advantages compared to traditional technologies. Under the conditions of high soil moisture, the application of these technologies allows for optimal results in reducing soil compaction and preserving soil fertility. A comparative analysis of different tire types demonstrated that low-pressure tires are the most effective for maintaining soil structure during heavy agricultural operations, such as plowing and seedbed preparation.

Conclusions:

1. The use of innovative materials for tires and track drives significantly reduces the negative impact on soil, particularly by reducing soil compaction and improving soil structure.
2. To achieve optimal ecological results, it is necessary to combine various methods, including low-pressure tires, dual tires, and interchangeable track drives, depending on soil type and climatic conditions.
3. Further research should focus on improving technologies to ensure soil fertility preservation while enhancing tractor efficiency, as well as analyzing the impact of different tire types on reducing energy consumption.

References:

1. Rebrov O.Yu. Scientific Justification for Improving the Efficiency of Wheel Tractor Drives in Energy-Intensive Agricultural Operations. Kharkiv: NTU "KhPI," 2021.
2. Nadikto V.T. Determining the Maximum Slippage of Wheel Drives Considering the Limitation of Their Ground Pressure. *Techniques and Technologies in Agricultural Production*, 2014, No. 7, pp. 34-38.
3. Lebedev A.T., Kalinin E.I. Evaluation of the Impact of Installing Dual Tires on Slippage of Tractor Drives in the Plowing Aggregate in High Moisture Conditions. *Bulletin of Kharkiv National Technical University of Agriculture*, 2010, Issue 103, pp. 199-205.

METHOD FOR DETECTING UNAUTHORIZED NODES

PhD student Yevhen Kovda
Department of Information Systems named after V. O. Kravtsia
PhD, Associated Professor Tetiana Poliakova
Cross-Cultural Communication and Foreign Languages Department
National Technical University “Kharkiv Polytechnic Institute”
Kharkiv, Ukraine

Abstract. This paper proposes an anomaly detection method based on a combination of Bayesian models for estimating the probability of node activity with stochastic filtering methods that provide adaptive real-time

update of estimates. This approach allows implementing an effective security control system capable of detecting potentially dangerous nodes even in the absence of additional cryptographic mechanisms or centralized monitoring.
Keywords: wireless telecommunication networks, MAC layer, Bayesian models, network node.

In modern wireless telecommunications networks, the media access control (MAC) layer remains one of the most vulnerable to malicious attacks. Attacks such as spoofing, flooding, and MAC impersonation can seriously disrupt the normal functioning of the network, threaten the confidentiality, integrity, and availability of information, and reduce overall system performance. The emergence of unauthorized nodes that masquerade as legitimate users and can imperceptibly perform unwanted or malicious actions is especially dangerous. In this context, the task of developing methods for detecting such nodes based on the analysis of their behavior is relevant. One of the promising approaches is the use of mathematical models that allow detecting deviations from the typical activity profile within the MAC layer.

The growth of the number of devices in wireless networks, particularly in IoT environments, necessitates the creation of security methods that do not require complex cryptographic procedures and are able to work in real time with limited computing resources. Traditional authentication and authorization mechanisms, although they remain an important component of network protection, do not always allow for a prompt response to dynamic threats, especially in decentralized topologies or when working in environments with frequent configuration changes.

Recent research in the field of information security shows a growing interest in behavioral methods, based on statistical analysis of node activity, for detecting anomalies. Among such approaches, Bayesian models deserve special attention. They provide a flexible representation of uncertainties and allow adapting to new conditions based on accumulated data. In combination with filtering algorithms, these methods create the prerequisites for building effective systems for detecting unauthorized actions without the need for external sources of knowledge or centralized databases of attack patterns.

The purpose of this work is to develop and study a method for detecting unauthorized nodes in wireless networks based on the analysis of activity dynamics at the MAC level. The main focus is on building a mathematical model that allows you to form a behavioral profile of each node, assess the degree of deviation of the current behavior from the expected one, and detect anomalies with a given sensitivity. To achieve this goal, the work uses a Bayesian approach to modeling activity, particle filtering methods for online parameter estimation, and formalizes decision-making criteria in the form of a loss function with weighting coefficients for false positive control.

In modern research devoted to detecting unauthorized nodes in wireless networks, various approaches using machine learning, statistical analysis, filtering, and artificial intelligence are actively being developed.

The application of deep neural networks to detect attacks in wireless sensor networks demonstrates high classification accuracy and the ability to generalize new types of anomalies [1]. However, such methods require large amounts of training data and significant computing resources, which makes their implementation in devices with limited energy difficult.

Machine learning algorithms, in particular decision trees, support vector machines, and random forests, are actively used for classifying network traffic and anomalies [2]. Their advantage is high speed and flexibility, but the results strongly depend on the quality of feature selection.

Naive Bayesian classifiers are also used to detect unauthorized nodes due to their simplicity and ability to work in real time [3]. Their main limitation is the assumption of independence between features, which is not always true in real networks.

To detect unauthorized or anomalous activity at the MAC level, it is necessary to build a mathematical model of the normal behavior of nodes in the network. Such a model should take into account how often each node accesses the data transmission medium, i.e. initiates access or transmits information.

To formalize the activity of nodes, we introduce the following notation. N is the total number of nodes in the network. Then $x_i(t)$ is node activity indicator i at a point in time t, where: $x_i(t) = 1$, if a node is transmitting or attempting to transmit data, $x_i(t) = 0$, if the node is inactive at this moment. In turn, the network state vector at time t, which describes the activity of all network nodes, has the form

$$X(t) = [x_1(t), x_2(t), \dots, x_t(t)]. \quad (1)$$

To model the probabilistic behavior of an individual node, a binomial model is used. It is a special case of a Bayesian network. It allows us to describe the probability with which a node will be active at a certain point in time. Such a model looks like this:

$$P(\, x_i(t) \mid \theta_i \,) = \theta_i^{x_i(t)} (1 - \theta_i)^{1 - x_i(t)}, \quad (2)$$

where: $\theta_i \in [0,1]$ — a parameter that describes the probability that a node i will be active at any given time, $x_i(t)$ — actual node activity status at time t.

The essence of the above formula (2) is that if $x_i(t) = 1$, i.e. the node is active at a given moment in time, then the probability of this event is equal to θ_i. Instead, if $x_i(t) = 0$, i.e. the node does not show any activity, the probability of such an event is $1 - \theta_i$. Thus, the behavior of each node can be

completely characterized by a single parameter θ_i, which describes the average frequency of its activity in the network.

Since the parameter θ_i is usually unknown in advance, it can be estimated based on the collected history of observations over a certain period of time T. For this purpose, the maximum likelihood method is used (Maximum Likelihood Estimation):

$$\hat{\theta}_i = \frac{1}{T}\sum_{t=1}^{T} x_i(t), \quad (3)$$

In other words, $\hat{\theta}_i$ is the average frequency of node activity i during the last T moments of time. This approach allows you to form a profile of the "normal" behavior of each node based on the real traffic observed in the network.

Thus, the basis for further anomaly analysis was formulated: if the behavior of the node begins to differ significantly from the estimated parameter $\hat{\theta}_i$, this may indicate an unauthorized access attempt or a MAC-level attack.

The results obtained indicate the balanced nature of the method, which provides high accuracy with a moderate level of false decisions. Thanks to the adaptive mechanism of activity estimation, the system demonstrates good sensitivity to deviations and at the same time remains robust to random fluctuations in the behavior of normal nodes.

The presented data confirm that the detection method based on the Bayesian model and activity estimation allows to effectively identify malicious behavior in the network.

As a result of the research, an effective method for detecting unauthorized nodes at the MAC level was developed. It

is based on the analysis of deviations in the behavior of devices without the need for additional hardware. The proposed approach combines Bayesian modeling and adaptive filtering, which allows for dynamic assessment of the activity parameters of each node in real time.

The flexibility of the method is ensured by the ability to self-learn based on historical data and update estimates when the network environment changes. This makes the proposed model especially useful in conditions of unstable traffic or variable topology. In addition, the selected algorithmic solutions allow for compatibility with a wide range of existing link-layer protocols, such as IEEE 802.11 or IEEE 802.15.4, which opens up opportunities for practical implementation in wireless networks for various purposes - from local IoT systems to large corporate infrastructures.

Thus, the method demonstrates both high detection efficiency and practical feasibility in modern telecommunication systems with limited resources.

References

1. Trubchaninova K. A. Artificial intelligence methods in wireless electronic communication systems / K. A. Trubchaninova, O. A. Serkov, V. M. Voronets // Information and control systems in railway transport: abstracts of poster presentations and speeches of participants of the 36th International Scientific and Practical Conference "Information and control systems in railway transport" (Kharkiv, November 16-17, 2023). – 2023. – No. 3 (supplement). – P. 26-27.
2. Serkov O. A. Methodology for increasing the efficiency of electronic communication systems / O. A. Serkov, N. V. Dzhenyuk, B. O. Lazurenko // Problems of informatics and modeling (PIM-2023): abstracts of the 23rd int. scientific and technical conference. conf., Kharkiv – Odesa, September 20-22, 2023 / scientific editor V. D. Dmytrienko; National Acad. of Sciences of Ukraine [and others]. – Kharkiv: Kontrast, 2023. – P. 17-19.
3. Voronets V. Method for forming a packet transmission plan at peak network load, which reduces response / V. Voronets, P. Pustovoitov // Systems of control, navigation and communication. Collection of scientific works. – Poltava: PNTU, 2024. – T. 1 (75). – P. 185-188. – doi:https://doi.org/10.26906/SUNZ.2024.1.185.

OPTIMIZATION OF SURFACE QUALITY IN PRECISION GRINDING USING DIAMOND WHEELS WITH VARIABLE GRAIN COMPOSITION

Ph.D student Dmytro Kulina
Research supervisor Ph.D., Doctor of Technical Sciences, Professor of the Department of Manufacturing Engineering and Metal-Cutting Machines, Hasanov Magomedemin
Department of Manufacturing Engineering and Metal-Cutting Machines
Language support supervisor DSc, Professor Tetyana Sergeyeva
Cross-Cultural Communication and Foreign Language Department

Abstract. The paper presents a study on the influence of diamond grinding wheels with variable grain composition on surface quality during precision grinding of hard-to-machine materials. The research examines how combinations of fine and coarse abrasive grains within a single tool affect surface roughness, thermal load, and tool wear. Grinding tests were conducted