UDC 004.75

Микита Меленчуков, Артем Волокита

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ТА АТАК У РОЗПОДІЛЕНИХ СИСТЕМАХ

Mykyta Melenchukov, Artem Volokyta

ANALYSIS OF DEFENSE AND ATTACK METHODS IN DISTRIBUTED SYSTEMS

Робота присвячена аналізу вразливостей розподілених систем та класифікації методів атак на них. Розглянуто основні рівні загроз: від контролю доступу та транспортування даних до складних Collusion attacks, таких як атаки Sybil та Eclipse. Описано методи захисту, що включають механізми автентифікації, безпечного зберігання та маршрутизації.

Ключові слова: розподілені системи, інформаційна безпека, атака Sybil, атака Eclipse, контроль доступу, маршрутизація.

Рис.: 1. Бібл.: 5.

The work is devoted to the analysis of vulnerabilities in distributed systems and the classification of attack methods against them. The main threat levels are considered: from admission control and data transportation to complex collusion attacks, such as Sybil and Eclipse attacks. Defense methods including authentication mechanisms, secure storage, and secure routing are described.

Keywords: distributed systems, information security, Sybil attack, Eclipse attack, admission control, routing.

Fig. 1. Bibl: 5

Relevance of the research topic. Distributed systems, composed of multiple nodes providing services to users, have become the backbone of modern IT infrastructure due to their ability to scale, handle distributed information resources effectively, and provide high reliability and fault tolerance. However, the complexity of these systems creates numerous entry points for malicious actors. Ensuring the security of data and services in such an environment is a critical task, making the analysis of potential threats and defense mechanisms highly relevant.

Target setting. Systematization of knowledge regarding vulnerabilities in distributed systems, classification of specific attacks (including collusion attacks), and determination of effective mitigation strategies to ensure confidentiality, integrity, and availability.

Actual scientific researches and issues analysis. Recent studies in the field of distributed systems security focus on specific vectors of attacks. Theoretical foundations of attacks on reputation systems, such as the Sybil attack, were described by J.R. Douceur [1]. Issues of routing security and "Eclipse" type attacks are widely discussed in the context of peer-to-peer networks and blockchain systems [2]. However, a comprehensive overview connecting basic infrastructure vulnerabilities with complex social-engineering and routing attacks requires constant updating due to the evolution of threats.

Uninvestigated parts of general matters defining. While individual attacks are well-studied, there is a need for a consolidated analysis that links vulnerabilities in admission control and data transport with complex scenarios like "White washing" and routing table poisoning, along with a unified approach to defense.

The research objective. To analyze the main vulnerable points of distributed systems (admission, transport, synchronization, data security), examine the mechanism of collusion attacks, and formulate the main methods for mitigating these threats.

The statement of basic materials. A distributed system is defined by its composition of multiple nodes working together to provide services. Its main benefits—scaling and fault tolerance—rely on the correct interaction of these nodes. However, several critical areas are susceptible to attacks. The first vulnerable area is Admission Control, which governs authorized access to data and services. Potential threats here include acquiring access to protected data by masquerading or spoofing identity, as well as Denial of Service (DoS) attacks that exhaust system resources.

The second area is Data Transportation, the process of moving data between components across communication channels. Threats include data modification and unauthorized listening or interception. A classic example is the Man-in-the-Middle (MitM) attack, where the attacker secretly relays and possibly alters the communications between two parties.

The third area involves the Organization and Synchronization of resources. Threats here lead to inadequate resource distribution, data inconsistencies, and time/event ordering issues. Specific attacks include Pollution attacks (index poisoning), which undermine system integrity by introducing false information, leading to service disruption.

The fourth area is Data Security itself, covering confidentiality, integrity, and availability. Threats include data leakage via side-channel or covert channel attacks, delays in access affecting availability, and direct compromise of integrity.
A significant category of threats in distributed systems is Collusion Attacks. These involve a group of peers working together to compromise the network targeting control mechanisms like reputation or bandwidth provisioning. Key types include:

1. Sybil Attack: An attacker undermines the reputation system by creating numerous pseudonymous identities, gaining exaggerated influence [1].
2. Eclipse Attack: Attackers surround a good peer with malicious nodes, blocking its view of the system to facilitate spoofing or censorship [2].
3. White Washing: Malicious peers illicitly alter or delete data to reset their bad reputation, leaving and rejoining the system as "new" users [3].

4. Routing Attacks: Aim to disrupt availability. Examples include Routing Table Poisoning (RTP) and Attraction/Repulsion attacks, which alter peer attractiveness during routing tasks (Fig. 1).

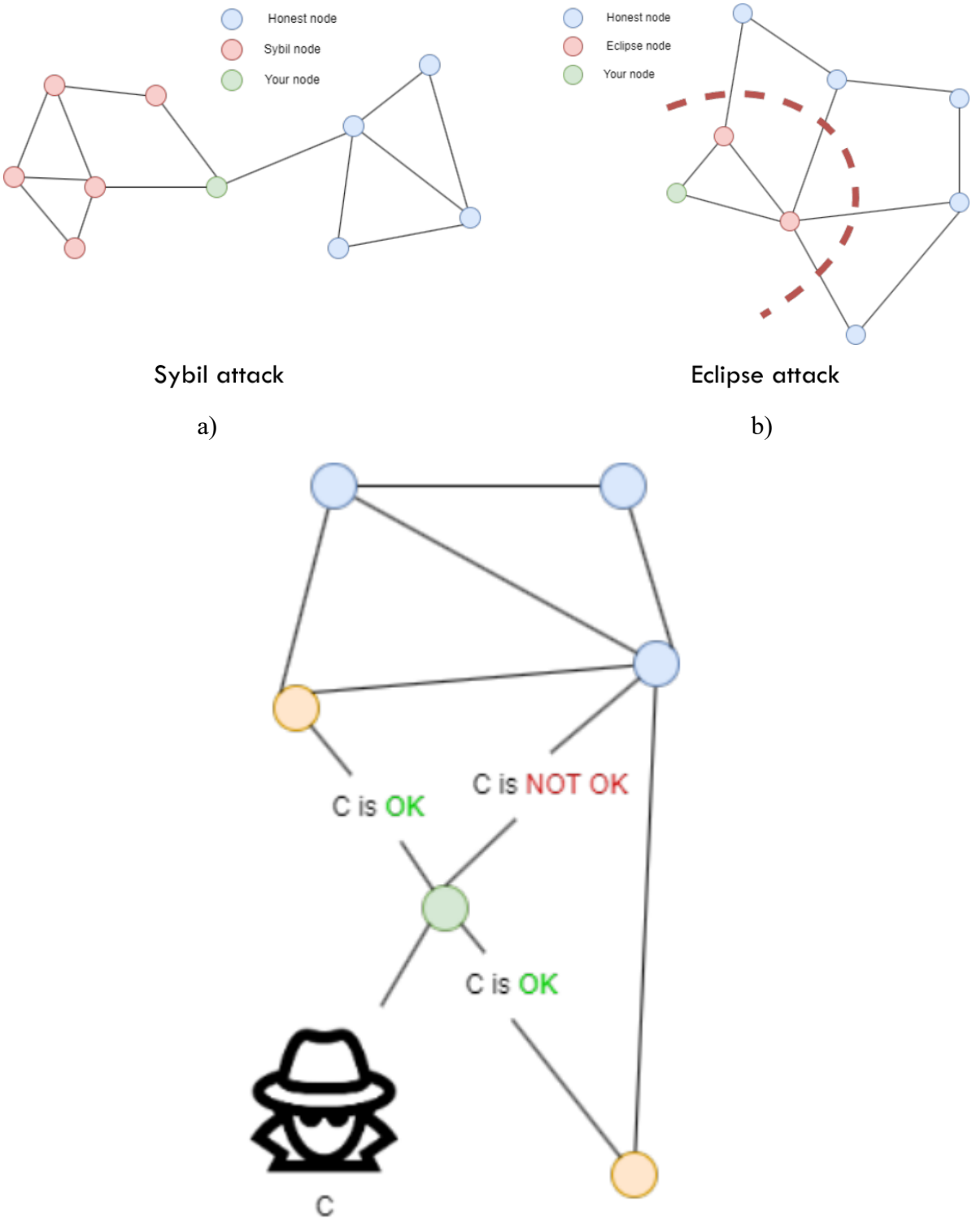

Fig. 1. Schematic representation of attacks: a – Sybil attack (one node controlling multiple identities); b – Eclipse attack (isolation of a target node)

To mitigate these attacks, three main mechanisms are used:

1. Authentication Mechanism: Helps maintain a low number of malicious peers. To mitigate Sybil and Eclipse attacks, a centralized authority can be utilized for managing peer enrollments. Alternatively, assigning certificates issued by a common Certificate Authority (CA) to network IDs during the joining process is effective [4].
2. Secure Storage: Prevents attackers from modifying information through cryptographic checks and redundancy.
3. Secure Routing: Mitigated by limiting the number of trusted routing paths and adding cryptographic overhead to verify the path integrity [5].

Conclusions. Security in distributed systems requires a multi-layered approach. While basic threats target data transport and access control, the most dangerous attacks involve node collusion (Sybil, Eclipse) and manipulation of routing logic. Effective defense relies on strong authentication infrastructure (PKI, Centralized Authorities) and secure routing protocols to ensure data integrity and system availability.

References

1. Douceur J. R. The Sybil Attack. Peer-to-Peer Systems. IPTPS 2002. Lecture Notes in Computer Science. 2002. Vol 2429. P. 251–260. URL: https://doi.org/10.1007/3-540-45748-8_24.

2. Heilman E., Kendler A., Zohar A., Goldberg S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. 24th USENIX Security Symposium. 2015. P. 129–144.

3. Feldman M., Papadimitriou C., Chuang J., Stoica I. Free-riding and whitewashing in peer-to-peer systems. IEEE Journal on Selected Areas in Communications. 2006. Vol. 24, no. 5. P. 1010–1019.

4. Coulouris G., Dollimore J., Kindberg T., Blair G. Distributed Systems: Concepts and Design. 5th Edition. Addison-Wesley, 2011. 1063 p.

5. Hu Y. C., Perrig A., Johnson D. B. Rushing Attacks and Defense Strategies in Wireless Ad Hoc Network Routing. WiSe ’03. 2003. P. 30–40.

ДОВІДКА ПРО АВТОРІВ

Меленчуков Микита Євгенович – аспірант, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Melenchukov Mykyta – PhD student, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: melenchukov.nikita@gmail.com

Волокита Артем Миколайович – кандидат технічних наук, доцент кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Volokyta Artem – Candidate in Technical Sciences, Associate Professor, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: artem.volokita@kpi.ua

РОЗШИРЕНА АНОТАЦІЯ

Микита Меленчуков, Артем Волокита

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ТА АТАК У РОЗПОДІЛЕНИХ СИСТЕМАХ

Актуальність теми дослідження. Розподілені системи є основою сучасних обчислень, забезпечуючи масштабованість та відмовостійкість. Проте їхня архітектура створює нові вектори загроз, які вимагають детального аналізу для побудови надійного захисту.

Постановка проблеми. Необхідність класифікації вразливих місць розподілених систем (контроль доступу, транспорт, синхронізація) та аналіз методів протидії атакам типу Collusion та Routing attacks.

Аналіз останніх досліджень та публікацій. Дослідження базується на класичних та сучасних роботах у сфері безпеки P2P мереж та розподілених обчислень, зокрема щодо атак Sybil та Eclipse.

Постановка завдання. Проаналізувати основні загрози конфіденційності, цілісності та доступності даних у розподілених системах та визначити ефективні методи захисту.

Викладення основного матеріалу. У роботі детально розглянуто чотири основні вразливі зони: контроль доступу (загрози спуфінгу та DoS), транспортування даних (загрози перехоплення та модифікації, атаки Man-in-the-Middle), організація ресурсів (атаки Pollution attacks або index poisoning) та загальна безпека даних (витоки через сторонні канали).

Окрему увагу приділено атакам типу Collusion attacks, коли група вузлів діє спільно для компрометації системи. Проаналізовано атаку Sybil (створення безлічі псевдонімів), атаку Eclipse (ізоляція чесного вузла), White washing (відбілювання репутації) та атаки Routing Table Poisoning (отруєння таблиць маршрутизації).

Визначено, що основними методами захисту є впровадження суворих механізмів автентифікації (використання централізованих центрів сертифікації для запобігання атакам Sybil), криптографічний захист сховищ даних та використання захищених протоколів маршрутизації з обмеженням довірених шляхів.

Висновки. Забезпечення безпеки розподілених систем вимагає комплексного підходу, що поєднує криптографічні методи захисту каналів зв'язку з архітектурними рішеннями для протидії атакам на репутацію та топологію мережі.

Ключові слова: розподілені системи, інформаційна безпека, атака Sybil, атака Eclipse, контроль доступу, маршрутизація.