Network Topology Masking in Distributed Information Systems

Roman V. Maximov, Ilya I. Ivanov, Sergei R. Sharifullin

Shtemenko Krasnodar Higher Military School
Krasnodar, Russia
rvmaxim@yandex.ru; 7570745@mail.ru; sharifullinsr@mail.ru

***Abstract*—In modern computer networks, it is possible for attackers to determine information about the algorithms of the distributed information systems functioning. For this purpose, methods of active and passive network intelligence are used. Therefore, it is necessary to ensure the secure functioning of distributed information systems in public networks. In this work, we investigated the full range of threats to which networks are exposed. Then we developed a masker, efficient software for obfuscation the network topology in distributed information systems. The topology protection of distributed information systems from the abusive and malicious actions with network topology obfuscation is considered to be one of the particular tasks while implementing the concept of software-defined networks. In addition, we determined a method for selecting the best-masked topology based on the estimation of efficiency indexes. Our findings suggest a significant increase of the protection level in masked distributed information system by increasing the resource required for network intelligence to suppress nodes.**

Keywords—cyber-security; security threats; obfuscation; network intelligence; software-defined networks; dynamic topology; network security management; secure interconnection.

I. INTRODUCTION

Software solutions for different hardware platforms appear today to replace hardware solutions providing network interconnection and managing of network infrastructure. This approach reduces the cost of technical solutions and increases the flexibility of distributed network infrastructure. However, the technical complexity of software, amount of services and business processes also increase, which requires the using of the best practices and public standards [1, 2]. The transparency and the common architecture of distributed information systems (DIS) contradict the principles of protection and the attacker's counteraction. In addition, the concept of software-defined networks (SDN) is being actively developed, providing a separation of control plane and data plane [3-7]. The high level of automation demands the appropriate security level of information technologies being used.

The core of DIS architecture is TCP/IP protocol stack that provides the integration of communication services and high level of convergence in all digital communication systems components. The basis of DIS architecture is a set of the territorially distributed subnetworks linked over public networks (PN). The modern DIS consists of the following objects [8]:

- End user devices: workstations, software, databases, e-mail.
- Communication equipment: access points, hubs, gateways.
- Data channels: leased lines, virtual private networks.

Security of end user devices is implemented using technical measures (anti-virus protection systems, access control systems) and organizational measures (security policies, group policies). Communication equipment and communication channels are the most vulnerable component of DIS because they have access to both PN and to the internal network. The characteristics of the modern DIS are: (1) distributed structure interconnects remote subnetworks, (2) high-speed transmission based on Ethernet, (3) several external links over public networks, (4) increasing users' demands in services.

The use of the communication channels over PN to provide information interaction leads to the potential security threats. Common model of information threats (Fig. 1) can be represented as a set of remote control points connected over PN (under the administrative control of service providers) and attacker's equipment. An attacker is able to connect to PN in non-controlled area between the protectable subnetworks. The integration of DIS with PN increases the capabilities of an attacker to discover a functional and logical structure (topology) through monitoring with the use of well-known methods [9-11]. As a result, the probability of destructive actions realization on DIS increases. Define the DIS's security threats based on analysis of the modern DIS characteristics:

- Implementation threats: Core elements of DIS often use an unknown technological base; therefore, they contain embedded undocumented features.
- Exploitation threats: the service providers (SP) define routing and switching based on quality of service. SP provide virtual private network (VPN) services between remote subnets without processing at transit nodes. However, third party SPs can be used.

- Additional threats: there is the possibility of destructive actions with the use of wide arsenal of methods.

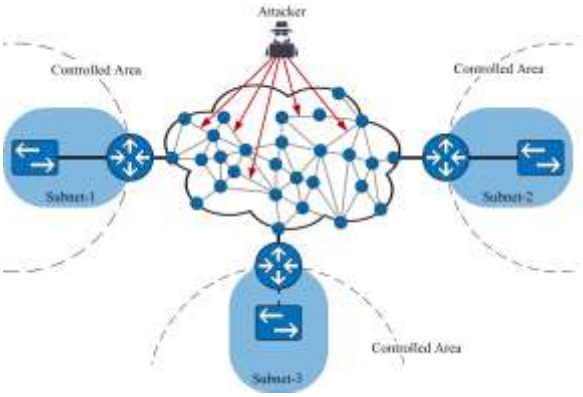

Fig. 1. Common model of information threats

The security problems that are successfully solved in small networks cannot be solved in the networks of a larger size, because of the high complexity of network designing and wide variety of attacks. Define the characteristics of large networks: (1) complicated topology, (2) low compatibility of network devices, (3) degradation of administrative zones' responsibility, (4) uncertainty of the source data about topology, (5) remote subnetworks.

These characteristics ensure a high vulnerability of large networks to various types of attacks (distributed attacks, in particular). Traditional security methods [12-18] are based on the use of firewalls and network filters, intrusion detection systems and security scanners, i.e. on the discovery of the abusive and malicious actions [19-21]. VPN services allow you to build dedicated networks based on a shared network infrastructure and thus implement a proactive security strategy. However, the security level provided by existing VPN protocols is not enough because they are based on link-layer technologies, which leads to potential security threats [22, 23]: (1) VLAN hopping, (2) MAC spoofing, (3) DHCP spoofing, (4) ARP spoofing.

The widespread use of multiprotocol label switching in VPN implementation expands the potential threats pool:

- Traffic encryption is not used.
- Inside attacks, including IP and Ethernet threats. It is possible to change the configuration of the routers after unauthorized access to equipment.
- Attacks through management network: SP often uses the management network to remote configuration and monitoring of equipment, which means external availability between control nodes and access nodes. Therefore, if the control nodes or the network infrastructure of SP is compromised, an attacker gains access to customer nodes.
- Indirect attacks. Edge routers usually provide services to several organizations. Therefore, attacks on them from the customer's network or from the PN may have an abuse adverse effect on the security or availability.
- Denial of service using TTL expiry. Situations of the TTL in customer's packages expiration may occur at the core router. In this case, the router discards the packet with the expired TTL and generates an ICMP response message to the source packet sender.
- IP option attacks. Packets with IP options are usually handled by a slow CPU and, therefore, can be used to attack transit routers. A stream of packets that have an alert label can adversely affect the core routers.
- Core routers overload. This leads to increased utilization of memory, processor capacity and bandwidth.

In addition, an attacker has wide opportunities to implement security threats bypassing protective mechanisms, because the fact of transmitting information on a compromised channel is transparent. Modern network intelligence tools allow to implement real-time traffic selection by defined characteristics (IP addresses of the sender and receiver, ports, the protocol used, etc.). Therefore, information about DIS topology is available to an attacker through the topology states attributes (TSA) even if there is no possibility to decode the selected information. In other words, it is possible to discover and build DIS topology model similarly to real DIS. Using this information, an attacker is able to implement abusive and malicious actions.

II. METHODOLOGY

In this section, we analyze performance indexes and suggest method for the best-masked topology selection. Then, we define main functions of masker and suggest addresses change algorithm.

To verify our hypotheses, we established masker in simulation network model and attacked the protected nodes by using Kali Linux tools. The experiment completes the evidence and establishes the validity of hypothesis.

A. Performance Indexes

Define the parameters of the topology as the coordinates of a multidimensional space. In this case, the real topology is described by the state vector $S(H_1 ... H_N)$, while $H_1 ... H_N$ are the parameters characterizing the properties of the DIS topology. The state vector S' describes the masked topology. If H_i and H'_i are the components of topology state vectors then the calculation of proximity measures between the real and masked topologies is carried out using Euclidean distance, since the use of other known proximity measures gives similar results:

$$R = \sqrt{\sum_{i=1}^{N} \left(H_i - H'_i \right)^2} \quad (1)$$

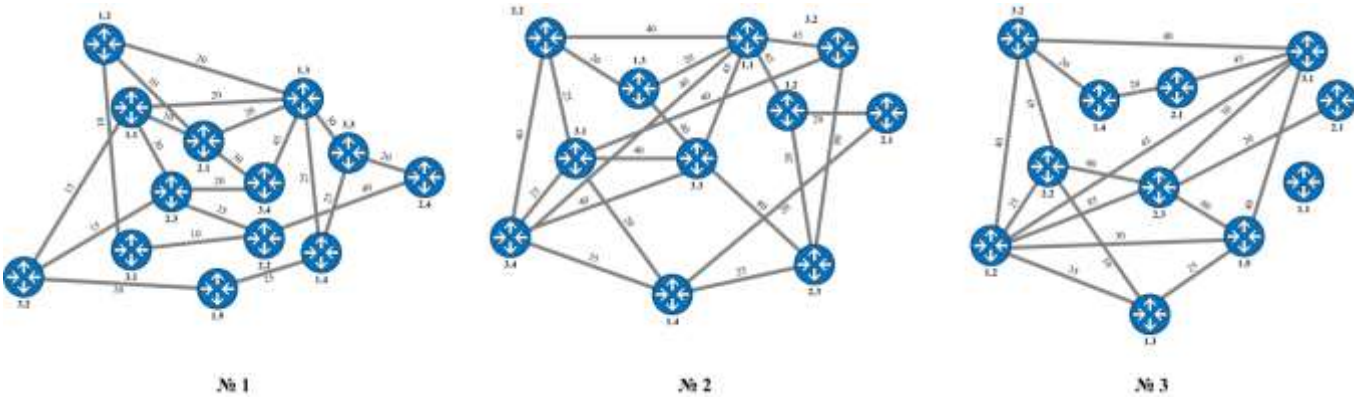

Fig. 2. Variants of changed topology

For each variant of the masked topology, the following performance indicators exist: (1) correlation index R_v without regard to the intensity of interconnection, (2) correlation index R'_v with regard to the intensity of interconnection.

When using the masker, a protected DIS topology is generated, as a result, the attacker will operate with false network nodes. To estimate the effectiveness of malicious attack preventing, we use the accessibility index of the protected node Q. If h_i is the importance factor and $k_i \in [0,1]$ is the state factor, then:

$$Q = [k_1, k_2, ..., k_N] = \sum_{i=1}^{N} h_i k_i \qquad (2)$$

If n is the cost for one address, N is the number of nodes, m is the cost for minimal unit of traffic and M is the intensity of interconnection then the total cost Z for the implementation of variant of the topology conversion include the following components:

$$Z = nN_j + mM_j \qquad (3)$$

Therefore, in order to choose the most acceptable topology structure (Fig. 2), it is necessary to solve the multicriteria optimization problem, which allows selecting the most effective variant of the transformation. The results for the estimation are presented in Table 1.

B. Masker

We build software, masker, to prevent network attacks. Masker runs on a standard Linux host but needs basic packet manipulation tool from repository: scapy. Scapy is used to capture, rebuild and send generated network packets.

Define main functions of system for masking network topology based on the analysis presented in the previous sections:

TABLE I. CALCULATION RESULTS FOR PERFORMANCE INDEXES

Performance index	Variant		
	1	*2*	*3*
R_v	0,887	0,481	0,618
R'_v	0,736	0,47	0,47
Q	0,9	0,78	0,5
Z	7830	7820	1830

- Reducing the influence of staff in DIS.
- Detection and recognition of abusive and malicious actions on the DIS.
- Reducing the negative impact of the protection system on the ordinary DIS functioning.

We developed software (masker) to implement these functions, which ensure masking communication links in distributed DIS by obfuscating their topology:

- Neutralization of abusive and malicious actions by reducing the availability of edge routers.
- Hiding the information about DIS topology by reducing TSA quality.
- Misinformation about the priority of communication links.

The masker extends the IP-address space by changing the source and destination values in IP-header in each package and synchronizes these changes between the routers involved in information exchange. Address changing algorithm has several steps:

- Reading the required parameters of the configuration file.
- Setting up IPTABLES rules.
- Creating an L3-socket for interaction on the internal interface.
- Starting a thread for intercepting, changing and forwarding IP packets on the internal interface of the masker.

Algorithm 1. Address changer

```
1:  F←OpenConfig(FILE);
2:  ConfigParametr P ← ReadNextConfigParametr(F);
3:  while ( P != NULL )
4:      SetConfigParametr(P);
5:      P ← ReadNextConfigParametr(F);
6:  SetRules(IptablesComand);
7:  S ← Socket();
8:  if P→Role == "Server"
9:      SendSynchronizationPacket(S);
10:     ReceiveConfirmationPacket(S);
11: else P→Role == "Client"
12:     ReceiveSynchronizationPacket(S);
13:     SendConfirmationPacket(S);
14: close(S);
15: S3 ← L3Socket(P→InEth);
16: S2 ← L2Socket(P→OutEth);
17: OpenThread(InterceptChangeResendFromInEth(S3));
18: OpenThread(InterceptChangeResendFromOutEth(S2));
19: OpenThread(ChangeIpConfig());
```

- Starting a thread responsible for intercepting, changing and forwarding IP-packets on the external interface of the masker.
- Synchronization based on sending a sync packet.
- Creating an L2-socket for interaction on the external interface.
- Starting a thread for intercepting, changing and forwarding IP packets on the internal interface of the masker.
- Starting a thread responsible for intercepting, changing and forwarding IP-packets on the external interface of the masker.
- Synchronization based on sending a sync packet.

The results can be effectively represented in the form of a vector diagram comparing the masked topologies (Fig. 3).

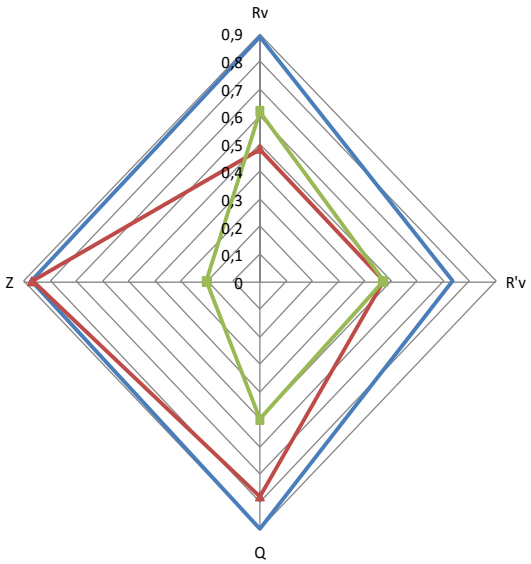

Fig. 3. Comparison diagram of masked topologies

III. Conclusion

The results of the work allow us to conclude that there is a significant increase protection level in distributed DIS, including the increasing attacker's investigation resources to implement abusive and malicious actions. For this, we used false network objects in the network structure, which form a masked topology. The structure of the masked topology deform the information received by attacker's network intelligence: (1) numbers of hosts, (2) software versions, (3) services, (4) interface identifiers. The masking process does not affect the interconnection between end-user nodes: it does not break the established TCP sessions and does not prevent the establishment of new ones.

Masker exhibit obfuscated network topology for incorrect reconstructing the structure of the protection DIS. Thus requires redundancy in the structure to reduce the informative of real interconnections, since structurally stationary DIS's topology is especially valuable for attacker's network intelligence.

Masker exhibit obfuscated network topology for incorrect reconstructing the structure of the protection DIS. Thus requires redundancy in the structure to reduce the informative of real interconnections, since structurally stationary DIS's topology is especially valuable for attacker's network intelligence.

References

[1] Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97 DOI: 10.1145/2799979.2799998.

[2] Opara E. U., Soluade O. A. Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities. In International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 10–18, 2015. DOI: 10.6636/IJEIE.201509.2(3).02.

[3] Cha, J. H., Han, Y. H., & Min, S. G. Named data networking over a Software-Defined Network using fixed-size content names. In IEICE Transactions on Communications, Vol. E99B, No. 7, 01.07.2016, p. 1455-1463.. DOI: 10.1587/transcom.2015EBP3464.

[4] You, L., Wei, L., Junzhou, L., Jian, J., Nu, X. An inter-domain multi-path flow transfer mechanism based on SDN and multi-domain collaboration. In in Proceedings of the 14th IFIP/IEEE International Symposium on Integrated Network Management (IM '15), 2017. pp. 758–761. DOI: 10.1109/INM.2015.7140369.

[5] P. Lin, J. Bi, and H. Hu, BTSDN: BGP-based transition for the existing networks to SDN. In Proceedings of the 6th International Conference on Ubiquitous and Future Networks (ICUFN '14), 2014. pp. 419–424. DOI: 10.1109/ICUFN.2014.6876826.

[6] D. Kreutz, F. M. V. Ramos, and P. Verissimo Towards secure and dependable software-defined networks. In Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN '13), 2013. pp. 55–60. DOI: 10.1145/2491185.2491199.

[7] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck Software defined networking for security enhancement in wireless mobile networks. In Computer Networks, 2014. pp. .94–101. DOI: 10. 1016/j.comnet. 2014.03.009.

[8] C. Fung, Y. L. Chen, X. Wang, J. Lee, R. Tarquini, and M. Anderson Survivability analysis of distributed systems using attack tree methodology. In IEEE Military Communications Conference

(MILCOM'05), pp. 583–589, 2005. DOI: 10.1109/MILCOM.2005.1605745.

[9] Behal, S., & Kumar, K. Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. In International Journal of Network Security, vol.19, no.3, pp.383-393, 2017. DOI: 10.6633/IJNS.201703.19(3).07.

[10] Hashemi, S.M. He, J. An Evolutionary Multi-objective Approach for Modelling Network Security. In International Journal of Network Security, vol.19, no.4, Pp.528-536, 2017. DOI: 10.6633/IJNS.201707.19(4).05.

[11] A. Behnia, R. A. Rashid, and J. A. Chaudhry A survey of information security risk analysis methods. In Smart Computing Review, vol. 2, no. 1, pp. 79–94, Feb. 2012. DOI: 10.6029/smartcr.2012.01.007.

[12] F. Amiri, M. M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, Feature selection for intrusion detection system using ant colony optimization. In International Journal of Network Security, vol. 18, no. 3, pp. 420–432, 2016. DOI: 10.1016/j.jnca.2011.01.002.

[13] Nezarat, A. Distributed Intrusion Detection System Based on Mixed Cooperative and Non-Cooperative Game Theoretical Model. In International Journal of Network Security, vol.20, no.1, pp.56-64, Jan. 2018. DOI: 10.6633/IJNS.201801.20(1).07.

[14] D. Singh, D. Patel, B. Borisaniya, and C. Modi Collaborative IDS framework for cloud. International Journal of Network Security, vol. 18, no. 4, pp. 699–709, 2016. DOI: 10.1007/978-94-007-2911-7_8.

[15] A. Tayal, N. Mishra and S. Sharma Active monitoring & postmortem forensic analysis of network threats: A survey. In International Journal of Electronics and Information Engineering, vol. 6, no. 1, pp. 49–59, 2017. DOI: 10.6636/IJEIE.201703.6(1).05.

[16] E. Popoola, A. O. Adewumi Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision. In International Journal of Network Security, vol. 19, no.5, pp. 660–669, 2017. DOI: 10.1145/2448556.2448566.

[17] A. Aziz, A. T. Azar, M. A. Salama, A. E. Hassanien, S. Hanafy Genetic algorithm with different feature selection techniques for anomaly detectors generation. In Proceedings of The Federated Conference on Computer Science and Information Systems (FedCSIS'13), pp. 769–774, Krakow, Poland, Sept. 2013.

[18] S. Elsayed, R. Sarker, J. Slay Evaluating the performance of a differential evolution algorithm in anomaly detection. In Proceedings of The Congress on Evolutionary Computation (CEC'15), pp. 2490–2497, Sendai, Japan, May 2015. DOI: 10.1109/CEC.2015.7257194.

[19] V. Jaganathan, P. Cherurveettil, P. M. Sivashanmugam Using a Prediction Model to Manage Cyber Security Threats. In Scientific World Journal, vol. 2015. DOI: 10.1155/2015/703713.

[20] E. T. Axelrad, P. J. Sticha, O. Brdiczka, and J. Shen A Bayesian network model for predicting insider threats. In Proceedings of the 2nd IEEE Security and Privacy Workshops (SPW '13), pp. 82–89, May 2013. DOI: 10.1109/SPW.2013.35.

[21] J. Wu, L. Yin, and Y. Guo Cyber attacks prediction model based on Bayesian network. In Proceedings of the 18th IEEE International Conference on Parallel and Distributed Systems (ICPADS '12), pp. 730–731, Singapore, December 2012. DOI: 10.1109/ICPADS.2012.117.

[22] Sheyner, J. Haines, S. Jha, R. Lippmann, J. M. Wing Automated generation and analysis of attack graphs. In Proceedings of the IEEE Symposium on Security and Privacy, pp. 273–284, May 2002. DOI: 10.1109/SECPRI.2002.1004377.

[23] L. Wang, A. Singhal, S. Jajodia Toward measuring network security using attack graphs. In Proceedings of the ACM Workshop on Quality of Protection, pp. 49–54, October 2007. DOI: 10.1145/1314257.1314273.