Research on Forecasting and Precise Prevention of Telecommunication Network Fraud Cases at the Grassroots Level Based on the ARIMA Model

Han Chuankai, Yan Xiaodan
China People's Police University, Langfang, Hebei, China

Abstract: The current wave of telecommunication network fraud has swept across the country, with the focus of incidents gradually penetrating into county and rural areas. Grassroots public security organs have become the main force in combating and managing telecommunication network fraud crimes. Although the current prevention and control efforts have begun to show results, the methods of fraud are constantly innovating, making it difficult to guard against. Grassroots public security needs to continue to exert efforts, deeply analyze the characteristics of crimes, the patterns of incidents, and case data, and use big data technology to promote the modernization of combating and managing work. In this context, the author applies the time series ARIMA model to analyze and predict the number of various types of fraud cases in grassroots telecommunication network fraud cases, and calculates the number of incidents of each type of fraud in the next twelve time periods. Based on the predicted results, targeted and precise measures are formulated for high-incidence types of fraud, with data prediction as the starting point, aiming at precise and targeted strategies, and gradually building a new mechanism for precise anti-fraud.

Keywords: Telecom Network Fraud; Time Series; ARIMA Model

1. Introduction

In recent years, telecommunication network fraud has shown an increasing trend in grassroots areas, with the variety of scams constantly evolving. According to relevant statistical data from the Ministry of Public Security [1], in just the past year, millions of new cases have emerged in grassroots areas across the country, with the amount involved reaching hundreds of billions of yuan. Five types of scams, includingOrder scalping and rebate (commission refund scams),Fake investment and financial management (fake investment and financial management), Fake online loans (fake online loans), Impersonating customer service (impersonating customer service), and Impersonating public security, procuratorial, and judicial authorities (impersonating public security and judicial authorities), accounted for nearly 80% of the total cases, becoming the most prominent five high-incidence types of cases. This paper takes the number of various types of fraud cases in Z County, H Province, from January 2020 to December 2024 as a data sample. By applying the time series ARIMA model to analyze and predict the future incidence trends of various types of fraud cases, it aims to reduce the incidence rate by accurately warning of high-incidence areas and periods and carrying out targeted prevention work to reduce the occurrence of fraud cases at the source. In terms of recovering losses, through accurate understanding of the trends in fraud cases, timely adjustments to crackdown strategies, and rapid freezing of funds involved, the economic losses of victims can be minimized as much as possible. From the perspective of enhancing the efficiency of grassroots policing, a precise strike and prevention strategy based on model predictions can optimize the allocation of police resources, avoid blind investment of police forces, and improve the efficiency and quality of police work.

2. Characteristics and Current Status of Ground-Level Telecommunication Network Fraud Cases

2.1 Characteristics of Grassroots Telecom Network Fraud Cases

Fraud methods are diverse and varied, with impersonation scams including those

impersonating public security and judicial authorities and customer service scams, online loan scams including fake loan platform scams and scams to eliminate bad records, online friendship scams including "pig-killing" scams and emotional scams, and false investment and financial management scams including Investment fraud(inducement investment scams) and pension investment and financial management scams. In addition, there are also part-time Order padding scams (part-time order scams) and game-related scams, etc. [2]

The modus operandi of criminal activities has become more intelligent in recent years. Fraudsters have fully utilized AI technology [3], employing voice synthesis and image synthesis techniques to mimic the voices and appearances of people familiar to the victims, thereby engaging in fraudulent activities and increasing the deception involved. For instance, some fraudsters use AI technology to synthesize the voice of a corporate boss and issue transfer instructions to financial personnel, resulting in significant losses to the company. In terms of big data, fraudsters obtain a large amount of personal information through illegal channels, including names, phone numbers, consumption habits, etc., and use this information for targeted fraud, enhancing the success rate of the scams. For example, based on the victim's consumption records, they recommend fraudulent goods or services that match, making it easier for the victim to be deceived.

Fraud organizations are becoming more organized, and telecommunication network fraud gangs typically exhibit a tight organizational structure. Taking a common fraud group as an example, the gang is divided into multiple levels within. The top level consists of the organizers, who are responsible for planning fraud schemes, recruiting personnel, and coordinating resources. The intermediate levels include technical support staff, who are responsible for building the fraud platform and maintaining network security; communication personnel, who communicate with victims through telephone and online chat to carry out the fraud; and information collection personnel, who are responsible for illegally obtaining personal information. The lowest level consists of money laundering personnel, who are responsible for legitimizing the proceeds of the fraud through complex financial channels, making them appear legal on the surface. This group-oriented operational model makes fraud activities more efficient and covert, increasing the difficulty of combating them[4].

2.2 Current Situation of Telecom Network Fraud Cases at the Grassroots Level

According to the statistical data from the Public Security Bureau of Province H, over the past five years, the number of grassroots telecommunication network fraud cases in Province H has increased from 50,000 per year to 150,000, with an annual growth rate of over 20%. The amount involved has also grown from an initial 1 billion yuan to 5 billion yuan, showing an astonishing increase. This indicates that not only is the number of grassroots telecommunication network fraud cases continuously rising, but the amount involved is also increasing, causing severe economic losses to society. Analysis of the data on telecommunication network fraud cases in grassroots areas across the country reveals that economically developed regions and densely populated areas have relatively high incidence rates. For instance, in economically developed areas such as the Yangtze River Delta and the Pearl River Delta, due to frequent commercial activities and large population movements, the number of telecommunication network fraud cases accounts for over 30% of the total number of grassroots cases nationwide. In some densely populated suburban areas, due to the large number of migrant populations and relatively weak public awareness of prevention, the incidence rate is also significantly higher than in other regions. This suggests that factors such as the level of economic development and population density are closely related to the occurrence of telecommunication network fraud cases.

In terms of case jurisdiction, telecom network fraud cases often involve multiple regions, and even cross-border operations. There is controversy over the definition of jurisdiction among police forces in different regions, leading to low efficiency in case investigation. In terms of investigation difficulty, fraudsters use the anonymity of the internet and the characteristics of cross-border operations to hide their identities and whereabouts, posing significant challenges for the police in tracking clues and collecting evidence. At the same time, the current linkage and collaboration mechanism between various departments is not yet perfect. There is a lack of

timely information sharing and close coordination between public security, banks, telecommunications companies, and other departments, making it impossible to form an effective joint effort to combat crime[5]. The current publicity methods are relatively single, mainly relying on traditional forms such as distributing promotional materials and holding lectures, which makes it difficult to attract public attention and results in limited publicity effects. Moreover, the content of the publicity lacks pertinency, and there is no differentiated publicity tailored to the characteristics of different victim groups, making it impossible to effectively improve the public's awareness of prevention. In terms of industry regulation, telecom operators do not implement the real-name registration system for telephone numbers effectively, resulting in a large number of non-real-name SIM cards being used for fraud activities. Banks also have loopholes in fund supervision, with inadequate monitoring of abnormal fund flows, making it impossible to effectively intercept fraudulent funds.

3. Principles of Applying Time Series ARIMA Models

3.1 Basic Principles of the Model

The ARIMA model, which stands for Autoregressive Integrated Moving Average, analyzes historical data to identify patterns of change over time and uses these patterns to forecast future data trends. The autoregressive component reflects the linear relationship between the current value of the time series and its past values, the differencing component is used to transform a non-stationary time series into a stationary one, and the moving average component takes into account the random fluctuations within the time series [6].

3.2 Application Feasibility

The data characteristics of the ARIMA model align with the prediction of telecommunication network fraud cases, as the data for such cases exhibit distinct time series characteristics, with the number of cases showing certain patterns of variation over time. This data encompasses information about the occurrence of cases in different time periods in the past, such as the number of cases per month or per quarter, meeting the data requirements of the ARIMA model. Through the analysis of historical case data, hidden trends, seasonality, and cyclical characteristics can be extracted, providing a basis for predicting future occurrences of cases. The ARIMA model has clear predictive advantages compared to other forecasting methods; it can fully utilize the information in historical data to effectively capture the complex patterns of case occurrences. It not only considers the long-term trends in the number of cases but also analyzes and forecasts short-term fluctuations. Based on the predictive results of the ARIMA model, the police can proactively develop targeted prevention and response strategies, strengthen the deployment of police forces in high-risk areas and periods, and carry out precise publicity. This enhances the efficiency and effectiveness of prevention and response efforts, providing robust data support for the governance of grassroots telecommunication network fraud cases.

3.3 ARIMA Model Modeling Process

Time series analysis (ARIMA) is a model that predicts future data based on historical data from past periods. The specific modeling process is as follows:

1. The modeling requires that the data meet the stationarity condition. Check the ADF test results and analyze whether the null hypothesis of non-stationarity can be significantly rejected based on the t-value ($P<0.05$). Data that are not stationary need to be differenced to meet the stationarity condition.
2. Examine the data comparison chart before and after differencing to determine if the series is stationary. Perform partial autocorrelation analysis and autocorrelation analysis on the time series, and estimate the p and q values based on the truncation condition.
3. Ensure the model exhibits pure randomness, meaning that the model residuals are white noise. Check the model diagnostic table and test the model white noise using the P-value of the Q statistic ($P>0.05$). Additionally, analysis can be conducted using information criteria such as AIC and BIC (the lower, the better). Analysis can also be performed through the model residuals ACF/PACF chart. Based on the model parameter table, derive the model equation and conduct a comprehensive analysis in conjunction with the time series analysis chart to obtain the order result for backward prediction.

4. Empirical Analysis of Telecommunication

Network Fraud Cases at Grassroots Level Based on ARIMA Model

4.1 Data Sources

To analyze the changing trends in the number of cases of various types of telecommunication network fraud at the grassroots level, this article conducts interviews with relevant police officers in the sample area and obtains data on various types of telecommunication network fraud cases in H Province's Z County from January 2020 to December 2024 for research.

4.2 Specific Modeling Process

4.2.1 Review the results of the ADF test to obtain a stationary time series

The results of the series test (Table 1) indicate that, based on the variable of impersonation of public security and judicial organs for fraud cases, when the difference is at the 0th order, the significance P-value is 0.224, not showing significance at the level, and the null hypothesis cannot be rejected, indicating that the series is not stationary. When the difference is at the 1st order, the significance P-value is 0.000***, showing significance at the level, and the null hypothesis is rejected, indicating that the series is stationary. When the difference is at the 2nd order, the significance P-value is 0.000***, showing significance at the level, and the null hypothesis is rejected, indicating that the series is stationary. Therefore, performing a first-order difference on the original data can yield a stationary time series. Figure 1 is the time series graph after the first-order difference, and it is evident that it basically possesses stability, meeting the modeling requirements.

Table 1. ADF Test Table

ADF Inspection Table							
Variable	Differential order	t	P	AIC	Critical value		
					1%	5%	10%
Impersonation of public security, procuratorial, and judicial authorities fraud cases	0	-2.153	0.224	220.25	-3.546	-2.912	-2.594
	1	-6.482	0.000***	215.047	-3.553	-2.915	-2.595
	2	-5.316	0.000***	215.727	-3.566	-2.92	-2.598
Note: ***,**,* represent respectively 1%,5%,10% the level of significance							

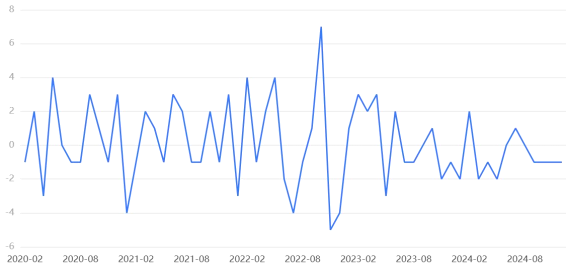

Figure 1. Time Series Graph after the First-Order Difference of the Original Data

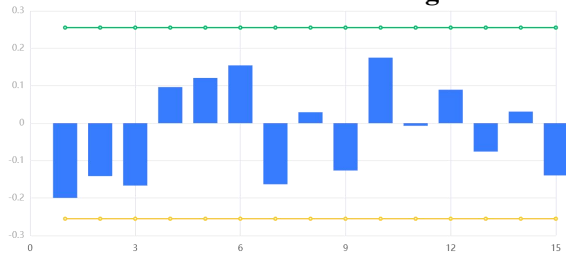

Figure 2: Autocorrelation Plot (ACF)

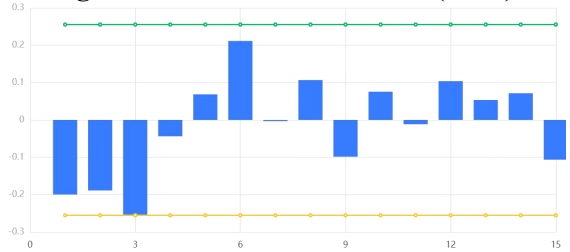

Figure 3. Partial Autocorrelation Plot (PACF)

ARIMA Model（0,1,1） Inspection form		
Item	symbol	Value
	DfResiduals	57
Sample size	N	60
Q statistic	Q6(P-value)	0.31(0.578)
	Q12(P-value)	9.853(0.131)
	Q18(P-value)	14.227(0.286)
	Q24(P-value)	17.387(0.497)
	Q30(P-value)	20.917(0.644)
Information Criteria	AIC	270.344
	BIC	276.576
Goodness of fit	R^2	0.781
Note: ***,**,* Represent respectively 1%,5%,10% the level of significance		

Table 2. Model Verification Table

4.2.2 Perform partial autocorrelation analysis and autocorrelation analysis on the time series, and check the model test table.

The system automatically searches for the optimal parameters based on the AIC information criterion, and the model results are for the ARIMA model (0,1,1) test table, based on the variable: the number of cases of impersonating public security and judicial fraud. From the analysis of the Q statistic results, it can be concluded that Q6 does not show significance at the level, and the hypothesis that the residuals

of the model are white noise sequences cannot be rejected. Meanwhile, the goodness of fit R^2 of the model is 0.781, indicating that the model performs quite well and meets the basic requirements. Therefore, this model can accurately predict future data.

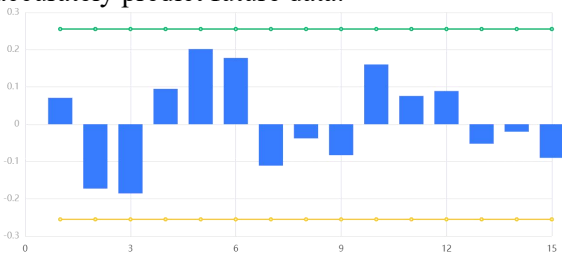

Figure 4. Residual Autocorrelation Plot (ACF) of the Model

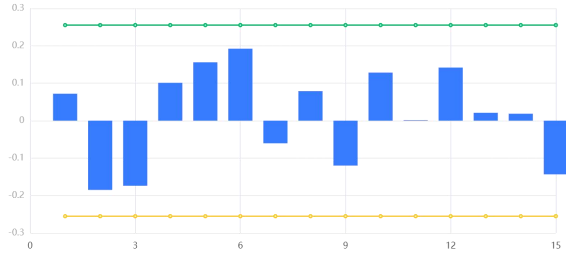

Figure 5. Model Residual Partial Autocorrelation Plot (PACF)

Model Parameter Table						
	nonsupport	Standard deviation	t	P>|t|	0.025	0.975
Constant	0.082	0.202	0.405	0.686	-0.314	0.477
ma.L1	-0.36	0.137	-2.627	0.009	-0.628	-0.091
sigma2	5.156	0.967	5.334	0	3.262	7.051
Note: ***,**,* Represent respectively 1%,5%,10% the level of significance						

Table 3: Model Parameter Results

4.2.3 Testing the model's white noise

Based on the number of cases of variable impersonation public security and judicial fraud, the system automatically searches for the optimal parameters based on the AIC information criterion, and the model results are as follows: the ARIMA model (0,1,1) test table, the model formula is as follows: $y(t)=0.082-0.36*\varepsilon(t-1)$

4.2.4 Derive future trend chart and predictive values

Figure 6 shows the original data chart of the model, the model fitting values, and the model predictive values. It is evident that the future trend is upward. Table 4 is the time series prediction table, which displays the predictive values derived from the model.

4.3 Analysis of Data Results

Figure 6 shows the original data graph, fitted values, and predicted values of the current model. It can be observed that the number of cases of telecom fraud impersonating public security and judicial authorities in this region is expected to continue an upward trend. This prediction result can serve as an important basis for the anti-fraud departments of this region to formulate measures for prevention and crackdown.

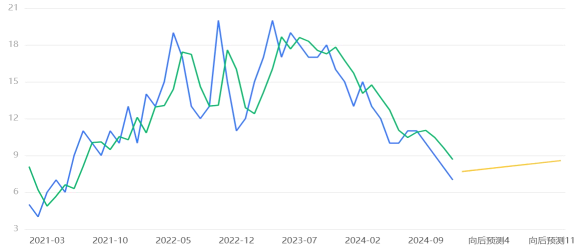

Figure 6. Shows the Original Data, Model Fit Values, and Model Prediction Values for the Model

Predicted value	
Order (time)	Predicted results
1	7.678944479701601
2	7.760598735139861
3	7.842252990578121
4	7.923907246016381
5	8.005561501454642
6	8.0872157568929
7	8.16887001233116
8	8.25052426776942
9	8.332178523207679
10	8.413832778645938
11	8.495487034084197
12	8.577141289522457

Table 4. Time Series Forecasting Table

5. Precision Combat and Prevention Strategies for Telecommunication Network Fraud Cases at the Grassroots Level

From the data results above, it is evident that the number of cases of impersonating public security and judicial authorities in Z County, H Province, is expected to gradually increase from January 2025 to December 2025. This method can also predict the occurrence of other types of fraud cases. Based on these findings, targeted precision combat and prevention measures can be formulated to reduce the incidence of these types of fraud cases. Consequently, this will control the overall number of telecommunication network fraud cases and enhance the effectiveness of grassroots anti-fraud centers in combating and managing telecommunication network fraud crimes.

5.1 Precision Prevention and Control, Source Suppression

In response to the forecasted upward trend in the number of cases in the local area for the next 7 months as mentioned above, precise prevention and control measures should be formulated. According to the peak and high-incidence areas predicted by the ARIMA model, the police should flexibly allocate their forces. For instance, when a high incidence period of telecommunications network fraud cases is predicted in a certain area, police forces from surrounding areas with relatively sufficient resources should be redeployed to reinforce the patrol and prevention forces in that area, increasing the frequency and scope of patrols to deter potential fraud activities. At the same time, comprehensive multi-faceted publicity campaigns should be carried out, focusing on the methods, tactics, scripts, and dialogue of scams such as Order padding for cashback (reimbursement scams) and Impersonating customer service (impersonating customer service scams), achieving full coverage and precise targeted prevention. On one hand, this aims to raise public awareness of anti-fraud, conducting targeted publicity for groups that are prone to such scams, such as organizing anti-fraud campaigns on campuses to address students; on the other hand, social influencing factors should be managed, such as tracing and investigating the accounts that publish lead ads, collaborating with platforms to close these accounts, etc., gradually achieving the elimination of social influencing factors.

5.2 Precision Strike, Full Force Deployment

In response to the predicted outcomes, accurately control the direction of strikes and timely adjust the targets. Develop police deployment and response measures corresponding to different levels of alerts, enhancing response speed. When the ARIMA model predicts that the number of cases will reach a certain threshold, triggering a low-level alert, the police should organize community police to strengthen contact with community grid staff, and release alert information through community bulletin boards, WeChat groups, and other channels, warning residents to be vigilant. If a medium-level alert is triggered, in addition to the above measures, departments such as criminal investigation and cyber security should intervene early, analyze the characteristics of recent fraud cases, and develop targeted investigation plans. Once a case occurs, they can quickly initiate investigations, fully trace calls and communication media related to fraud, and work with the three major telecom operators to manage and block fraudulent numbers, cutting off the source of the scam. When a high-level alert is triggered, activate the emergency response mechanism, multi-force joint operations, increase control over key areas, and conduct checks on suspicious individuals and vehicles. Track and analyze from various aspects such as information flow, capital flow, and network flow, improving the effectiveness of strikes. At the same time, strengthen collaboration with banks and communication enterprises, monitor capital flows and communication anomalies in real-time, and promptly interrupt the fraud chain.

5.3 Combining Prevention and Suppression for Precision and Efficiency

Combining prevention with suppression, on one hand, it is necessary to strengthen internal collaboration within the public security organs. The investigation department is responsible for the investigation and cracking of fraud cases, collecting evidence through traditional means such as on-site investigation and investigative visits, and tracking down suspects. The cyber security department utilizes its technological advantages to monitor and analyze the online platforms and communication tools used by fraudsters, tracking IP addresses and locking down the locations of criminal dens. The economic investigation department focuses on tracking the flow of funds, cooperating with financial institutions such as banks to freeze the funds involved and prevent the outflow of funds. On the other hand, it is essential to deepen cooperation with external institutions to cut off the chain of fraud. Telecom operators should not only manage telephone numbers with real-name registration but also regularly clean up and rectify non-real-name telephone cards, using technical means to monitor abnormal call behaviors, such as high-frequency calls and off-site calls. Once suspicious situations are discovered, communication services for the relevant numbers should be promptly suspended. Banks need to strengthen the supervision of account funds, improve the accuracy of the early warning system for abnormal fund transactions, and while avoiding causing inconvenience to the

property use of the people, focus on situations where large amounts of funds enter and exit frequently in a short period, and the flow of funds is unclear. After verifying the funds involved in fraud or being defrauded, accounts should be frozen promptly and the police notified. Internet companies need to strengthen the review of platform content, cut off at the source of platform publication, promptly block and delete information related to fraud, and cooperate with the police to provide relevant user information and technical support. Combining prevention and suppression is the creation of a new pattern of precise anti-fraud at the grassroots level of public security, which can achieve precise and efficient crackdown and governance of telecom network fraud crimes, and improve the operational efficiency of public security organs.

6. Conclusion

This paper selected the number of various types of telecommunication network fraud cases in Z County, H Province from January 2020 to December 2024 as the data sample. First, it used SPSSPRO to conduct time series analysis and prediction on the sample data, determining that the sequence was non-stationary. After applying second-order differencing, a stationary sequence was obtained, which passed the ADF test and white noise test. Further analysis of its autocorrelation and partial autocorrelation graphs yielded corresponding p-values and q-values. The best model was found to be ARIMA(0,1,2) through testing. Subsequently, a white noise test was conducted on the model's residuals, and the results indicated that the residuals were a white noise sequence, suitable for prediction. The model's goodness-of-fit R^2 was 0.781, indicating excellent performance and meeting basic requirements. This suggests that the prediction model is relatively accurate and can precisely forecast the number of cases of impersonating public security and judiciary fraud in Z County, H Province, over the next seven months, with a high degree of credibility. These results can provide a reference for grassroots anti-fraud centers to adjust their work measures in a timely manner. This innovative approach of utilizing data analysis to achieve precise anti-fraud is a pioneering move towards modernizing and informatizing police work, and it is also a significant step in enhancing the overall effectiveness of grassroots public security.

References

[1] Bai Chengying. How should we prevent the iterative renewal of telecom network fraud? [N]. Yuxi Daily, 2025-02-25(003).

[2] Dong Fanchao. The Ministry of Public Security announces five types of high-frequency telecommunication network fraud cases [N]. Legal Daily, 2022-05-12(004). DOI:10.28241/n.cnki.nfzrb.2022.002509.

[3] Jin Yuting. Research on New Types of Cyber Fraud and Countermeasures in the Context of AIGC[J]. Network Security Technology and Application, 2025, (02): 143-145.

[4] Zhuang Hua, Liao Guangjun. A Governance Framework for Telecommunication Network Fraud Crimes from the Perspective of "Supply-Demand" [J]. Public Security Research, 2023, (02).

[5] Xu Zhou, Bao Han. Operational Risks and Improvement Paths of Anti-Fraud Early Warning and Dissuasion Mechanism[J]. Journal of Railway Police College, 2023, (01).

[6] Han Yishi, Fan Yingsheng, Li Guojun, et al. Analysis of the Growth Trend of Communication Network Fraud Crimes Based on ARIMA Model—Taking Quzhou City, Zhejiang Province as an Example[J]. Theoretical Observation, 2017, (05): 101-103.

