International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 2958-2968

https://doi.org/10.70517/ijhsa464246

Analysis of Transnational Security Enforcement Cooperation Models Based on Intelligence Sharing Mechanisms

Jian Li[1] and Yuqian He[2,*]
[1] Public Security College, Nanjing Police University, Nanjing, Jiangsu, 210023, China
[2] Anti-Drug Academy, Yunnan Police College, Kunming, Yunnan, 650223, China
Corresponding authors: (e-mail: tougaoyx1696@126.com).

Abstract This paper explores the construction of intelligence sharing mechanisms in the context of cross-border security law enforcement cooperation. It analyzes intelligence sharing models under different counter-terrorism interests and establishes a corresponding counter-terrorism utility model. An improved PBFT consensus algorithm is adopted to optimize the consensus process. A blockchain-based intelligence transaction and sharing framework is designed to achieve secure and efficient intelligence resource exchange. Through numerical simulation experiments, the performance of the proposed scheme and the evolution of intelligence sharing game processes are explored. When the number of user attributes in the proposed scheme reaches a maximum of 42, the encryption computation time is approximately 183.4 ms, the key generation time is approximately 226.7 ms, and the decryption time is approximately 40.9 ms. These time consumptions are within normal ranges and can meet practical application requirements. The larger the intelligence sharing cooperative benefit coefficient/penalty coefficient between the two parties, the more it promotes national intelligence sharing.

Index Terms transnational law enforcement, intelligence sharing mechanism, improved PBFT consensus algorithm, blockchain

I. Introduction

The development of economic globalisation has increasingly transformed the world into an interconnected global village, where cooperation and exchange between nations have become the norm and the underlying theme of international relations [1], [2]. However, as the globalisation process expands and deepens, a series of transnational and global issues have also emerged [3]. In recent years, cross-border crime has become increasingly rampant, involving serious illegal activities such as drug trafficking, human trafficking, cyber fraud, and money laundering [4], [5]. In these cross-border criminal activities, criminals exploit differences in national laws, enforcement procedures, and regulatory frameworks to evade prosecution [6]-[8]. For example, drug traffickers may use complex transnational transportation routes to transport drugs from production areas to consumption areas, passing through multiple countries along the way, exploiting loopholes in border controls and differing enforcement rhythms to facilitate the smooth flow of drugs [9]-[11]. The harm caused by non-traditional security issues and the losses they incur are growing increasingly severe, posing a significant challenge to criminal justice systems worldwide [12], [13]. In this context, the necessity and urgency of cross-border security law enforcement cooperation models become particularly evident [14].

International law enforcement cooperation refers to cross-border exchanges in law enforcement matters, where law enforcement agencies from different countries provide mutual assistance and coordinate efforts in combating transnational crimes and maintaining international social order, in accordance with their domestic laws or the international conventions they have joined [15]-[18]. However, transnational security law enforcement faces serious challenges such as cultural differences and shortages of information resources, which hinder the progress of transnational law enforcement [19], [20]. In this context, transnational security law enforcement cooperation based on intelligence-sharing mechanisms becomes critically important. By establishing intelligence-sharing mechanisms for transnational law enforcement, breaking down national borders, and enabling law enforcement agencies from various countries to promptly and comprehensively monitor criminal activities, such mechanisms are key to the smooth operation of international law enforcement cooperation [21]-[24]. Without intelligence sharing, countries would have to act independently, allowing criminal gangs to exploit information gaps to continue their activities, resulting in significantly reduced enforcement effectiveness and an inability to effectively curb the spread of cross-border crime [25]-[27].

Reference [28] examines the impact of conceptual confusion surrounding the legal language governing the relationship between entities and information, and conducts a case study using information sharing for law enforcement purposes as an example, proposing a classification system to determine the allocation of responsibilities and powers related to information. Reference [29] emphasises the importance of multi-agency information sharing and analyses the methods of information sharing in law enforcement operational environments, providing empirical, original evidence indicating that law enforcement officers' information sharing practices vary. Literature [30] explores the differences in the level of confidentiality between observable police agencies and secret services, and analyses the relationship between information sharing, confidentiality, and accountability among security agencies, discussing the level of confidentiality in the work of security agencies within a democratic rule-of-law system. Literature [31] highlights the global prevalence of terrorist organisations and the threats they pose to the entire world, noting that the people of Pakistan have long been targets of terrorist attacks. Literature [32] indicates that transnational crime poses a severe challenge to international security and emphasises international law enforcement cooperation as an important component of international exchange. It introduces the threats faced by China and the United States in the field of cybersecurity and suggests that the two countries engage in comprehensive cooperation in combating cybercrime. Document [33] studies the theories, concepts, and methods of international cooperation among law enforcement agencies in safeguarding economic security, aiming to establish a coherent methodology to understand the collaborative efforts of law enforcement entities in protecting national economic interests. Document [34] aims to examine the factors driving the mobility of police work by studying two different systems, their internal obstacles, and their interactions. Literature [35] identifies the primary narrative frameworks defining the nature of European criminal cooperation and constructs a deep judicial integration model based on the narrative of a common European region, aiming to promote proper management of criminal justice and handling of cross-border personal matters. Literature [36] explores the full range of law enforcement means and tools available to the Chinese government in combating transnational crime, aiming to eliminate obstacles to its national sustainable development.

This paper first analyzes different intelligence sharing models in the field of counter-terrorism and quantifies the contribution of sharing strategies to national security through a counter-terrorism utility model. It proposes a value consensus algorithm based on a trusted execution environment to dynamically assess node value. Combining blockchain technology, it establishes a decentralized intelligence trading framework. Multiple simulation experiments are designed to validate the advantages of the proposed design in terms of performance overhead, node reliability, and fault tolerance. Based on evolutionary game theory, the evolutionary game process of cross-border intelligence sharing is simulated. Through numerical simulation verification, the influence mechanisms of different factors on the selection of intelligence sharing strategies are revealed.

II. Building intelligence sharing mechanisms for transnational law enforcement cooperation

Cross-border law enforcement cooperation is becoming increasingly important in the context of globalization, and intelligence sharing, as its core component, directly affects the effectiveness of such cooperation. This article systematically analyzes the establishment and optimization of intelligence sharing mechanisms from both theoretical and practical perspectives.

II. A. Design of Counter-Terrorism Intelligence Sharing Mechanisms

II. A. 1) Different models of counterterrorism intelligence sharing

Based on differing counter-terrorism interests, countries may directly share counter-terrorism intelligence in accordance with domestic law or indirectly exchange intelligence through third-party counter-terrorism organizations (such as Interpol or Europol). When the purpose of sharing intelligence is to safeguard national security and maximize individual counter-terrorism interests, countries tend to establish bilateral cooperation and directly exchange counter-terrorism intelligence. For example, China and Pakistan share counter-terrorism intelligence to prevent terrorist activities in Afghanistan from spilling over into their own territories. When the purpose of sharing intelligence is driven by stronger common interests, aiming to achieve regional stability and security and maximize overall interests, countries tend to share intelligence through international or regional counter-terrorism organizations. For example, Thailand and Malaysia strengthen their intelligence exchange and cooperation through the Association of Southeast Asian Nations (ASEAN) to prevent international terrorists from infiltrating the Southeast Asian region. Therefore, based on different counter-terrorism interests, intelligence-sharing models can be summarized into three categories: no intelligence sharing, direct intelligence sharing, and indirect intelligence sharing. Different counter-terrorism intelligence-sharing models are illustrated in Figure 1.

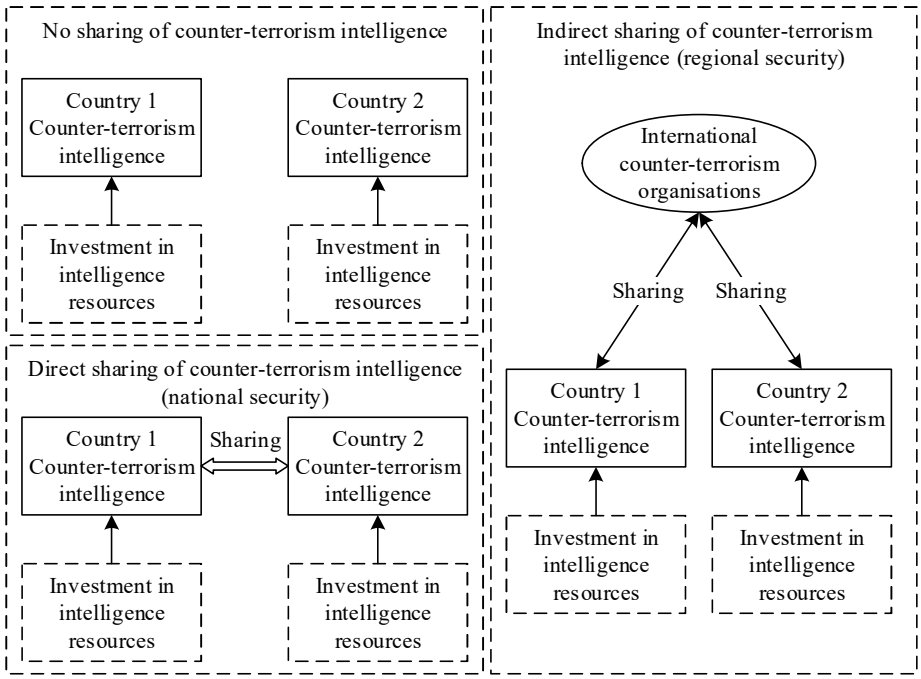


Figure 1: Different Modes of Counter-Terrorism Intelligence Sharing

II. A. 2) Counterterrorism Effectiveness Model for Direct Intelligence Sharing

Due to constraints such as limited counter-terrorism budgets and insufficient intelligence-gathering technologies, some countries seek bilateral counter-terrorism cooperation by exchanging intelligence to ensure their own security. At this point, while both countries allocate their intelligence resources at level x_k, they must also determine the level of intelligence sharing at level s_k. For the country receiving counter-terrorism intelligence, this effectively grants them access to additional counter-terrorism resources, with the two countries now possessing intelligence resources at levels x_1+s_2 and x_2+s_1, respectively. Regarding the setting of the impact of externalities on network information security investment decisions, when Country 1 obtains positive (negative) externalities, it possesses intelligence resources of $x_1 \pm \alpha_2(x_2+s_1)+s_2$, and when Country 2 obtains positive (negative) externalities, it possesses intelligence resources of $x_2 \pm \alpha_1(x_1+s_2)+s_1$. Thus, when directly sharing counter-terrorism intelligence, the probabilities of counter-terrorism success for Country 1 and Country 2 are respectively:

$$\begin{aligned} P_1^s &= 1-\exp\left[-\left(x_1 \pm \alpha_2\left(x_2+s_1\right)+s_2\right)\right] \\ P_2^s &= 1-\exp\left[-\left(x_2 \pm \alpha_1\left(x_1+s_2\right)+s_1\right)\right] \end{aligned} \tag{1}$$

Due to significant differences in data modalities among governments and intelligence agencies, sharing intelligence incurs certain costs associated with standardizing sharing protocols, among other factors. Therefore, the costs associated with processing and transmitting intelligence are denoted as c_k^s. Countries sharing intelligence face the risk of information leaks; if intelligence is intentionally leaked, it could render prior counter-terrorism deployments by intelligence agencies ineffective; unintentional leaks of intelligence (such as passenger information or counter-terrorism operation information) may expose citizens' privacy or allow the receiving country to infer the sending country's defense capabilities or key leading technologies. Therefore, the losses from information leaks are recorded as d_k. The benefits to the receiving country from unintentional intelligence leaks are denoted as φ_k. When both countries share intelligence, they derive a collaborative benefit λ from information sharing. Regarding the setting of cybersecurity information sharing costs, the sharing costs for Country 1 and Country 2 when sharing counter-terrorism intelligence are as follows:

$$\begin{aligned} \Gamma_1\left(s_1;s_2\right) &= \left(c_1^s+d_1\right)s_1^2-\varphi_2 s_2^2-\lambda s_1 s_2 \\ \Gamma_2\left(s_2;s_1\right) &= \left(c_2^s+d_2\right)s_2^2-\varphi_1 s_1^2-\lambda s_1 s_2 \end{aligned} \tag{2}$$

Among these, c_k^s represents the costs incurred by a country when sharing intelligence, including the costs of collecting, transmitting, and processing the shared information; d_k represents the losses incurred by a country due

to intelligence leaks; φ_k represents the potential benefits that an unintended intelligence leak from one country may bring to another country; and λ represents the collaborative benefits when both countries share intelligence. The above cost function satisfies $\partial\Gamma_1(s_1;s_2)/\partial s_1 > 0$; $\partial^2\Gamma_1(s_1;s_2)/\partial s_1^2 > 0$; $\partial\Gamma_2(s_2;s_1)/\partial s_2 < 0$, $\partial^2\Gamma_2(s_2;s_1)/\partial s_2^2 < 0$; $\partial^2\Gamma_1(s_1;s_2)/\partial s_1\partial s_2 \le 0$; $\partial^2\Gamma_2(s_2;s_1)/\partial s_2\partial s_1 \le 0$.

In summary, when both parties directly share intelligence to achieve their respective national security, the counter-terrorism utility maximization problems for both parties are:

$$\begin{aligned}\max_{\{x_1,s_1\}} U_1^S &= v_1 P_1^S - c_1 x_1 - \Gamma_1(s_1;s_2)\\ \max_{\{x_2,s_2\}} U_2^S &= v_2 P_2^S - c_2 x_2 - \Gamma_2(s_2;s_1)\end{aligned} \tag{3}$$

Both countries simultaneously decide on their intelligence resource investment and intelligence sharing ratio. The superscript S indicates the probability of successful counterterrorism and the effectiveness of counterterrorism when intelligence is shared directly. In the rest of this paper, the superscript S is used to indicate the analysis of both sides directly sharing intelligence to pursue national security.

II. B. Value Quantity Consensus Algorithm Based on Trusted Execution Environment

II. B. 1) Overall Algorithm Scheme Process

This consensus algorithm protects Orderer sorting nodes in a trusted execution environment to complete broadcast requests, message processing, configuration transaction messages, and other steps. It uses an improved PBFT consensus algorithm to generate node value based on node performance, and calculates the mixed value of nodes together with consensus completion status, node performance value, and trusted security environment identification, and allocates node identities accordingly. By assigning node identities, it simplifies consensus complexity and reduces communication complexity. Key management and remote authentication within the trusted execution environment provide a secure, isolated runtime environment for smart contracts, safeguarding algorithm security. The consensus process is illustrated in Figure 2.

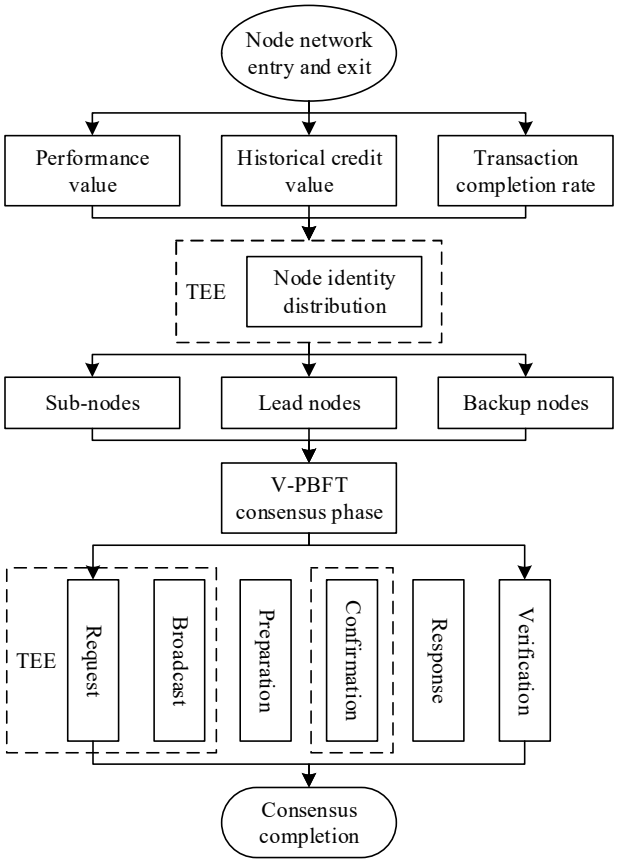


Figure 2: Consensus Process

II. B. 2) Node Value Quantity Model

Definition 1: Performance value calculation is related to the value carried by nodes. By reading the value carried by each node, we can see the expectations for nodes with higher value weights.

The performance value calculation method is defined as follows: Using the Analytic Hierarchy Process (AHP), the value is treated as an element within a hierarchical structure to construct a hierarchical model for calculating the value of nodes. Specifically, this includes:

S1: For a specific node, using the AHP, the value criteria are treated as elements within a hierarchical structure to construct the node's hierarchical model. This hierarchical model includes, from highest to lowest, the objective layer, criteria layer, and sub-criteria layer:

The first level represents the target layer, which contains the value $value_k$, where value is a rational number and k is a node;

The second level represents the standard layer, which contains t elements, where t is a positive integer, $t \le 9$;

The third level represents the sub-standard layer, which contains p elements, where p is a positive integer, $p \le 20$;

S2: Collect node value scores based on the standard layer to obtain the value carried by each element. Compare the values carried by the standard layer in pairs, quantify the comparison results as numerical values, and normalize them to obtain the weights $W_{B_1}, W_{B_2}, ..., W_{B_t}$, where $B_1, B_2, ..., B_t$ represent the t elements in the standard layer;

S3: Calculate the sub-standard layer data based on the number of failure messages, the number of times it became a leader node, and the number of TEE identifiers in the sub-standard layer to obtain the security weight S. Compare the elements in the sub-standard layer in pairs, quantify the comparison results as numerical values, and normalize them to obtain the weights $W_{S_1}, W_{S_2}, ..., W_{S_p}$, where $S_1, S_2, ..., S_p$ represent the p elements in the sub-standard layer;

S4: The total weight of each element in the standard layer is W_{V_i}:

$$W_{V_i} = w_{S_i} \times w_{B_j} \tag{4}$$

Among them, S_i denotes the i th element in the sub-standard layer, and B_j denotes the j th element in the standard layer;

S5: The performance value $value_k$ of node k is as follows:

$$value_k = \sum_{N=1}^{20} \left(value_{ks_i} \times W_{V_i} \right) \tag{5}$$

Among them, $value_{ks_i}$ represents the performance value generated by node k after passing through the standard layer; S_i represents the safety weight of the standard layer, W_{V_i} represents the total weight of each element in the standard layer, N is a built-in constant in the formula, and $value_k$ is the obtained performance value.

Definition 2: Historical credit value is related to time. By considering the proportions of the current credit value and past credit values, it can be shown that the historical credit value is dynamically changing. The expression is:

$$C(i) = \left[1 - \left(\frac{C(i-1)'}{C_{\min}} \right)^3 \right] * 60 \tag{6}$$

Among them, $C(i)$ represents the historical credit value of the current node i, $C(i-1)'$ represents the credit value in the previous period, and $C_{\min}$ represents the minimum credit value allowed by the exchange. If the credit value is lower than the minimum credit value, it means that the node will not participate in the supervision and leadership node competition behavior.

Definition 3: The transaction completion rate associated with each node is derived from the proportion of successful transactions after the node enters the network, expressed as:

$$T(i) = \frac{60}{m} \sum_{i=1}^{n} f_i \tag{7}$$

Among them, m represents the total number of network transactions, and n represents the number of transactions completed by node i. f indicates whether the transaction was successful. If the transaction was successful, f is 1; if the transaction failed, f is -1. Through this positive and negative feedback on the completion of transactions, nodes can be better distinguished.

Definition 4: The formula for calculating the final mixed value of a node is as follows:

$$V(i)=\frac{1}{3}\left(xC(i)+yT(i)+value_k\right)$$
$$=\left(60x\left[1-\left(\frac{C(i-1)'}{C_{\min}}\right)^3\right]+60y\left(\frac{1}{m}\sum_{i=1}^{n}f_i\right)\right. \tag{8}$$
$$\left.+z*\sum_{N=1}^{20}\left(value_{ks_i}\times W_{V_i}\right)\right)$$

Among them, x is the weight of the node's credit value ratio, y is the weight of the node's own transaction success rate, and z is the weight of the performance value. Let $x+y+z=1$. The mixed value intuitively reflects the comprehensive performance of the node.

II. C.Blockchain-based intelligence trading and sharing

II. C. 1) Access Control and Transaction Requests

When a node wishes to request intelligence resources, it can query the locally stored data chain backup based on intelligence feature descriptions and intelligence pricing information. Once the required intelligence resources are identified, the node can send a data request to the provider based on the provider ID and reach a transaction consensus. The intelligence owner then submits the transaction request to the shared platform for review and approval. Additionally, intelligence service providers can query intelligence requests submitted by requesters. When a suitable intelligence request is found, they can communicate with the other party using the provider ID to negotiate terms (such as transaction time and price), and after reaching a transaction consensus, the intelligence service provider submits the transaction request to the shared platform for review and approval.

II. C. 2) Establishment of the transaction chain

The shared platform is responsible for collecting and aggregating transaction requests submitted by intelligence owners during the consensus cycle, including transaction time, data summaries of transaction intelligence, signatures of intelligence providers, signatures of intelligence purchasers, transaction prices, delivery formats, and other information. The on-duty node writes each submitted application into the transaction record during the consensus cycle, generates a Merkel value, packages it into a block, and stamps it with a timestamp. The block is then broadcast within the community, and approved blocks are added to the end of the transaction chain.

III. Experimentation and analysis of intelligence sharing mechanisms

III. A. Performance Analysis

III. A. 1) Program Overhead

The main computational overhead of this scheme is concentrated in two aspects: the computational overhead of the ciphertext policy attribute encryption algorithm and the execution cost of the corresponding smart contract algorithm calls. To this end, this paper simulates the scheme process in an actual physical environment and calculates the actual overhead of each stage to evaluate the scheme's performance.

First, regarding the computational overhead of the ciphertext strategy attribute encryption algorithm, an improved PBFT consensus algorithm was used to implement data encryption/decryption algorithms and data key generation algorithms. Under identical physical conditions, key generation and content confidentiality key encryption/decryption operations were performed. The computational overhead was calculated by averaging the results of 200 experiments with an interval of 7 attributes. The runtime under different attribute counts is shown in Figure 3. As the number of attributes increases, the corresponding intelligence data encryption time and intelligence consumer attribute key generation time exhibit a linear growth trend. When the number of user attributes in the scheme reaches a maximum of 42, the encryption computation time is approximately 183.4 ms, the key generation time is approximately 226.7 ms, and the decryption time is approximately 40.9 ms. The time consumption remains within a reasonable range and can meet practical application requirements.

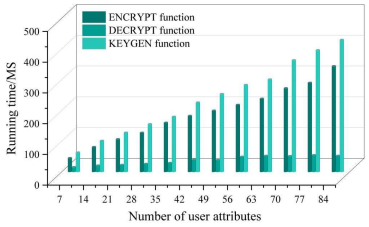


Figure 3: Running Time under Different Numbers of Attributes

To simulate the actual costs associated with each stage of the intelligence-sharing scheme, we calculated the execution costs of various algorithms within the smart contract. Using Remix-IDE as the development platform, we wrote the smart contract using the Solidity smart contract programming language. We deployed and tested the contract on the Ropsten blockchain test network via the MeatMask blockchain wallet, obtaining the gas consumption of the program and calculating the corresponding actual consumption. The corresponding costs for the relevant operations of the smart contract described in the scheme are shown in Table 1 below. This simulation uses the ETH price on August 15, 2024, as the standard, where the actual Gas consumption equals the product of the consumed Gas quantity and the Gas unit price (Gwei). The results indicate that this scheme has relatively low consumption in terms of smart contract execution costs.

Table 1: Smart Contract Costs

Smart contract operation	Gas consumption/ Gwei	ETH consumption/ unit	Actual cost/ dollar
DsharesignContract Create	1295664	0.001186332	4.018633566
userinfoset	101375	0.000097253	0.297514657
datainfoset	197863	0.000198366	0.718546638
DIdentityContract Create	1138565	0.001353231	3.093752415
sethistory	137543	0.000136432	0.501856414
updatehistory	89936	0.000083986	0.318645243
getfrequentinfo	127535	0.000153642	0.397515862
InfoTranContract Create	937521	0.000893754	3.017545674
setskinfo	146342	0.000201756	0.501864663

III. A. 2) Node Reliability

Assuming that an attacker mimics the behavior of normal contributors, in order to disguise themselves as ordinary users, attackers need to participate in consensus normally. These normal behaviors are used as the cost of executing malicious actions, thereby maintaining the node reliability required for the attacker to sustain their attacks.

Therefore, we conducted simulation experiments to demonstrate the impact of the attacker's attack costs under malicious behavior in cycle t. In this section of the experiment, three types of nodes were simulated: normal contributing nodes with no malicious behavior, i.e., t=0; cautious malicious nodes that perform a malicious attack every 10 rounds and contribute normally the rest of the time to disguise themselves, i.e., t=9; and reckless malicious nodes that perform a malicious attack every two rounds and contribute normally the rest of the time, i.e., t=3. In terms of initial value selection, after comparing the results of multiple experiments, the reliability change d was set to 0.02. At this value, the amplitude of node reliability changes is moderate, avoiding nodes converging too quickly toward the peak value of 1 or being prematurely excluded from the consensus set due to excessive changes, which aligns with the design expectations and scenario requirements of this paper. Depending on the value of the penalty coefficient p, the change trends of the two types of malicious nodes also differ. To better align with real-world data, Gaussian noise (m=0, s.d=0.01) was introduced, where m is the mean and s.d is the standard deviation. In the experiments, if a node's reliability reaches 0, it no longer changes. The experimental results under different penalty coefficients are shown in Figure 4 (a–b).

In the figure, when p = 10, although the reckless-type malicious nodes quickly drop to 0, the cautious-type malicious nodes are not identified, and their reliability reaches 1 only after 95 rounds of consensus. When p is 20, the reliability of reckless malicious nodes rapidly drops to 0, and the reliability of cautious malicious nodes also reaches 0 after 60 rounds. The experimental results indicate that under high p values, this method can effectively identify both types of malicious nodes and cause their reliability to rapidly approach 0.

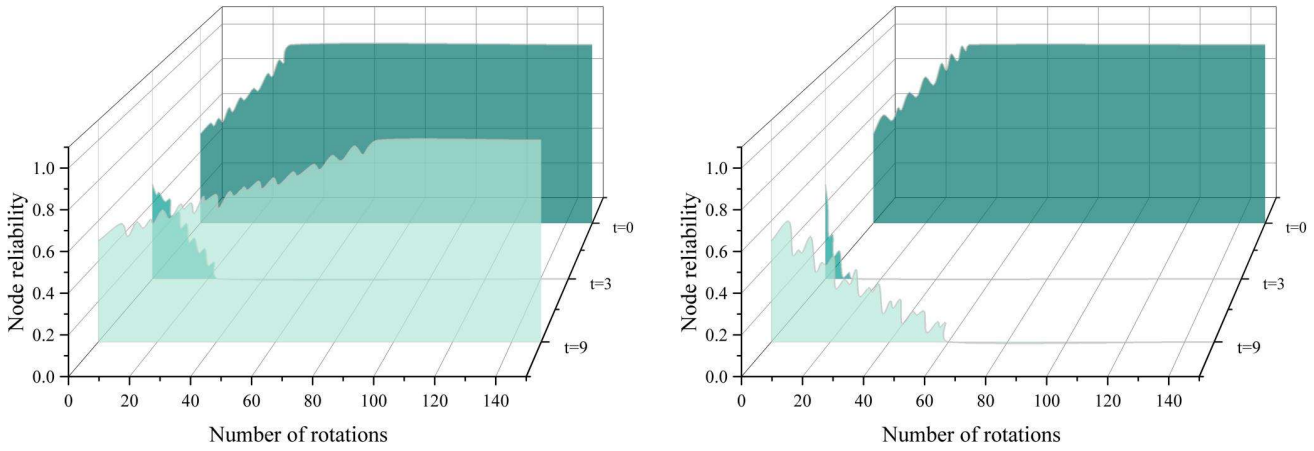
III. A. 3) Consensus Fault Tolerance Performance

To address the issue of low fault tolerance in the PBFT algorithm, where consensus cannot be reached normally once the number of Byzantine nodes exceeds 33%, this solution adopts an improved PBFT consensus algorithm. Through simulation experiments, it has been proven that the system can effectively exclude malicious nodes from the consensus set, thereby enhancing the fault tolerance performance of the improved PBFT consensus.

Since the message complexity of the improved PBFT consensus increases exponentially with the number of nodes, the experiment selected a blockchain network with 200 nodes when setting the number of nodes. The number of Byzantine nodes in the consensus scheme is shown in Figure 5. In an initial blockchain system with 200 nodes, there are 68 marked Byzantine nodes, including 35 cautious malicious nodes and 33 reckless malicious nodes. After 20 consensus rounds, only 4 marked Byzantine nodes remain in the consensus set.

It can be observed that as the number of consensus rounds increases, this scheme gradually excludes Byzantine nodes from the consensus set. Moreover, this scheme not only rapidly identifies and excludes unmasked reckless

malicious nodes but also, after a certain number of consensus rounds, can identify cautious malicious nodes that disguise themselves as normal nodes to perform malicious actions, significantly enhancing the fault tolerance performance of the consensus algorithm.



(a) p=10 (b) p=20

Figure 4: Experimental results under different penalty coefficients

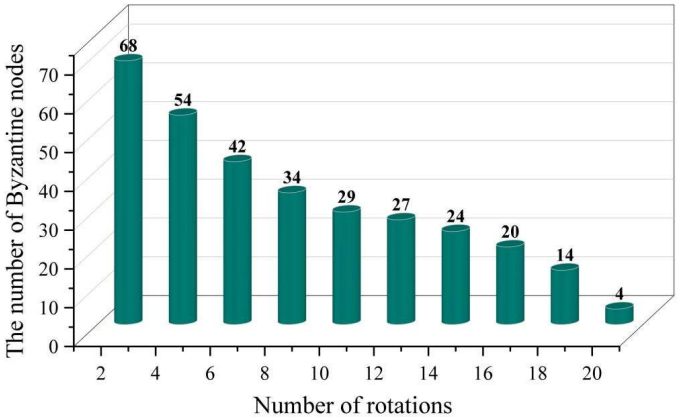


Figure 5: The number of Byzantine nodes in the consensus scheme

III. B. Evolutionary Game Simulation Analysis

Since the mechanisms by which certain parameters influence the shared game system are similar, this paper employs the method of taking partial derivatives for their analysis, with no errors present. Therefore, the following sections will not conduct detailed numerical simulations for each parameter; instead, similar parameter groups will be represented by a single example.

Selecting parameter values where the difference between the shared benefits and speculative benefits of cross-border cooperation between Country A and Country B is greater than 0, the evolutionary game process of national intelligence sharing is shown in Figure 6. Specifically, when the probabilities of countries A and B choosing to share intelligence are 0.4 and 0.3, respectively, at t = 0.035, both countries ultimately choose to share intelligence, meaning the shared game system stabilizes at (1,1). Next, numerical simulations are conducted on the relevant influencing factors in the game system. By altering the numerical values of these factors, the strategy choices of the two parties and the overall stability of the system are observed.

By adjusting the value of the cooperative benefit coefficient and setting multiple comparison values ((70, 70), (100, 100), (10, 10), and (30, 30)), the evolutionary game process of cooperative benefits is shown in Figure 7, where the letter A represents Country A and the letter B represents Country B. When the cooperative payoff of information sharing between Country A and Country B increases to (70,70), the slope of the corresponding curve also increases, indicating that in the information-sharing game system, the time required for both parties to ultimately choose the sharing strategy is shorter, and the system stabilizes more quickly at (1,1). When it increases to (100,100), the slope

approaches positive infinity, and both sides choose the sharing strategy more quickly, ultimately stabilizing at (1,1). However, when the cooperative payoff of intelligence sharing between Country A and Country B decreases to (30,30), the slope of the corresponding curve is less than 0. At this point, both sides choose not to share information as the optimal strategy, and the sharing game system ultimately stabilizes at (0,0). When reduced to (10,10), the slope approaches negative infinity, indicating that both parties more quickly choose the non-sharing strategy, and the system ultimately stabilizes at (0,0). Therefore, the larger the intelligence sharing cooperative benefit coefficient between the two parties, the higher the benefits obtained through intelligence sharing, and the more it promotes national intelligence sharing. The principle of the penalty coefficient is entirely consistent with that of the cooperative coefficient; thus, the larger the penalty coefficient, the more it promotes both parties to choose intelligence sharing.

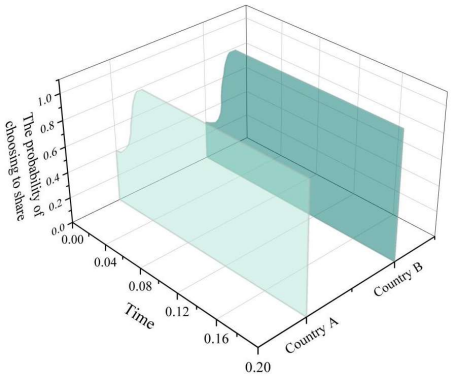


Figure 6: The Evolutionary Game Process of National Intelligence Sharing

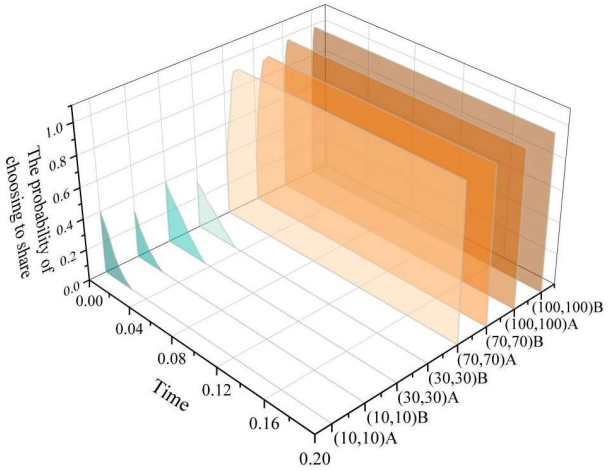


Figure 7: Evolutionary Process of Synergistic Benefits Game

IV. Conclusion

This paper addresses the issue of intelligence sharing in cross-border law enforcement by proposing a multi-layered, multi-technology integrated solution.

When the number of user attributes reaches a maximum of 42, the encryption computation time is approximately 183.4 milliseconds, the key generation time is approximately 226.7 milliseconds, and the decryption time is approximately 40.9 milliseconds. These time consumptions are within normal ranges and can meet practical application requirements. Under high p-value conditions, the solution can effectively identify two types of malicious nodes and rapidly reduce their node reliability to 0. In a blockchain network with 200 nodes, after 20 rounds of consensus, only 4 marked Byzantine nodes remain in the consensus set, significantly enhancing the fault tolerance performance of the consensus algorithm.

When the probabilities of countries A and B choosing to share intelligence are 0.4 and 0.3, respectively, and t = 0.035, both countries A and B ultimately choose to share intelligence, meaning the intelligence-sharing game system stabilizes at (1,1). The larger the intelligence-sharing coordination benefit coefficient between the two parties, the higher the benefits obtained through intelligence sharing, thereby more effectively promoting national intelligence sharing. Similarly, the larger the penalty coefficient, the more it promotes both parties to choose intelligence sharing.

Funding

This work was supported by Jiangsu University Philosophy and Social Science Research Project (2021SJA0572); Safety Capacity Construction Project of Chinese Civil Aviation Administration "Research on the Control of Overseas Terror-related Safety Risks in Civil Aviation in China".

References

[1] DERVIŞ, K. (2019). International cooperation and global governance. PRODUCTIVE EQUITY, 233.
[2] Acharya, A., Estevadeordal, A., & Goodman, L. W. (2023). Multipolar or multiplex? Interaction capacity, global cooperation and world order. International Affairs, 99(6), 2339-2365.
[3] Enderwick, P. (2019). Understanding cross-border crime: the value of international business research. critical perspectives on international business, 15(2/3), 119-138.
[4] Filippov, S. (2017). The Borders Barrier Properties vs Cross-Border Criminality. Law Rev. Kyiv UL, 245.
[5] Minnaar, A. (2022). Border security: An essential but effective tool in combatting cross-border crime. In The Handbook of Security (pp. 357-378). Cham: Springer International Publishing.
[6] Folami, O. M., & Naylor, R. J. (2017). Police and cross-border crime in an era of globalisation: The case of the Benin–Nigeria border. Security Journal, 30(3), 859-879.
[7] Lisakafu, J. (2020). Interregionalism and police cooperation against cross-border crime in East Africa: Challenges and prospects. Broadening the Debate on EU–Africa Relations, 115-131.
[8] Bernasco, W., Lammers, M., & van der Beek, K. (2016). Cross-border crime patterns unveiled by exchange of DNA profiles in the European Union. Security journal, 29(4), 640-660.
[9] Filippov, S. (2018). Information support for counteraction to cross-border crime. Visegrad Journal on Human Rights, 2(4), 102-112.
[10] Heusala, A. L., & Koistinen, J. (2018). 'Rules of the game'in cross-border cooperation: legal-administrative differences in Finnish–Russian crime prevention. International Review of Administrative Sciences, 84(2), 354-370.
[11] Ojiakor, N., Nzewi, L. C., & Arize, B. C. (2021). Effects of Cross Border Crimes on Security in Nigeria: A Focus on Seme Border, 2007-2015. Interdisciplinary Journal of African & Asian Studies (IJAAS), 7(1).
[12] Mahida, A. (2020). Cross-Border Financial Crime Detection-A Review Paper. International Journal of Science and Research(IJSR), 9(4), 1808-1813.
[13] Malechi, A. S., & Mathias, B. A. (2021). Patterns of cross-border crimes in Idiroko border community of Ogun State, Nigeria. International Journal of Health and Social Inquiry, 7(1).
[14] Davies, G. (2021). Facilitating cross-border criminal justice cooperation between the UK and Ireland after Brexit:'Keeping the lights on'to ensure the safety of the Common Travel Area. The Journal of Criminal Law, 85(2), 77-97.
[15] Hufnagel, S., & McCartney, C. (2014). Police cooperation against transnational criminals. In Routledge handbook of transnational criminal law (pp. 107-120). Routledge.
[16] Meško, G., & Furman, R. (2014). Police and prosecutorial cooperation in responding to transnational crime. Handbook of transnational crime and justice, 323-352.
[17] Sallavaci, O. (2018). Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange. European Journal on Criminal Policy and Research, 24(3), 219-235.
[18] Legrand, T., & Leuprecht, C. (2021). Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy. Policy and Society, 40(4), 565-586.
[19] Lemieux, F. (2018). Police cooperation across jurisdictions. In Oxford Research Encyclopedia of Criminology and Criminal Justice.
[20] Cozine, K., & Sundberg, K. W. (2025). The evolution of law enforcement and intelligence cooperation between Canada and the United States. In The Elgar Companion to North American Trade and Integration (pp. 335-351). Edward Elgar Publishing.
[21] Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.
[22] Cocq, C. (2015). Development of regional legal frameworks for intelligence and information sharing in the EU and ASEAN. Tilburg Law Review, 20(1), 58-77.
[23] da Cruz, J. D. A. (2019). Intelligence sharing among agencies and internationally. In Online Terrorist Propaganda, Recruitment, and Radicalization (pp. 389-400). CRC Press.
[24] Cocq, C. C. (2024). Sharing Data with Peers from the Same Region: A Matter of Mutual Trust. In Mutual Trust in Regional and Interregional Cooperation on Counterterrorism: EU and ASEAN Approaches (pp. 245-318). Cham: Springer Nature Switzerland.
[25] Ballaschk, J. (2015). In the unseen realm: transnational intelligence sharing in the European Union-Challenges to fundamental rights and democratic legitimacy. Stan. J. Int'l L., 51, 19.
[26] Esparza, D., & Bruneau, T. C. (2019). Closing the gap between law enforcement and national security intelligence: Comparative approaches. International Journal of Intelligence and CounterIntelligence, 32(2), 322-353.
[27] Brown, R. (2018). Understanding law enforcement information sharing for criminal intelligence purposes. Trends and Issues in Crime and Criminal Justice, (566), 1-15.
[28] Moses, L. B. (2020). Who owns information? Law enforcement information sharing as a case study in conceptual confusion. UNsWLJ, 43, 615.
[29] Phythian, R., Kirby, S., & Swan-Keig, L. (2024). Understanding how law enforcement agencies share information in an intelligence-led environment: how operational context influences different approaches. Policing: An International Journal, 47(1), 112-125.
[30] Aden, H. (2020). Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union. In Secrecy in European Politics (pp. 157-178). Routledge.
[31] Ghani, I. (2018). Intelligence collaboration between law enforcement, military and national security agencies in Pakistan. Pakistan Journal of Criminology, 10(4), 135-149.

[32] Li, A., & Chen, Y. (2017, June). Research on Sino-US Cybersecurity Law Enforcement Cooperation From the Perspective of International Law Enforcement Cooperation. In 2nd International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2017) (pp. 1058-1062). Atlantis Press.
[33] Arakelian, M., Behruz, H., & Biriukov, R. (2025). INTERNATIONAL CO-OPERATION OF LAW ENFORCEMENT BODIES OF STATES IN THE SPHERE OF ENSURING ECONOMIC SECURITY. Baltic Journal of Economic Studies, 11(2), 104-111.
[34] Hufnagel, S. (2020). Regulation of cross-border law enforcement:'locks' and 'dams' to regional and international flows of policing. In The Policing of Flows (pp. 54-72). Routledge.
[35] Luchtman, M. (2020). Transnational law enforcement cooperation–fundamental rights in European cooperation in criminal matters. European Journal of Crime, Criminal Law and Criminal Justice, 28(1), 14-45.
[36] Sadoff, D. A. (2017). How law enforcement cooperation abroad is pivotal to sustainable development at home. BU Int'l LJ, 35, 337.