US 20250258911A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0258911 A1**

Guo (43) **Pub. Date: Aug. 14, 2025**

(54) **METHOD AND SYSTEMS FOR COVERT PATH DISCOVERING**

(71) Applicant: **Siemens Aktiengesellschaft**, München (DE)

(72) Inventor: **Dai Fei Guo**, Beijing, Hia Dian District (CN)

(73) Assignee: **Siemens Aktiengesellschaft**, München (DE)

(21) Appl. No.: **19/099,147**

(22) PCT Filed: **Jul. 28, 2022**

(86) PCT No.: **PCT/CN2022/108741**

§ 371 (c)(1),
(2) Date: **Jan. 28, 2025**

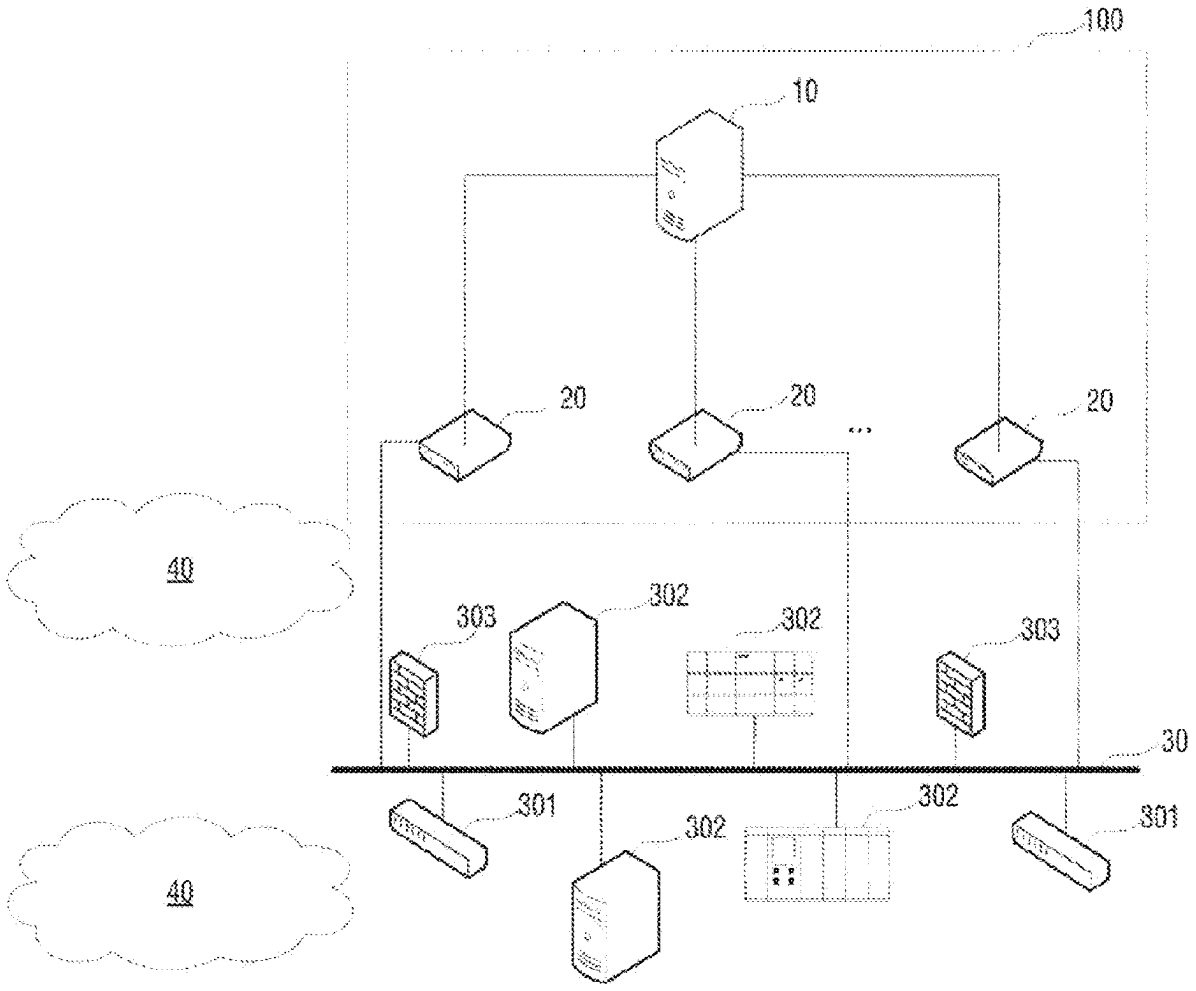
Publication Classification

(51) **Int. Cl.**
G06F 21/55 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/554*** (2013.01); *G06F 2221/034* (2013.01)

(57) **ABSTRACT**

Various embodiments of the teachings herein include a method for covert path discovering in OT security monitoring. An example includes: receiving IP configuration data of network connections among the OT network and an IT network connected to the OT network from a data collector connected to the OT network; identifying subnets among the OT network and the IT network based on the IP configuration data; determining different security zones among the OT network and the IT network based on the identified subnets; and discovering a covert path across a first identified subnet and a second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone.



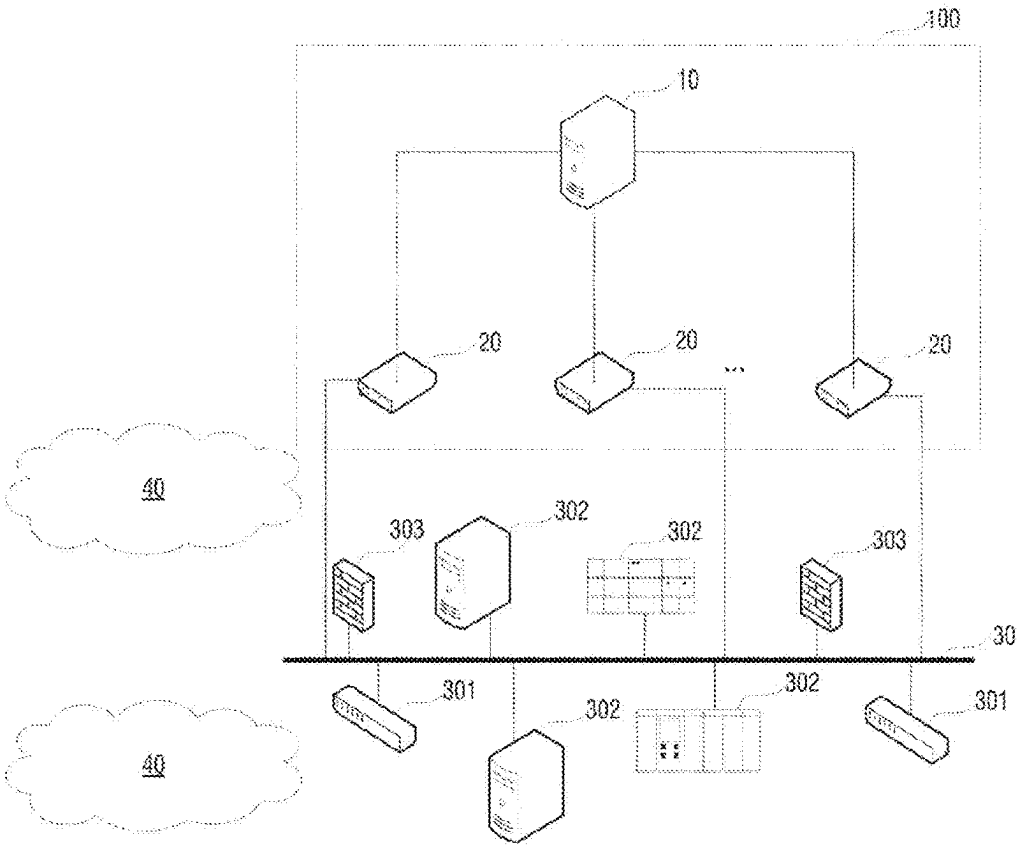


FIG.1

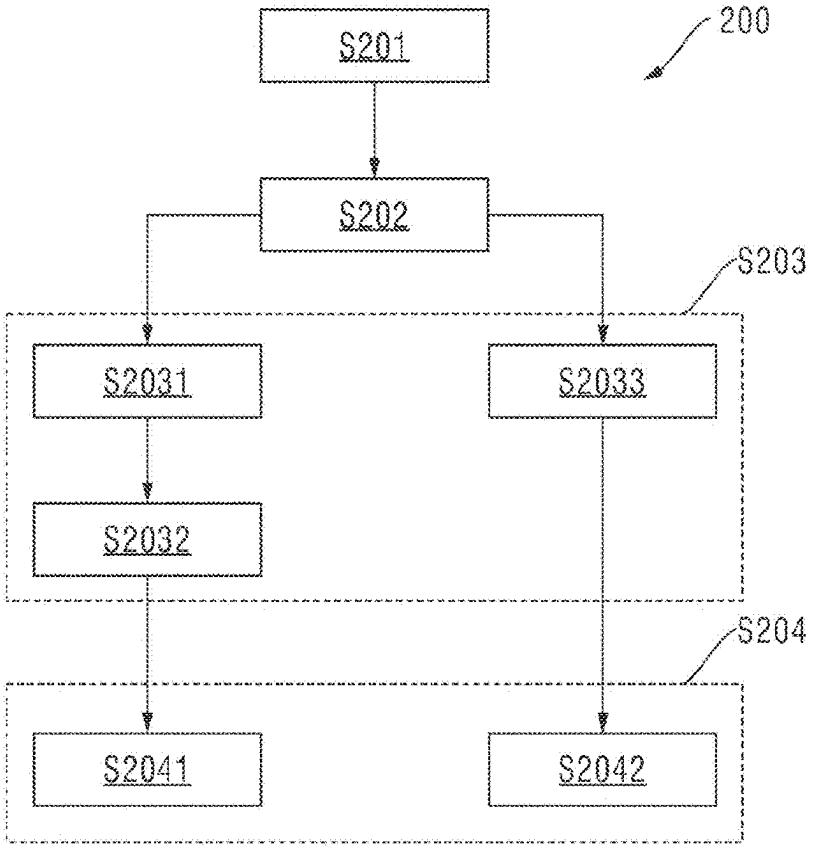


FIG. 2

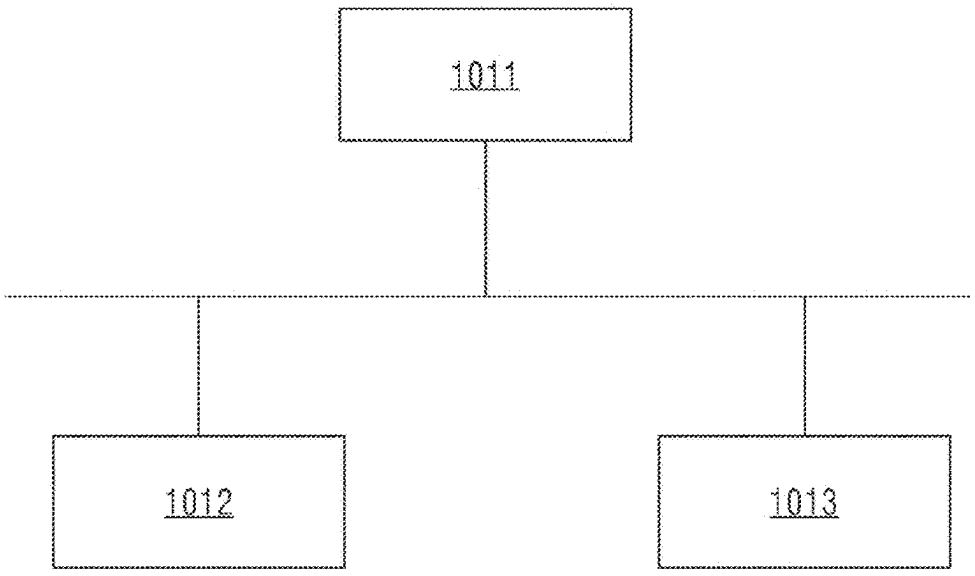


FIG. 3

METHOD AND SYSTEMS FOR COVERT PATH DISCOVERING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a U.S. National Stage Application of International Application No. PCT/CN2022/108741 filed Jul. 28, 2022, which designates the United States of America, the contents of which are hereby incorporated by reference in their entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to OT security monitoring. Various embodiments of the teachings herein includes methods and/or systems for covert path discovering in OT security monitoring.

BACKGROUND

[0003] In an industrial control system, industrial control devices work together to control industrial processes. Some of the industrial control devices, such as PLC, industrial hosts, working stations are connected via a network, which is usually called an OT (operational technology) network to differentiate from a traditional IT (information technology) network. With the development of industrial digitalization, OT networks and IT networks are more and more connected, which may expose OT networks to cyberattacks, malware intrusions and other kinds of threat from IT networks.

[0004] Security devices, such as firewalls, can isolate logically an OT network from an IT network. Physical isolation can also be applied to disrupt threats from the IT network. With security policies set on security devices, an OT network and connected IT network(s) can be divided into different security zones, devices in the same security zone can communicate with each other freely, while devices in different security zones cannot. However, such isolations may be bypassed via covert paths across different security zones. A covert path, otherwise known as covert channel or concealed channel, is a network connection across different security zones, which is unknown to the network management system or the network administrator. For example, a server with multiple network interface cards deployed on border of an OT network may cause potential access path from an IT network to the OT network. In addition, IoT (internet of things) devices used for data collecting may also create covert paths across production control systems in an OT network and monitoring system in an IT network. Covert paths are unknown by the network management system, which may bring great potential risk to the OT network.

SUMMARY

[0005] Teachings of the present disclosure include methods and systems for covert path discovering in OT security monitoring to find covert paths across different security zones among an OT network and at least one connected IT network.

[0006] As an example, some embodiments include a method for covert path discovering in OT security monitoring, which can be executed by a central OT security monitoring server. The central OT security monitoring server can be connected to at least one data collector and receive IP configuration data from the at least one data collector; the at least one data collector is connected to an OT network. The method can include: receiving IP configuration data of network connections from the at least one data collector, wherein the IP configuration data can be acquired by the at least one data collector from network flow data, IP configuration data of network interface cards installed on OT devices in the OT network and log of permitted communications in at least one security device in the OT network, etc.; identifying subnets among the OT network and at least one IT network connected to the OT network based on the IP configuration data; determining different security zones among the OT network and the at least one IT network based on the identified subnets; discovering at least one covert path across a first identified subnet and a second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone.

[0007] As an example, some embodiments include an apparatus for covert path discovering in OT security monitoring is provided, the apparatus can be implemented as software installed on the central OT security monitoring server, including modules to execute one or more of the methods described herein.

[0008] As an example, some embodiments include an apparatus for covert path discovering in OT security monitoring, which can be part of the central OT security monitoring server, or the central OT security monitoring server itself. The apparatus can include at least one memory, configured to store computer executable instructions; at least one processor, coupled to the at least one memory and upon execution of the computer executable instructions, configured to execute one or more of the methods described herein.

[0009] As an example, some embodiments include a system for covert path discovering in OT security monitoring, it can include at least one data collector connected to an OT network, configured to acquired IP configuration data of network connections among the OT network and at least one IT network connected to the OT network; a central security monitoring center connected with the at least one data collector, wherein the central security monitoring center can include one or more of the apparatus described herein.

[0010] As an example, some embodiments include a computer program product, which can be stored on a readable medium of an apparatus, and includes computer executable instructions, wherein the computer executable instructions, when executed, cause at least one processor to execute one or more of the methods described herein.

[0011] As an example, some embodiments include a computer-readable storage medium is provided, which stores computer executable instructions thereon, wherein the computer executable instructions, when executed, can cause at least one processor to execute one or more of the methods described herein.

[0012] IP configuration data of network connections can be received timely from the OT network via data collectors, subnets involved in the network connections can be acquired based on the IP configuration data. Based on whether the subnets involved in a network connection belong to the same security zone, potential covert path(s) between different security zones can be recognized as many as possible. Missing possible covert path can be avoided.

BRIEF DESCRIPTION OF DRAWINGS

[0013] To more clearly describe the teachings of the present disclosure, the accompany drawings to be used in the

description of the embodiments will be briefly introduced below. The accompanying drawings in the description below are merely some example embodiments disclosed in the embodiments of the present disclosure. For those of ordinary skills in the art, other drawings may also be obtained based on these drawings.

[0014] FIG. **1** is a schematic diagram of an example system for covert path discovering in OT security monitoring incorporating teachings of the present disclosure;

[0015] FIG. **2** is a flowchart of an example method for covert path discovering in OT security monitoring incorporating teachings of the present disclosure;

[0016] FIG. **3** is a schematic diagram of an example apparatus for covert path discovering in OT security monitoring incorporating teachings of the present disclosure.

Reference numerals in the figures

100: a system for covert path discovering in OT security monitoring		
10: a central security monitoring center	20: data collector	
30: OT network	40: IT network	
301: network device	302: OT device	303: security device
200: a method for covert path discovering in OT security monitoring		
S201: receiving IP configuration data of network connections		
S202: identifying subnets		
S203: determining security zones		
S2031: counting number of OT devices involved in network connections across two identified subnets		
S2032: determining the two identified subnets belong to different security zones, if the number of OT devices involved in network connections across the two identified subnets is less than a predefined threshold		
S2033: determining different security zones according to predefined relationship between security zones and their included subnets		
S204: discovering covert path(s)		
S2041: determining a network connection across the first identified subnet and the second identified subnet as a covert path if the network connection is not predefined as permitted by security policies in the OT network		
S2042: determining that a network connection across the first identified subnet and the second identified subnet is a covert path, wherein the first identified subnet belongs to the first determined security zone and the second identified subnet belongs to the second determined security zone		
101: an apparatus for covert path discovering in OT security monitoring		
1011: at least one memory	1012: at lest one processor	1013: communication module

DETAILED DESCRIPTION

[0017] The described embodiments are merely a part, instead of all, of the potential embodiments of the teachings of the present disclosure. All other embodiments obtained by those of ordinary skills in the art based on embodiments among the embodiments of the present disclosure shall fall within the scope of protection of the present disclosure. Specific implementations of the embodiments of the present disclosure will be further described below with reference to the accompanying drawings.

[0018] FIG. **1** shows an example system **100** for covert path discovering for an OT network incorporating teachings of the present disclosure. For the covert path analysis in the present disclosure is for an OT network, the methods of data acquisition and covert path discovering are related to the structure of an OT network. So firstly, a common structure of an OT network will be introduced.

OT Network

[0019] As shown in FIG. **1**, an OT network **30** can include:

[0020] OT devices **302**

[0021] OT devices can include industrial controllers, industrial hosts, etc. An industrial controller can be a PLC (programmable logical controller), a DCS (distributed control system) controller, a RTU (remote terminal unit), etc. An industrial host can include a host computer such as a workstation or a server implemented based on a PC (personal computer), for example, an engineer station, an operator station or a server. Industrial hosts may further include an HMI (human machine interface). In an OT network, industrial hosts monitor and control the industrial controllers. Control industrial controllers can read data from field devices (for example, read a status parameter of the field device from a sensor), store the data in a historical database, and send control commands to industrial controllers according to instructions of an operator or according to a preset control program or logic. The engineer station may also configure industrial controllers.

[0022] network devices **301**

[0023] With network devices such as switches and routers, data can be transmitted among an OT network. For example, network devices can connect industrial controllers to industrial hosts. Currently, a growing quantity of OT networks are implemented based on industrial Ethernet, and communication in an OT network can base on the TCP (transmission control protocol), UDP (user datagram protocol), IP (internet protocol).

[0024] security devices **303**

[0025] Security devices can keep an OT network to work normally and safely, prevent cyberattacks from outside OT networks, such as attacks from an IT networks. As men-

tioned above, with the industrial digitalization, OT networks are connected with IT networks, which expose OT networks to cyberattacks, malware intrusion and other threats from IT networks. Security policies can be set on security devices to mitigate such risks. Security devices may include firewalls, anti-virus software, security gateway, IDS (intrusion detection system), etc.

[0026] Now, referring to FIG. **1**, structure of the system **100** and methods of data acquisition from the OT network **30** will be introduced.

Structure of the System **100**

[0027] The system **100** may include a central security monitoring center **10** and at least one data collector **20**. The at least one data collector **20** is connected to the OT network **30** to collect network connection data in the OT network **30** and extract IP configuration data of network connections from the network connection data. The central security monitoring center **10** receives IP configuration data from the data collectors **20** to analyze covert path in security monitoring for the OT network **30**.

[0028] The central security monitoring center **10** can be implemented as one or multiple servers, which performs security monitoring on the OT network **30**. It can receive data about the OT network **30** via the data collectors **20** and based on which to accomplish security monitoring, such as threat analysis, vulnerability scanning, risk assessment, etc. In present disclosure, the central security monitoring center **10** can receive IP configuration data via the data collectors **20**, and based on the IP configuration data, to discover covert paths among the OT network **30** and at least one IT network **40** connected to the OT network **30**.

[0029] The data collectors **20** can be connected to a SPAN (switched port analyzer) port of a network device **301** in the OT network **30**, to perform port mirroring, so that all packets passing through ports of the network devices **301** can be captured. Alternatively, data collectors **20** can connect to network tap(s) to get packets in the OT network **30**. In this way, packets flow to the network tap from the OT network **30**.

Network Connection Data

[0030] In present disclosure, the network connection data may include but not limited to:

[0031] network flow data

[0032] IP configuration data of network interface cards installed on OT devices **302**

[0033] log of permitted communications in security devices **303**

[0034] Once acquiring the network connection data, the data collectors **20** can extract IP configuration data of network connections from the network connection data and send to the central security monitoring center **10**, which will identify subnets involved in the network connections. Network connections across subnets will be further identified by the central security monitoring center **10**. To differentiate the filtered network connections, here we call the original network connections derived from the IP configuration data as "first network connections", call the network connections filtered from the first network connections, which across a first identified subnet and a second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone, as "second network connections".

[0035] Next, for each of the above 3 types of network connection data, the data collectors **20** will execute data collection and IP configuration data extraction. IP configuration data can include source IP address and destination IP address of a network connection; optionally, it can also include port, protocol, subnet and other related information.

Data Collection and IP Configuration Data Extraction

[0036] network flow data

[0037] The data collectors **20** can collect network flow data and extract IP addresses from the network flow data, optionally, it can also extract port and protocol related information. One example of the extracted information can include:

[0038] (1) Source IP address

[0039] (2) Destination IP address

[0040] (3) Source Port

[0041] (4) Destination port

[0042] (5) Protocol used in the OT network traffic

[0043] (6) Vlan tag

[0044] The extracted information, that is the IP configuration data, will be sent to the central security monitoring center **10** for further analysis. For example, based on the source IP address and the destination IP address, the central security monitoring center **10** can identify subnets involved in the network connection.

[0045] IP configuration data of network interface cards installed on OT devices **302**

[0046] The data collectors **20** can collect the host network configuration information and connection information by an agent installed on an OT device **302**, then analyzes how many network interface cards are installed on the OT devices **302** and which of them are active, next extract IP configuration data of the active network interface cards. The data collectors **20** can get the IP configuration data, such as IP addresses and subnet information, through the agent installed on the OT devices **302**. For example, they can run the command "Ipconfig/all" in the OT devices **302** with windows operating system to get the IP configuration data of network interface card(s).

[0047] log of permitted communications in security devices **303**

[0048] The data collectors **20** can get logs of permitted communications in security devices **303**, such as firewalls, and extract the source IP address and destination IP address from the allowed traffic in the log.

[0049] In addition, the data collectors **20** can directly get network connection data from network interface cards in the OT devices **302**. For example, it can run the command "netstat" on an OT device **302** with windows operating system installed to get the network connection data, which can contain following information:

[0050] Source IP address

[0051] Destination IP address

[0052] Source Port

[0053] Destination port

[0054] Connection status

[0055] Based on the source IP address and the destination IP address, the central security monitoring center **10** can identify subnets related to the network connections. If the

Connection status of one network connection is "ESTABLISHED", it means there is communication behavior.

Subnets Identification and Second Network Connection Filtering

[0056] For a first network connection, the subnet identification can rely on the source IP address and destination IP address. For IP addresses of type A, if the first 8 bits of source and destination IP address are the same, the first network connection is inside a subnet; otherwise, the first network connection is across two subnets. For IP addresses of type B, if the first 16 bits of source and destination IP addresses are the same, the first network connection is inside a subnet; otherwise, the first network connection is across two subnets. For IP addresses of type C, the subnet identification has to rely on the IP addresses and subnet mask. XOR of IP address and its subnet mask is the identifier of subnet. If the subnet of the source IP address is same with the destination IP address, the first network connection is inside same subnet; otherwise, the first network connection is across two subnets.

[0057] Then, the second network connections will be further filtered from the first network connections to get network connections across subnets in different security zones.

[0058] In present disclosure, covert path discovering is based on security zones analysis. If there is a network connection across two subnets belonging to different security zones among the OT network **30** and the connected at least one IT network **40**, and the network connection's existence is not known to the network management system or security monitoring, then the network connection will be determined as a covert path. Next, detailed description will be presented to introduce two optional schemes of covert path identification. Usually, a security zone includes at least one subnet, while a subnet only belongs to one specific security zone.

Scheme 1. Security Zone Determination and Covert Path Identification

[0059] In scheme 1, there is no restriction on communication between the two subnets according to security policies in the OT network **30**. Then for each two identified subnets, the central security monitoring center **10** can count number of OT devices **302** which are involved in the first network connections across the two subnets. If the number of OT devices **302** involved in the first network connections across the two subnets is less than a predefined threshold, the central security monitoring center **10** can determine the two subnets belong to different security zones.

[0060] For example, for subnet A with address "192.168.123.0" and subnet B with address "192.168.234.0", a first network connection with source IP address "192.168.123.6" and destination IP address "192.168.234.3", the subnet masks of the source IP address and the destination IP address are both "255.255.255.0", which means the OT devices **302** involved in the network connection belonging respectively to subnet A and subnet B (for example, there are more than one network interface cards installed on a specific OT device **302**). Then the number of OT devices **302** involved in the first network connection across subnet A and subnet B can be added by 2. Optionally, if one specific OT device **302** is involved in several first network connections across subnet A and subnet B, the number of the specific OT device **302** can be added respectively for each first network connection.

[0061] There is no restriction on communication between the two subnets according to security policies in the OT network **30**. Under such circumstances, if the number of OT devices **302** involved in the first network connections across subnet A and subnet B is not less than a predefined threshold and, subnet A and subnet B will be determined belonging to same security zone. For example, there are 10 OT devices **302** in subnet A and there are 10 OT devices **302** in subnet B, if the number of OT devices **302** involved in network connections across the two subnet is less than 8, it can be decided that the two subnets belong to different security zones.

[0062] Although there might be not many OT devices **302** involved in first network connections across two specific subnets, the two specific subnets might be in same security zone with another subnet, then the central security monitoring center **10** can determine the two specific subnets are in the same security zone. For example, subnet A and subnet B are in the same security zone, subnet B and subnet C are in the same security zone according to the above mentioned method of counting OT devices **302**. Although for subnets A and C, there are not many OT devices involved in first connections across subnets A and C, they can still be determined belonging to same security zone with subnet B.

[0063] With the determined security zones, the central security monitoring center **10** can determine a second network connection as a covert path if the second network connection is not predefined as permitted by security policies in the OT network **30**. As explained above, a second network connection is across subnets belonging to different security zones. For example, an OT device **302** with two network interface cards connect an IT network **40** and the OT network **30** will be considered as an anomaly network connection which will not be defined in the security policies of security devices **303**.

[0064] With scheme 1, although without clear definition of security zones, taking that covert paths are usually potential and not explicitly defined, security zones can be determined by the frequency of communications across subnets, combined with the available restriction rules on network communications. The more OT devices **302** involved in communications across two subnets, the less possibility the two subnets belong to different security zones.

Scheme 2 Predefined Security Zones and Covert Path Identification

[0065] Different from scheme 1, in scheme 2, security zones are predefined. That is, whether subnets belong to same security zone is predefined. Preferably, information of security zones and included subnets can be stored in a DB and when discovering covert path, the information can be read from the DB.

[0066] When discovering covert paths, the central security monitoring center **10** can determine a second network connection as a covert path if the second network connection is across subnets belonging to different security zones according to the predefined relationship. As explained above, a second network connection is across subnets belonging to different security zones. With the predefined security zones, discovering covert path becomes easier.

[0067] For both scheme 1 and scheme 2, the central security monitoring center **10** can collect security policies

from security devices **303** via data collectors **20** connected to the network devices **301**. Allowed IP addresses and/or subnet information and the denied IP addresses and/or subnet information can be explicitly defined in the security policies.

[0068] The central security monitoring center **10** can inform discovered covert paths to a network administrator, to block them or make the traffic pass through the security devices **303**, such as firewalls.

[0069] In the embodiments of the present disclosure, network connection data can be collected timely from the OT network via data collectors, with the network connection data, network connections can be derived and subnets involved in the network connections can be acquired. Based on whether the subnets involved in a network connection belong to same security zone, potential covert path(s) between different security zones can be recognized as many as possible. Missing possible covert path can be avoided.

[0070] Now, referring to FIG. **2**, procedure of method **200** for covert path discovering in OT security monitoring will be introduced. As shown in FIG. **2**, the procedure can include following steps:

[0071] S**201**: receiving, from at least one data collector **20** connected to an OT network **30**, IP configuration data of network connections among the OT network **30** and at least one IT network **40** connected to the OT network **30**.

[0072] In some embodiments, the IP configuration data can be acquired by the at least one data collector **20** from collected network flow data.

[0073] In some embodiments, the IP configuration data can include IP configuration data of network interface cards installed on OT devices **302** in the OT network **30**.

[0074] Optionally, the IP configuration data can be acquired by the at least one data collector **20** from logs of permitted communications in at least one security device **303** in the OT network.

[0075] S**202**: identifying subnets among the OT network **30** and the at least one IT network **40** based on the IP configuration data.

[0076] S**203**: determining different security zones among the OT network **30** and the at least one IT network **40** based on the identified subnets.

[0077] S**204**: discovering at least one covert path across the identified subnets belonging to the determined different security zones.

[0078] In some embodiments, the step S**203** can further include two sub steps S**2031** and S**2032**. In the sub step S**2031**, if there is no restriction on communication between the two subnets according to security policies in the OT network **30**, number of OT devices **302** involved in the network connections across two subnets will be counted, and in the sub steps S**2032**, the two subnets belonging to different security zones can be determined if the number of OT devices **302** involved in the network connections across the two subnets is less than a predefined threshold. Accordingly, the step S**204** can further include sub step S**2041**, in the sub step S**2041**, it can be determined that a network connection across the first identified subnet and the second identified subnet is a covert path if the network connection is not predefined as permitted by security policies in the OT network **30**.

[0079] In some embodiments, the step S**203** can further include sub step S**2033**. In the sub step S**2033**, different security zones can be determined according to predefined relationship between security zones and their included subnets. In some embodiments, the step S**204** can further include sub step S**2042**. In the sub step S**2042**, it can be determined that a network connection across the first identified subnet and the second identified subnet is a covert path, wherein the first identified subnet belongs to the first determined security zone and the second identified subnet belongs to the second determined security zone. Here, the "first" and the "second" are used to differentiate two different items. Other optional implementation of the method **200** can be referred to from the above details of the system **100**.

[0080] Now, referring to FIG. **3**, an apparatus **101** for covert path discovering in OT security monitoring will be introduced. As shown in FIG. **3**, the apparatus **101** can include at least one memory **1011**, configured to store computer executable instructions; and at least one processor **1012**, coupled to the at least one memory **1011** and upon execution of the computer executable instructions, configured to execute method **200**. In some embodiments, the apparatus **101** can further include a communication module **1013**, via which the apparatus **101** can receive network connection data and log of security devices **303** in the OT network **30**. Furthermore, another apparatus for covert path discovering in OT security monitoring can be implemented as software installed on the central OT security monitoring server, including modules to execute the method **200**.

[0081] As another example, some embodiments include a computer program stored on a readable tangible medium of a controller, and includes computer executable instructions, where the computer executable instructions, when executed, cause at least one processor to execute one or more of the methods described herein.

[0082] As another example, some embodiments include a computer readable storage medium storing computer executable instructions thereon, where the computer executable instructions, when executed, cause at least one processor to execute one or more of the methods described herein.

[0083] It should be noted that, depending on the implementation requirements, the components/steps described in the embodiments of the present disclosure may be split into more components/steps, or two or more components/steps or partial operations of the components/steps may be combined into novel components/steps without leaving the scope of the present disclosure.

[0084] The above methods and/or systems may be implemented in hardware or firmware, or be implemented as software or computer code storable in a recording medium (such as a CD ROM, RAM, floppy disk, hard disk, or magnetic disk), or be implemented as computer code that is downloaded from a network, is originally stored in a remote recording medium or a non-transitory machine-readable medium, and will be stored in a local recording medium, such that the method described herein may be processed by such software stored on a recording medium using a general-purpose computer, a special-purpose processor, or programmable or dedicated hardware (such as an ASIC or FPGA). It is understandable that a computer, processor, microprocessor controller, or programmable hardware includes a storage component (e.g., RAM, ROM, or flash memory) that can store or receive software or computer code. The method for generating check code described herein is implemented when the software or computer code is accessed and executed by the computer, processor, or hardware. Further, when a general-purpose computer accesses the code for

implementing the method for generating check code shown herein, the execution of the code converts the general-purpose computer to a special-purpose computer configured to execute the method for generating check code shown herein.

[0085] As will be appreciated by those of ordinary skills in the art, the various example units and method steps described in combination with the embodiments disclosed herein can be implemented by electronic hardware, or a combination of computer software and electronic hardware. Whether these functions are performed by hardware or software depends on specific applications and design constraints of the technical solutions. Those skilled in the art may implement described functions for each specific application using different methods, but such implementation should not be considered as falling beyond the scope of the embodiments of the present disclosure.

[0086] The above implementations are only used to illustrate example embodiments of the present disclosure and are not intended to limit the scope of the present disclosure. Those of ordinary skills in the relevant technical field may further make various alterations and modifications without departing from the spirit and scope of the embodiments of the present disclosure. Therefore, all equivalent technical solutions also belong to the scope of the embodiments of the present disclosure.

What is claimed is:

1. A method for covert path discovering in OT security monitoring, the method comprising:

receiving IP configuration data of network connections among the OT network and an IT network connected to the OT network from a data collector connected to the OT network;

identifying subnets among the OT network and the IT network based on the IP configuration data;

determining different security zones among the OT network and the IT network based on the identified subnets; and

discovering a covert path across a first identified subnet and a second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone.

2. The method according to claim **1**, wherein the IP configuration data is acquired by the at least one data collector from collected network flow data in the OT network.

3. The method according to claim **1**, wherein the IP configuration data includes IP configuration data of network interface cards installed on OT devices in the OT network.

4. The method according to claim **1**, wherein the IP configuration data is acquired by the data collector from logs of permitted communications in a security device in the OT network.

5. The method according to claim **1**, wherein

determining different security zones among the OT network and the IT network based on the identified subnets comprises:

for each two identified subnets, if there is no restriction on communication between the two identified subnets according to security policies in the OT network,

counting a number of OT devices involved in network connections across the two identified subnets, and

determining the two identified subnets belong to different security zones, if the number of OT devices is less than a predefined threshold; and

discovering a covert path across a first identified subnet and a second identified subnet comprises determining a network connection across the first identified subnet and the second identified subnet as a covert path if the network connection is not predefined as permitted by security policies in the OT network.

6. The method according to claim **1**, wherein

determining different security zones among the OT network and the IT network based on the identified subnets comprises

determining different security zones according to predefined relationship between security zones and their included subnets; and

discovering a covert path across a first identified subnet and a second identified subnet comprises

determining that a network connection across the first identified subnet and the second identified subnet is a covert path, wherein the first identified subnet belongs to the first determined security zone and the second identified subnet belongs to the second determined security zone.

7. An apparatus for covert path discovering in OT security monitoring, the apparatus comprising:

a memory storing computer executable instructions;

at least one processor coupled to the memory;

wherein, upon execution of the computer executable instructions, the at least one processor:

receives IP configuration data of network connections among the OT network and an IT network connected to the OT network from a data collector connected to the OT network;

identifies subnets among the OT network and the IT network based on the IP configuration data;

determines different security zones among the OT network and the IT network based on the identified subnets; and

discovers a covert path across a first identified subnet and second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone.

8. A system for covert path discovering in OT security monitoring, the system comprising:

a data collector connected to an OT network to acquire IP configuration data of network connections among the OT network and an IT network connected to the OT network; and

a central security monitoring center connected with the data collector;

wherein the central security monitoring center includes a memory storing computer executable instructions;

at least one processor coupled to the memory, wherein, upon execution of the computer executable instructions, the at least one processor:

receives IP configuration data of network connections among the OT network and an IT network connected to the OT network from a data collector connected to the OT network;

identifies subnets among the OT network and the IT network based on the IP configuration data;

determines different security zones among the OT network and the IT network based on the identified subnets; and

discovers a covert path across a first identified subnet and a second identified subnet, wherein the first identified subnet belongs to a first determined security zone, and the second identified subnet belongs to a second determined security zone.

9-10. (canceled)

* * * * *