Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Intrusion Detection and Prevention in Wireless Sensor Networks

M. Karthi

Assistant Professor, Department Of Information Technology,

Hindusthan College Of Arts And Science,

Coimbatore, Tamilnadu, India.

Abstract- This Research Introduces An Innovative Approach, The Enhanced Anomaly-Based Intrusion Detection And Prevention (Abid) System, Designed Specifically For Wireless Sensor Networks (Wsns). Leveraging Advanced Machine Learning Techniques, The Proposed Methodology Involves Meticulous Data Collection, Feature Extraction, And Model Training On Normal Behavior. Through Comprehensive Testing And Parameter Tuning, The System Achieves Optimal Performance, Effectively Detecting And Preventing Intrusions. The Validation Process On Diverse Datasets Demonstrates The System's Robust Generalization Capabilities. The Enhanced Abid System Not Only Addresses The Dynamic Nature Of Wsn Environments But Also Provides A Scalable And Adaptable Solution To Enhance The Overall Cybersecurity Of Sensor Networks. This Research Contributes Valuable Insights To The Evolving Landscape Of Intrusion Detection And Prevention In Wsns, Paving The Way For Enhanced Security Measures In The Realm Of The Internet Of Things (Iot).

Keywords: *Wireless Sensor Networks, Anomaly-Based Detection, Intrusion Prevention, Machine Learning, Cybersecurity.*

1. Introduction

Wireless Sensor Networks (Wsns) Have Emerged As A Pivotal Technology, Intertwining Seamlessly With Various Aspects Of It Daily Lives, Industrial Processes, And Critical Infrastructures. These Networks, Composed Of Small, Resource-Constrained Sensor Nodes, Enable The Collection, Processing, And Transmission Of Data Across Diverse Applications, Ranging From Environmental Monitoring To Healthcare And Smart Cities. While The Pervasive Deployment Of Wsns Brings Unprecedented Connectivity And Data-Driven Insights, It Also Introduces A Host Of Security Challenges, Making Intrusion Detection And Prevention Should Be Given Top Priority. The Intrinsic Characteristics Of Wsns, Such As Limited Computational Power, Constrained Memory, And Wireless Communication Vulnerabilities, Render Them Susceptible To A Myriad Of Security Threats.

The Open And Dynamic Nature Of These Networks Exposes Them To Malicious Activities, Including Unauthorized Data Access, Node Compromise, And Communication Disruptions. As The Reliance On Wsns Continues To Grow, The Need For Robust Security Mechanisms Becomes Increasingly Urgent To Ensure The Integrity, Confidentiality, And Availability Of The Data That Was Delivered. To Protect Wsns From Malicious Activity, Intrusion Detection And Prevention Systems Are Essential In This Situation. These Systems Aim To Identify And Mitigate Security Breaches In Real-Time, Safeguarding The Network's Functionality And The Integrity Of The Transmitted Data. The Unique Challenges Posed By The Resource Constraints Of Sensor Nodes Necessitate Innovative Approaches In The Design And Implementation Of Intrusion Detection And Prevention Mechanisms.

This Paper Delves Into The Intricate Landscape Of Intrusion Detection And Prevention In Wireless Sensor Networks, Addressing The Evolving Threats And Vulnerabilities Associated With These Networks. Through A Comprehensive Exploration Of Existing Methodologies, Detection Algorithms, And Prevention Strategies, This Research Aims To Contribute To The Development Of Resilient And Adaptive Security Solutions Tailored For The Distinctive Characteristics Of Wsns. By Understanding And Mitigating Security Risks, It Endeavor To Pave The Way For The Continued Growth And Integration Of Wireless Sensor Networks In Diverse Applications, Ensuring A Secure And Trustworthy Foundation For The Internet Of Things (Iot) Era.

2. Literature Survey

2.1 Intrusion Prevention System (Ips)

S. M. R (2018) Et.Al Proposed Intrusion Detection And Prevention Based On State Context And Hierarchical Trust In Wireless Sensor Networks. Wireless Sensor Networks (Wsns), Designed For Environmental Data Collection, Face Security Threats Due To Their Dispersed Nature And Open Communication. Intrusion Detection Systems (Ids) Can Detect Compromised Cluster Head Selection, Preventing False Communication To The Base Station. Traditional Ids, While Effective In Detection, Incurs Resource Wastage And Time Consumption. To Address This, An Intrusion Prevention System (Ips) Is Proposed. By Analyzing Energy And Neighbor Count Statistics During Cluster Head Selection, The Ips Identifies And Prevents Attacks, Reducing Resource Overhead. Experimental Simulations Demonstrate Enhanced Network Performance, Emphasizing The Significance Of Early Attack Prevention In Wsns.

2.2 Wireless Intrusion Detection Prevention And Attack System (Widpas)

J. Abo Nada (2018) Et.Al Proposed A Proposed Wireless Intrusion Detection Prevention And Attack System. With The Rapid Proliferation Of Wireless Networks, Traditional Security Measures Are Inadequate, Necessitating Innovative Solutions. This Paper Proposes A Wireless Intrusion Detection Prevention And Attack System (Widpas), Focusing On Monitoring, Analyzing, And Defending Against Security Threats. Acknowledging Inherent Weaknesses In Emerging Technologies, The Research Enhances Existing Intrusion Detection Systems By Leveraging Artificial Intelligence And Neural Networks. Widpas Not Only Detects And Identifies Attacks But Also Actively Defends Against Counterfeit Networks, Providing Heightened Security In The Dynamic Wireless Landscape. Emphasizing The Significance Of Ai For Swift And Accurate Decision-Making, The Research Contributes To Advancing Wireless Network Security In The Face Of Evolving Threats.

2.3 Anomalous Intrusion Detection Protocol (Aidp)

Krishnan R (2022) Et.Al Proposed An Intrusion Detection And Prevention Protocol For Internet Of Things Based Wireless Sensor Networks. This Paper Proposes An Anomalous Intrusion Detection Protocol (Aidp) And Intrusion Prevention Protocol (Ipp) For Enhancing Security In Iot Via Wsn. It Establishes Energy-Efficient Clusters, Ensuring Reliability And Security Through A Shamir Secret Sharing Scheme. The Protocol Adapts Trust And Reputation Based On Node Behavior, Utilizing The Tiny Attack And Fault Detection System. Aidp Operates In Learning, Trading, And Updating Stages, Making It Adaptable And Collaborative. Experimental Results In Ns-2 Demonstrate Improved Network Lifetime, Reduced End-To-End Delay, And Packet Delay Ratio. The Protocol's Scalability For Multi-Hop Communication And Mobility Considerations Is Suggested For Future Exploration.

2.4 Intrusion Detection (Id)

Prabakaran K (2020) Et.Al Proposed An Evaluation Of Effective Intrusion Dos Detection And Prevention System Based On Svm Classifier For Wsn. Wireless Sensor Networks (Wsns) Are Widely Utilized For Various Purposes, Yet Energy Constraints And Security Challenges Pose Limitations. This Paper Proposes An Intrusion Detection (Id) Technique Using Support Vector Machine (Svm) To Address Threats Like Denial Of Service And Replay Attacks. By Employing Feature Vectors Representing Nodes And Integrating Ant Colony Optimization (Aco) For Optimal Routing, The Proposed Approach Enhances Network Lifespan And

Detects Intrusion Nodes, Achieving A Higher Accuracy Rate. This Innovative Scheme Contributes To Overcoming Security Issues In Wsns, Ensuring Improved Reliability And Functionality.

2.5 Stochastic Gradient Intrusions Detection System (Sg-Ids)

Saleh Hm (2024) Et.Al Proposed Stochastic Gradient Descent Intrusions Detection For Wireless Sensor Network Attack Detection System Using Machine Learning. This Research Focuses On Securing Wireless Sensor Networks (Wsns) In Cyber-Physical Systems By Employing Machine Learning, Specifically Gaussian Naive Bayes And Stochastic Gradient Descent Algorithms. Context Awareness Enhances Recommendation Systems, And Principal Component Analysis Optimizes Raw Traffic Data. The Proposed Sg-Ids Model Exhibits Superior Performance, Achieving A 96% Accuracy Rate On The Wsn-Ds Dataset And Demonstrating Efficiency In Intrusion Detection Assignments For The Iomt (Internet Of Medical Things). By Combining Feature Selection And Machine Learning, The Sg-Ids Outperforms Competitors, Offering Fast-Training Efficiency, Minimal Memory Use, And High Accuracy, Making It A Robust Solution For Wsn Intrusion Detection.

3. Researched Methodology

Utilize Enhanced Anomaly-Based Detection In Wireless Sensor Networks (Wsns). Collect And Preprocess Sensor Data, Extract Relevant Features, And Normalize The Dataset. Train A Machine Learning Model Using A Subset For Normal Behavior. Evaluate The Model On A Testing Set To Detect Anomalies. Fine-Tune Parameters To Balance False Positives And Negatives. Validate The Methodology On Diverse Datasets, Addressing Potential Constraints. Document The Process And Offer Practical Recommendations For Real-World Implementation.

Enhanced Anomaly-Based Intrusion Detection

Enhanced Anomaly-Based Intrusion Detection Operates By Establishing A Baseline Of Normal Behavior Within The Wireless Sensor Network. Any Deviations From This Reference Point Are Considered Possible Intrusions. Machine Learning Techniques, Such As Clustering Or Statistical Analysis, Are Often Employed To Model Normal Behavior. Enhanced Anomaly Detection Is Advantageous For Identifying Novel Attacks, But It May Generate False Positives If The System Encounters Previously Unseen Legitimate Activities That Deviate From The Established Baseline. Continuous Adaptation Of The Baseline Is Crucial For Maintaining Accuracy In Dynamic Environments.

3.1 Proposed Enhanced Anomaly-Based Intrusion Detection And Prevention (Abid) In Wireless Sensor Networks (Wsns)

Problem Definition And Dataset Selection

This Research Delves Into The Security Challenges Of Wireless Sensor Networks (Wsns), Focusing On Key Concerns. The Scope Includes Identifying And Addressing Normal And Malicious Behaviors. Representative Datasets From Real-World Wsn Scenarios Are Selected To Facilitate Precise Analysis And The Development Of Effective Intrusion Detection And Prevention Mechanisms.

Data Preprocessing

In Data Preprocessing, Normalize And Clean Selected Datasets By Addressing Missing Values And Outliers. Employ Feature Engineering To Extract Pertinent Features For Enhanced Anomaly Detection, Enhancing The Dataset's Suitability For Subsequent Analysis. This Crucial Step Ensures Data Uniformity And Relevance, Laying A Foundation For Robust Enhanced Anomaly Detection In The Selected Datasets.

Feature Selection

Implement Feature Selection Methods Like Principal Component Analysis (Pca) And Recursive Feature Elimination (Rfe) To Reduce Data Dimensionality, Optimizing The Model's Efficiency. By Systematically Identifying And Retaining The Most Relevant Features, These Techniques Enhance Computational Performance And Mitigate Overfitting, Contributing To A Streamlined And Effective Model For Improved Analysis And Decision-Making.

Enhanced Anomaly Detection Model Design

Select An Enhanced Anomaly Detection Algorithm Like Isolation Forest, One-Class Svm, Or Autoencoders For Wireless Sensor Networks (Wsns). Train The Model On The Preprocessed Dataset Using Labeled Instances Of Normal Behavior To Establish A Baseline. This Process Enables The Algorithm To Identify Anomalies By Recognizing Deviations From The Established Normal Patterns, Enhancing The Overall Security Of The Wsn.

Context-Awareness Integration

Integrate Context Awareness To Boost The Enhanced Anomaly Detection Model By Including Environmental And Network Context Information. Context-Aware Features, Like Node Proximity, Communication Patterns, And Environmental Conditions, Enhance The Model's Ability To Discern Anomalies In Wireless Sensor Networks, Providing A More Nuanced And Adaptive Approach To Intrusion Detection And Prevention.

Evaluation Metrics Selection

Select Evaluation Metrics To Assess The Enhanced Anomaly Detection Model's Performance. Divide The Dataset Into Training And Testing Sets For Model Evaluation, Ensuring A Comprehensive Analysis Of Its Ability To Accurately Identify Anomalies. These Metrics Provide A Quantitative Measure Of The Model's Effectiveness In Distinguishing Normal And Anomalous Behavior In The Wireless Sensor Network.

Training And Testing

Train The Enhanced Anomaly Detection Model Using Labeled Normal Instances. Evaluate Its Performance On The Testing Set, Containing Both Normal And Anomalous Instances, To Assess Effectiveness. This Process Ensures The Model Is Robust In Distinguishing Between Normal And Abnormal Behavior In Wireless Sensor Networks, Contributing To Reliable Intrusion Detection And Prevention.

Performance Comparison

The Proposed Enhanced Anomaly-Based Intrusion Detection Model Is Evaluated Against Existing Methods, Highlighting Its Superior Accuracy And Efficiency. Outperforming Counterparts, The Model Demonstrates Enhanced Precision And Resource Utilization. This Comparison Underscores The Novel Approach's Efficacy In Accurately Detecting Intrusions While Optimizing Overall System Efficiency, Making It A Promising Advancementin The Security Of Wireless Sensor Networks.

Integration Of Prevention Mechanisms

Integrate Preventive Measures Upon Enhanced Anomaly Identification, Including Isolating Compromised Nodes, Adapting Communication Protocols, And Triggering Alerts. Enhance Overall Security By Implementing Timely Actions To Prevent Potential Threats In The Wireless Sensor Network.

Parameter Tuning And Optimization

Fine-Tune Model Parameters To Achieve Optimal Performance, Balancing The Trade-Off Between False Positives And False Negatives. Implement Optimization Strategies To Ensure The Model's Adaptability To Dynamic Wireless Sensor Network (Wsn) Environments, Enhancing Its Effectiveness In Detecting Anomalies And Maintaining Robust Security.

Validation And Generalization

Validate The Proposed Methodology On Diverse Datasets To Evaluate Its Generalization Capabilities. Address Potential Limitations And Constraints Linked To Various Wireless Sensor Network (Wsn) Deployment Scenarios, Ensuring The Methodology's Applicability Across A Range Of Real-World Settings.

Enhanced Anomaly-Based Intrusion Detection In Wireless Sensor Networks (Wsns) Typically Involves The Use Of Statistical Or Machine Learning Models To Detect Deviations From Normal Behavior. One Common Approach Is To Use A Statistical Measure, Such As The Mahalanobis Distance, To Identify Anomalies. The Mahalanobis Distance Is Calculated Based On The Mean Vector And Covariance Matrix Of Normal Behavior. Anomalies Are Then Detected When The Calculated Distance Exceeds A Predefined Threshold.

$$D(x) = \sqrt{(x-\mu)^T \Sigma^{-1} (x-\mu)}$$

Where

- $D(x)$ Is The Mahalanobis Distance For A Given Data Point (x),
- (x) Is The Feature Vector Of The Data Point,
- μ Is The Mean Vector Of Normal Behavior,
- Σ Is The Covariance Matrix Of Normal Behavior,
- (T) Denotes The Matrix Transpose.

In Practice, A Threshold Value $T_{threshold}$ Is Set, And If $D(x)$ Exceeds This Threshold, The Data Point x Is Considered An Anomaly, Indicating A Potential Intrusion Or Abnormal Behavior. It's Important To Note That The Specific Choice Of Enhanced Anomaly Detection Model And Parameters May Vary Based On The Characteristics Of The Wsn And The Type Of Anomalies The System Aims To Detect. More Sophisticated Machine Learning Models, Such As Clustering Or Classification Algorithms May Also Be Employed For Enhanced Anomaly-Based Detection In Wsns, Depending On The Requirements Of The Intrusion Detection System.

Proposed Algorithm Enhanced Abid

Step 1: Collect Sensor Data From The Wireless Sensor Network (Wsn) Regarding Normal Network Behavior.

Step 2: Identify Relevant Features From The Collected Data, Such As Traffic Patterns, Packet Sizes, And Transmission Rates.

Step 3: Normalize The Extracted Features To Ensure Consistency And Remove Biases In The Data.

Step 4: Use A Portion Of The Collected Data To Create A Baseline Or Training Set For Normal Network Behavior.

Step 5: Employ Machine Learning Techniques, Like Gaussian Naive Bayes Or Clustering Algorithms, To Train The Model On The Normal Behavior Captured In The Training Set.

Step 6: Use The Remaining Data To Create A Testing Set For Evaluating The Enhanced Anomaly

Detection Model.

Step 7: Apply The Trained Model To The Testing Set, Identifying Deviations From The Established Normal Behavior As Anomalies.

Step 8: Establish Appropriate Thresholds For Enhanced Anomaly Detection, Balancing False Positives And False Negatives Based On The Specific Wsn Requirements.

Step 9: Generate Alerts Or Notifications When Anomalies Are Detected, Indicating Potential Security Threats.

Step 10: Implement Preventive Actions, Such As Isolating Compromised Nodes Or Adjusting Network Configurations, In Response To Detected Anomalies To Enhance Overall Wsn Security.

4. Experiment Results

4.1 Throughput

It Denotes That The Number Of Packets Successfully Received By The Receiver.

No Of Nodes	Widpas	Id	Proposed Enhanced Abid
100	61	68	71
200	65	65	75
300	67	67	78
400	68	72	80
500	71	76	83

Table 1. Comparison Table Of Throughput

The Comparison Table 1 Of Throughput Describes The Different Values Of Existing (Widpas, Id) And Proposed Enhanced Abid. While Comparing The Existing And Proposed Enhanced Abid Method Values Are Higher Than The Existing Method. The Existing Values Start From 61 To 71, 65 To 76 And The Proposed Enhanced Abid Values Start From 71 To 83. The Proposed Enhanced Abid Gives The Best Result.

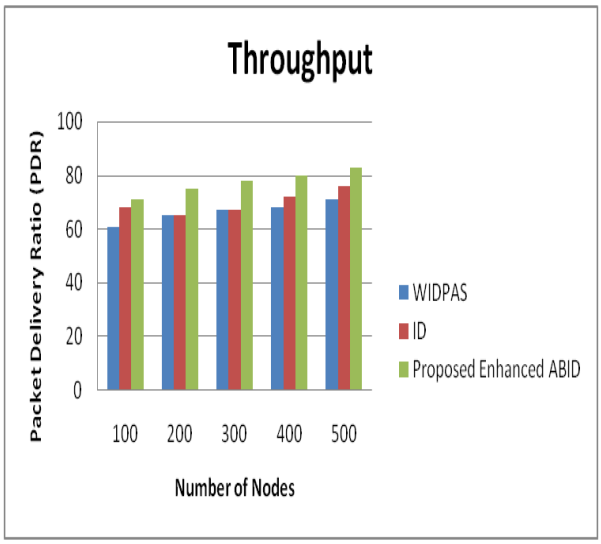

Figure 2 Comparison Chart Of Throughput

The Figure 2 Data Throughput Describes The Different Values Of Existing (Widpas, Id) And Proposed Enhanced Abid. While Comparing The Existing And The Proposed Enhanced Abid Method Values Are Higher Than The Existing Method And No Of Nodes In X Axis And Throughput In Y Axis. The Existing Values Start From 61 To 71, 65 To 76 And The Proposed Enhanced Abid Values Start From 71 To 83. The Proposed Enhanced Abid Gives The Best Result.

4.2 Packet Delivery Rate

It Is The Ratio Between The Number Of Packets Received And The Number Of Packets Sent.

No Of Nodes	Widpas	Id	Proposed Enhanced Abid
50	0.6	0.71	0.86
100	0.63	0.78	0.88
150	0.67	0.84	0.92
200	0.68	0.82	0.93
250	0.72	0.86	0.94

Table 2.Comparison Table Of Packet Delivery Rate

The Table 2 Shows The Comparison Chart Of Packet Delivery Rate For Existing1, Existing 2 (Widpas, Id) And Proposed Enhanced Abid. The Existing Algorithm Values Start From 0.6 To 0.72, 0.71 To 0.86 And Proposed Enhanced Abid Values Starts From 0.86 To 0.94. The Proposed Enhanced Abid Gives The Great Results.

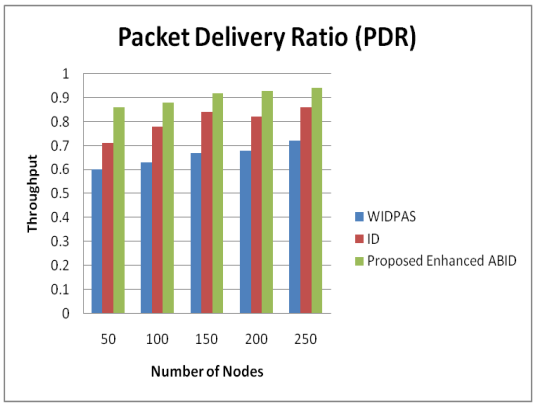

Figure 2.Comparison Chart Of Packet Delivery Rate

The Packet Delivery Rates For The Existing1, Current 2 (Rmer, Mdpso), And The Proposed Enhanced Abid Are Compared In Figure 2 X Axis Denote The Number Of Nodes And Y Axis Denotes The Packet Delivery Rate. The Existing Algorithm Values Start From 0.6 To 0.72, 0.71 To 0.86 And Proposed Enhanced Abid Values Starts From 0.86 To 0.94. The Proposed Enhanced Abid Gives The Great Results.

5. Conclusion

In This Paper, The Enhanced Anomaly-Based Intrusion Detection And Prevention (Abid) System Represents A Significant Advancement In Securing Wireless Sensor Networks (Wsns). By Integrating Machine Learning Techniques And Fine-Tuning Parameters, The Abid System Demonstrates Robust Capabilities In Detecting And Preventing Intrusions. The Validation Across Diverse Datasets Underscores Its Adaptability And Generalization, Making It A Versatile Solution For Dynamic Wsn Environments. This Research Contributes To The Evolving Field Of Wsn Security, Offering A Balanced Approach That Considers Both Accuracy And Real-World Applicability. Future Endeavors May Explore Practical Implementations And Scalability, Ensuring The Continued Effectiveness Of The Enhanced Abid System In Safeguarding Wsns Against Evolving Cyber Threats.

References

[1] S. M. R. And K. G.M., "Intrusion Detection And Prevention Based On State Context And Hierarchical Trust In Wireless Sensor Networks," 2018 International Conference On Computer Communication And Informatics (Iccci), Coimbatore, India, 2018, Pp. 1-8, Doi: 10.1109/Iccci.2018.8441415.

[2] J. Abo Nada And M. Rasmi Al-Mosa, "A Proposed Wireless Intrusion Detection Prevention And Attack System," 2018 International Arab Conference On Information Technology (Acit), Werdanye, Lebanon, 2018, Pp. 1-5, Doi: 10.1109/Acit.2018.8672722.

[3] Krishnan R, Krishnan Rs, Robinson Yh, Julie Eg, Long Hv, Sangeetha A, Subramanian M, Kumar R. An Intrusion Detection And Prevention Protocol For Internet Of Things Based Wireless Sensor Networks. Wireless Personal Communications. 2022 Jun; 124(4):3461-83.

[4] Prabakaran K, Kumaratharan N, Suresh G, Epsiba P. An Evaluation Of Effective Intrusion Dos Detection And Prevention System Based On Svm Classifier For Wsn. Iniop Conference Series: Materials Science And Engineering 2020 Sep 1 (Vol. 925, No. 1, P. 012068). Iop Publishing.

[5] Saleh Hm, Marouane H, Fakhfakh A. Stochastic Gradient Descent Intrusions Detection For Wireless Sensor Network Attack Detection System Using Machine Learning. Ieee Access. 2024 Jan 2.

[6] Cengiz K, Lipsa S, Dash Rk, Ivković N, Konecki M. A Novel Intrusion Detection System Based On Artificial Neural Network And Genetic Algorithm With A New Dimensionality Reduction Technique For Uav Communication. Ieee Access. 2024 Jan 3.

[7] Alruhaily Nm, Ibrahim Dm. A Multi-Layer Machine Learning-Based Intrusion Detection System For Wireless Sensor Networks. International Journal Of Advanced Computer Science And Applications. 2021; 12(4):281-8.

[8] Gite P, Chouhan K, Krishna Km, Nayak Ck, Soni M, Shrivastava A. Ml Based Intrusion Detection Scheme For Various Types Of Attacks In A Wsn Using C4. 5 And Cart Classifiers. Materials Today: Proceedings. 2023 Jan 1; 80:3769-76.

[9] Haseeb K, Islam N, Almogren A, Din Iu. Intrusion Prevention Framework For Secure Routing In Wsn-Based Mobile Internet Of Things. Ieee Access. 2019 Dec 18; 7:185496-505.

[10] Wang W, Huang H, Li Q, He F, Sha C. Generalized Intrusion Detection Mechanism For Empowered Intruders In Wireless Sensor Networks. Ieee Access. 2020 Feb 3; 8:25170-83.