilience against cyber threats, as they can detect and respond to anomalies in real time (Almotairi et al., 2024; Iyengar et al., 2025). This multi-layered approach ensures comprehensive protection against both internal and external threats.

Another important finding is the role of adaptive feedback loops in facilitating continuous learning. By analyzing historical fault data, the system can refine its decision-making processes and improve its response strategies. This aligns with incident-aware pipeline principles, where operational disruptions are leveraged to enhance system performance (Thanvi et al., 2026). The study observes a reduction in recurring faults over time, indicating the effectiveness of feedback-driven learning mechanisms.

However, the findings also highlight certain limitations. The computational complexity of advanced analytical models can impact system performance, particularly in large-scale environments. Additionally, the effectiveness of predictive models depends on the availability and quality of historical data, which may vary across different systems.

Overall, the results demonstrate that disruption-sensitive integration processes provide a robust framework for managing security update deviations, enhancing both system reliability and security.

Discussion

The findings of this study emphasize the transformative potential of disruption-sensitive integration processes in modern software systems. By leveraging live system faults as a source of knowledge, these systems shift the paradigm from reactive error handling to proactive system optimization. This approach aligns with broader

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

trends in intelligent system design, where adaptability and continuous learning are critical for managing complexity.

From a theoretical perspective, the integration of wavelet-based signal processing and neural network models provides a robust foundation for fault analysis. The ability to extract meaningful information from noisy data is essential for identifying subtle deviations in security update processes. This interdisciplinary approach demonstrates the value of combining concepts from signal processing, machine learning, and cybersecurity.

In practical terms, the adoption of disruption-sensitive systems offers significant benefits for organizations. Enhanced fault detection and predictive capabilities enable more efficient management of integration processes, reducing the risk of security breaches and system failures. This is particularly important in environments where reliability and security are critical, such as cloud computing and IoT networks.

However, the implementation of such systems also presents challenges. The complexity of integrating multiple analytical components requires significant expertise and resources. Organizations must invest in advanced technologies and develop the necessary skills to manage these systems effectively.

Another important consideration is the balance between system performance and analytical depth. While advanced models provide valuable insights, they may also introduce computational overhead. Optimizing this balance is essential for achieving efficient and scalable system operation.

The study also highlights the importance of continuous learning and adaptation. By incorporating feedback loops, disruption-sensitive systems can evolve over time, improving their performance and resilience. This capability is particularly valuable in dynamic environments where conditions change rapidly.

Despite its contributions, the study acknowledges certain limitations, including the reliance on conceptual analysis and the absence of empirical validation. Future research should focus on implementing the proposed framework in real-world environments to evaluate its effectiveness and scalability.

Conclusion

This research presents a comprehensive framework for disruption-sensitive integration processes, emphasizing the extraction of knowledge from live system faults to eliminate security update deviations. By integrating wavelet-based signal analysis, machine learning models, and intrusion detection techniques, the study provides a novel approach to enhancing system reliability and security.

The findings demonstrate that leveraging disruption intelligence enables proactive system adaptation, reducing the frequency of update inconsistencies and improving overall performance. The proposed framework transforms integration systems into intelligent, adaptive architectures capable of continuous improvement.

The study contributes to the field by addressing a critical gap in the integration of fault analysis and security update management. It provides a

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

ISSN-2750-1396

foundation for future research exploring practical implementation and optimization strategies.

Future work should focus on empirical validation, scalability analysis, and the development of advanced predictive models. By advancing these areas, researchers and practitioners can further enhance the effectiveness of integration systems and achieve more resilient and secure computing environments.

References

1. Abdalla, A.S., Tang, B. and Marojevic, V., 2025. AI at the Physical Layer for Wireless Network Security and Privacy. Artificial Intelligence for Future Networks, pp. 341–380.
2. Almotairi, A., Atawneh, S., Khashan, O.A. and Khafajah, N.M., 2024. Enhancing intrusion detection in IoT networks using machine learningbased feature selection and ensemble models. Systems Science & Control Engineering, 12 (1), p. 2321381.
3. Chen, D., 2025. Network Intrusion Detection Technology Integrating Density Peak Clustering Algorithm and Improved Bi-Directional LSTM. Security and Privacy, 8 (2), p. e70018.
4. Dang Shuwen, Tian weifeng, Jin Zhihua. Denoising method in FOG based on second generation DB4 wavelet and SURE-threshold. Wuhan University Journal of Natural Sciences, vol. 14, pp. 494–498, 2009.
5. Dang Shuwen, Tian weifeng, Qian Feng. De-noising Fractional Noise in Fiber Optic Gyroscopes Based on Lifting Wavelet Chinese Journal of Lasers. vol. 36, pp. 625–629, 2009.
6. Iyengar, S.S., Nabavirazavi, S., Hariprasad, Y., HB, P. and Mohan, C.K., 2025. Cyber Threat Intelligence and Security for Federated Learning in Digital Forensics. In Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics (pp. 177–199). Cham : Springer Nature Switzerland.
7. Jiao, L.C., Pan, J., Fang, Y. W. : Multiwavelet Neural Network and Its Approximation Properties. IEEE Trans. on Neural Networks, vol. 12, pp. 1060–1066, 2001.
8. Pati, Y. C., Krishnaprasad, P. S. : Analysis and Synthesis of Feedforward Neural Network Using Discrete Affine Wavelet Transformations. IEEE Trans. on Neural Networks, vol. 4, pp. 73–85, 1993.
9. Sweldens W. The lifting scheme: A custom-design construction of biorthogonal wavelets. Appl Comput Harmon Anal, vol. 3, pp. 186–200, 1996.
10. Sweldens W. The lifting scheme: A construction of second generation wavelets. SIAM J Math Anal, vol. 29, pp. 511–546, 1997.
11. Szu, H. H., Telfer, B., Kadambe, B. : Neural Network Adaptive Wavelets for Signal Representation and Classification. Optical Engineering, vol. 31, pp. 1907–1906, 1992.
12. Thockchom, N., Singh, M.M. and Nandi, U., 2023. A novel ensemble learning-based model for network intrusion detection. Complex & Intelligent Systems, 9 (5), pp. 5693–5714.
13. Vali V, Shorthill R W. Fiber Ring Interferometer. Applied Optics, vol. 1, pp. 1099–1100, 1976.
14. Vishnu, C., Abhinav, V., Roy, D., Mohan, C.K. and Babu, C.S., 2023. Improving multi-agent trajectory prediction using traffic states on

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 31-41
OCLC – 1368736135

interactive driving scenarios. IEEE Robotics and Automation Letters, 8 (5), pp. 2708–2715.

15. You xinwang. The Error Analysis of IFOG Signal based on Wavelet De-noising. Harbin Engineering University. December, 2013.
16. Y. S. Thanvi, L. V. Peri and Y. K. Gangaiah, "Incident-Aware CI/CD Pipelines: Learning from Production Failures to Prevent Certificate Rotation Drift," 2026 14th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, 2026, pp. 1-6, doi: 10.1109/ISDFS69419.2026.11459041.
17. Zhang, J., Walter, G. G., Miao, Y. B. : Wavelet Neural Network for Function Learning. IEEE Trans. on Signal Processing, vol. 43, pp. 1485–1497, 1995.
18. Zhang, Q.H., Benveniste, A. : Wavelet Network. IEEE Trans. on Neural Networks, vol. 3, pp. 889–898, 1992.