(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2016 (28.04.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/064397 A1

(51) International Patent Classification:
*H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2014/061934

(22) International Filing Date:
23 October 2014 (23.10.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **EDWARDS, Nigel**; Longdown Avenue, Stoke, Gifford, Bristol BS34 8QZ (GB). **KRAUSE, Michael R.**; 3000 Hanover Street, Santa Cruz, California 94304-1112 (US).

(74) Agents: **SHOOKMAN, Jeb A.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17**:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

**Published**:

— *with international search report (Art. 21(3))*

WO 2016/064397 A1

(54) Title: ADMISSIONS CONTROL OF A DEVICE

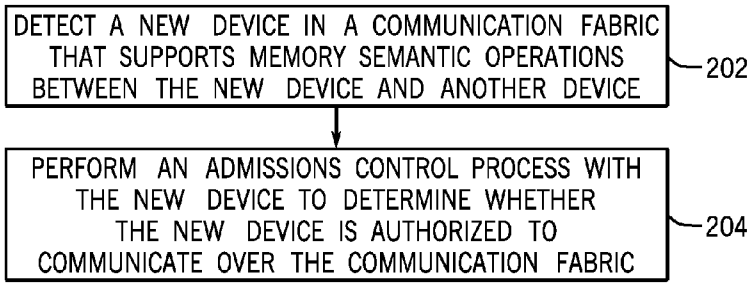


FIG. 2

(57) Abstract: A method for a control device in a communication fabric is provided. The method comprises detecting, by the control device, a first device in the communication fabric that supports memory semantic operations between the first device and a second device, and performing, by the control device, an admissions control process with the first device to determine whether the first device is authorized to communicate over the communication fabric that supports memory semantic operations.

# ADMISSIONS CONTROL OF A DEVICE

## Background

[0001] A system, such as a computer or other type of system, can include various types of devices. Such devices can include a processor, an input/output device, a memory device, and other devices. The processor or I/O device can issue memory access commands over a memory bus to the memory device. The memory device can send data to the requesting processor or I/O device over the memory bus.

## Brief Description Of The Drawings

[0002] Some implementations are described with respect to the following figures.

[0003] Fig. 1 is a schematic diagram of an example arrangement that includes a communication fabric and devices coupled to the communication fabric, according to some implementations.

[0004] Fig. 2 is flow diagram of an example process according to some implementations.

[0005] Fig. 3 is a schematic diagram of a further example arrangement that includes a communication fabric and devices coupled to the communication fabric, according to further implementations.

[0006] Fig. 4 is a message flow diagram of an example process among a new device, a switch, and a control device, according to some implementations.

[0007] Fig. 5 is a schematic diagram of an example format of a transaction packet, according to some implementations.

[0008] Fig. 6 is a schematic diagram of another example arrangement that includes a communication fabric and devices coupled to the communication fabric, according to additional implementations.

[0009] Fig. 7 is a block diagram of an example control device, according to some implementations.

[0010] Fig. 8 is a block diagram of an example gateway, according to some implementations.

Detailed Description

[0011] Network protocols such as the Transmission Control Protocol (TCP) and the Internet Protocol (IP) define formats and procedures for communication of data over communication fabrics. However, some network protocols may not be efficient for certain types of communications, such as communications for accessing memory (or another type of storage). Network protocols may not support high-bandwidth and low-latency communications that are often involved in access memory or another type of storage. In addition, network protocols can employ protocol headers that lead to increased overhead, which may not be appropriate for memory/storage access operations.

[0012] A different communication protocol (referred to as an "interconnect protocol" in the present disclosure) can be provided that supports memory semantic operations over a communication fabric. A "memory semantic operation" can refer to an operation that employs memory requests to communicate between a source device and a destination device. For example, the source device can be a processor, while the destination device can be a memory. The memory requests can include a read request, a write request, an atomic operation request, and so forth, which can be issued by the source device to access data in the destination device. In some implementations, the interconnect protocol can support memory semantic operations as well as other types of operations between a source device and a destination device.

[0013] In other examples, a source device can include a different type of electronic device, such as a graphics controller, an input/output (I/O) controller, a network interface controller, a computer, and so forth, while a destination device can also include any of the foregoing devices. More generally, a source device or

destination device can include an entire machine (*e.g.* a computer, storage system, communication system, a handheld device such as a smartphone or personal digital assistant, a game appliance, etc.), or alternatively, can include one or a combination of electronic components within a machine (*e.g.* a processor, a memory device, a persistent storage device, a graphics controller, an I/O controller, a network interface controller, etc.).

[0014] In some implementations, the interconnect protocol can support relatively high bandwidth and low latency transactions over a communication fabric that is appropriate for memory access operations. Some details regarding transaction packet formats according to the interconnect protocol that can be communicated over the communication fabric are provided further below.

[0015] In a communication fabric that can interconnect many devices that are able to communicate using the interconnect protocol, security can become an issue. To provide security, the interconnect protocol may specify use of a security feature, which can be used to prevent unauthorized or malicious communications by devices connected to the communication fabric.

[0016] In accordance with some implementations, as shown in Fig. 1, techniques or mechanisms are provided to perform an admissions control process for a new device 102 that is able to communicate using the interconnect protocol that supports memory semantic operations. A "new device" can refer to a device that was not previously connected to a communication fabric 104 and has been newly added to the communication fabric for the first time. Alternatively, a "new device" can refer to a device that was previously disconnected or deactivated and then re-connected or re-activated on the communication fabric 104.

[0017] The admissions control process can be performed by admissions control logic 106 in a control device 108 connected to the communication fabric 104. The admissions control process uses a security element to verify the new device 102 so that the control device 108 can determine whether or not the new device is authorized to communicate over the communication fabric. As discussed further

below, examples of the security element can include a public key and/or a private key, a certificate, or any other item that can be used by one device to determine whether another device is authorized to perform a certain task (or tasks). If authorized, a transaction integrity key can be provided to the new device 102 to allow implementation of the security feature of the interconnect protocol by the new device 102. As discussed further below, the security feature of the interconnect protocol can include a security header provided in each transaction packet communicated over the communication fabric 104.

[0018] In some examples, a transaction integrity key (TIK) can include a symmetric key that can be generated by a key distribution server that is able to communicate over the communication fabric 104. A symmetric key is a key that is used for both encryption and decryption of a message. In other examples, other types of TIKs can be employed.

[0019] In some cases, the new device 102 may not support the security feature. In such cases, a gateway (discussed further below) may be configured to act as proxy for the new device 102. The proxy is provided between the new device 102 and other devices connected to the communication fabric 104. The proxy can implement the security feature of the interconnect protocol on behalf of the new device 102. The proxy can also perform other tasks on behalf of the new device 102.

[0020] Once the admissions control logic 106 determines that the new device 102 is allowed to communicate over the communication fabric 104, the new device 102 can perform communications with an existing device 110 connected to the communication fabric 104. An “existing device” can refer to a device that has previously been connected to or activated on the communication fabric 104.

[0021] The communication fabric 104 includes various communication media (*e.g.* electrical conductors, electrical wires, optical fibers, optical paths, wireless links, etc.) and communication nodes (*e.g.* switches, routers, etc.) that are capable of forwarding or routing data packets between a source device and a destination

device. Although just one new device 102 and one existing device 110 is depicted in Fig. 1, it is noted that there can be many devices connected to the communication fabric 104.

[0022] Fig. 2 is a flow diagram of an example process that can be performed by the admissions control logic 106. The admissions control logic 106 detects (at 202) the new device 102 in the communication fabric 104 over which an interconnect protocol can be used that supports memory semantic operations between devices. The admissions control logic 106 performs (at 204) an admissions control process with the new device to determine whether the new device is authorized to communicate over the communication fabric 104.

[0023] The admissions control process can use a security element to determine whether or not the new device 102 is authorized to communicate over the communication fabric 104. In some examples, the security element can include a key (*e.g.* a public key and/or a private key). As a further example, the admissions control process can employ a challenge-response protocol initiated by the admissions control logic 106. In the admissions control process that involves the control device 108 and the new device 102, the control device 108 is the challenger, and the new device 102 is the responder. The challenge-response protocol includes the challenger (control device 108) sending the responder (new device 102) a newly created random nonce. A nonce is an arbitrary number used just once in a cryptographic communication. A nonce can be a random or pseudo-random number.

[0024] In response to the nonce, the responder returns, to the challenger, a signature derived from the nonce using the responder's private key. The challenger can then verify the signature using the corresponding public key. Verification of the signature using the corresponding public key by the challenger results in a successful admissions control process, such that the new device 102 is admitted to the communication fabric 104. However, if the challenger is unable to verify the signature, then the admissions control process is considered to have failed, in which

case the new device 102 is not allowed to communicate over the communication fabric 104.

[0025] Another example of a challenge-response protocol is one in which encryption and decryption are used. The challenger creates a nonce (similar to the nonce discussed above) and encrypts the nonce using the responder's public key. The encrypted nonce is sent as ciphertext (an encrypted version of the nonce) to the responder. The responder decrypts the ciphertext using the private key of the responder, and returns the decrypted nonce back to the challenger. If the challenger determines that the nonce received from the responder matches the nonce sent by the challenger to the responder, then the admissions control process is considered to have succeeded.

[0026] Note that the public key used by the challenger in either of the challenger-response protocols discussed above may have been communicated to the control device 108 by a specific entity, which can be a trusted entity.

[0027] In other implementations, the admissions control process may be based on use of a certificate provided at the new device 102. The certificate at the new device 102 includes information about a public key. The certificate is signed by an issuing authority that is trusted in the communication fabric 104. The certificate can reside at a specified location in the new device 102, where the specified location can be a “well-known address”—an address that is established by a standard or by agreement. The control device can access the certificate in the new device 102 at the specified location. The certificate is signed by the private key of the issuing authority. When the certificate is retrieved by the control device 108, the control device 108 uses the corresponding public key to verify the certificate. Successful verification of the certificate results in successful performance of the admissions control process.

[0028] Fig. 3 is a schematic diagram of an example arrangement according to further implementations. Fig. 3 shows a switch 302 provided as part of the communication fabric 104. The new device 102 is connected to an interface 304 of

the switch 302. The switch 302 detects the new device 102 if the interface 304 was previously inactive but becomes active in response to connection of the new device 102 to the interface 304 or activation of the new device 102 that was previously deactivated. Alternatively, the switch 302 can detect the new device 102 in response to a message or other indication sent by the new device 102 to the switch 302 upon connection of the new device 102 to the switch 302 or activation of the new device 102.

[0029] Upon detecting the new device 102 (but prior to the new device 102 having gone through an admissions control process), the switch 302 allows the new device 102 to send packets to a specified address (or set of specified addresses). In some implementations, devices on the communication fabric 104 are uniquely identified using component identifiers (CIDs). Each device on the communication fabric 104 is assigned one or multiple CIDs. In a given transaction, the source device is identified using a source SID (SCID), while the destination device is identified using a destination CID (DCID). In other examples, the source device and the destination device can be identified using other types of identifiers, such as IP addresses, TCP ports, and so forth.

[0030] For the new device 102 that has not yet gone through the admissions control process, the switch 302 allows the new device 102 to send packets to just a specific DCID (or set of DCIDs), which correspond(s) to the control device 108 (or other control device) that performs admissions control. Any packet sent to a DCID other than the specified DCID(s) is dropped by the switch 302.

[0031] As further shown in Fig. 4, in response to receiving a packet received from the new device 102, where the packet can correspond to a request (402) by the new device 102 to access the communication fabric 104, or to register in the communication fabric 104, the admissions control logic 106 in the control device 108 can start the admissions control process as discussed above.

[0032] The admissions control process involves admissions control messaging (404) exchanged between the control device 108 and the new device 102. The

admissions control messaging is forwarded through the switch 302. The admissions control messaging 404 can include a challenge and a response, as discussed above, or retrieval of a certificate from the new device 102 for verification at the control device 108.

[0033] If the control device 108 determines that the admissions control process is successful, then the control device 108 sends an enable routing message (406) to the switch 302 to enable routing for the new device 102. Once routing is enabled for the new device 102, packets sent by the new device 102 or packets destined to the new device 102 can be routed accordingly by the switch 302. In some examples, along with the enable routing message (406), the control device 108 can also send control information to update forwarding information (*e.g.* forwarding table, flow table, routing table, etc.) at the switch 302. The switch 302 uses the forwarding information to forward packets to a target destination.

[0034] In addition, in some implementations, the control device 108 can act as a key distribution server and can issue one or multiple transaction integrity keys (TIKs) (408) to the new device 102. In some examples, a TIK provides for security for transactions over the communication fabric 104. The TIK can be used to generate a security value that is included in a security header of a transaction packet.

[0035] A transaction packet can include various fields as depicted in Fig. 5, in some examples. Although example fields are shown in the transaction packet of Fig. 5, it is noted that in other examples, other fields or other arrangements of fields can be provided. As depicted in Fig. 5, one of the fields included in a transaction packet includes a security header 502, which can include the security value produced using the TIK according to some implementations.

[0036] For example, given a message MSG, where MSG can represent any content that is to be communicated between a source device and a destination device in a transaction packet, a security value, SMH, can be produced according to the following: SMH = HMAC(TIK, MSG), where HMAC represents “Hash-Based Message Authentication Code.” In some examples, HMAC is described in Request

for Comments (RFC) 2104, "HMAC: Key-Hashing for Message Authentication," dated February 1997; and RFC 6151, entitled "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms," dated March 2011. In other examples, other techniques for producing the security value based on the TIK for inclusion in the security header 502 of Fig. 5 can be employed.

[0037] In some examples, a TIK can be a symmetric key that can be generated by the key distribution server 306 of Fig. 3, which can be implemented in the control device 108 or in another device. A symmetric key is a key that is used for both encryption and decryption of a message. In other examples, other types of TIKs can be employed.

[0038] The security value included in the security header 502 of a transaction packet can be used to perform device-device authentication over the communication fabric 104 in which any two devices are able to authenticate each other using a cryptographically secure mechanism based on the security value.

[0039] In some examples, the security value in the security header 502 can be used to prevent spoofing of a sender identifier (*e.g.* SCID in an SCID field 504 shown in Fig. 5) of a sender device. Spoofing of a sender identifier occurs when one entity successfully masquerades as another entity by falsifying information, in this case the sender identifier, to gain access to a resource. By using the security value in the security header 502, the sender device can be cryptographically verified by a destination device using the TIK at the destination device. For example, the destination device can decrypt the security value, using the TIK, in the security header 502 to produce a value that can be compared to a value that is calculated based on content of the transaction packet that is to be protected. If the values match, then transaction packet is authentic.

[0040] The security value in the security header 502 can also be used to prevent spoofing of another value included in a transaction packet, such as an access key included in an access key field 506 of the transaction packet shown in Fig. 5. An access key can be an identifier used to validate access privileges to a specified

resource (or resources). A resource can include any or some combination of the following: a memory region of a memory device (or memory devices), a storage region of a persistent storage device (or storage devices), an electronic component or a portion of an electronic component (*e.g.* a processor, a memory, a switch, a PGA, a digital signal processor or DSP, a general processing unit or GPU, etc.), an accelerator (which is an entity that is used to perform computations on behalf of another device), a shared I/O component (*e.g.* a network or storage controller, a graphics controller, etc.), an ingress or egress interface, and so forth. If a given resource is associated with an access key, then any transaction packet targeting the resource that does not contain the access key in the access key field 506 will violate resource permissions and can trigger an access violation error.

[0041] In some cases, an access key can be spoofed by a malicious entity, to gain unauthorized access to a resource. However, by including a security value in the security header 502, TIK can be used to verify the authenticity of the access key in the access key field 506.

[0042] In some examples, the transaction packet of Fig. 5 can include other fields, including a payload field 508 (for carrying a data payload when appropriate) of the respective transaction, a DCID field 510 (that includes the DCID for identifying the destination device), and an Opcode field 512 that contains an operation code for specifying a respective operation (*e.g.* a read operation, a write operation, etc.).

[0043] The foregoing describes admissions control for a new device (such as new device 102 in Fig. 1 or 3) and provision of a TIK to allow for implementation of a security feature according to some implementations.

[0044] A further issue associated with an arrangement that includes a communication fabric connected to various devices is that some devices may not support the security feature of the communication fabric 104. For example, some devices may not support the security header 502 included in a transaction packet as shown in Fig. 5. Such devices would not be able to produce a security value in the

security header 502, and also would not be able to perform verification using the security header 502.

[0045] In some examples, as shown in Fig. 6, a gateway 602 can be provided to act as a proxy for a device (*e.g.* the new device 102) that does not support the security header 502 and/or other features of the interconnect protocol governing communications over the communication fabric 104. In some implementations, in the arrangement of Fig. 6, the control device 108 can perform admissions control as discussed above for the new device 102 that does not support at least the security header 502. Assuming that the admissions control is successful, the control device 108 can configure the gateway 602 to act as a proxy for the new device 102. Any communications between the new device 102 and another device (*e.g.* the existing device 110) over the communication fabric 104 is passed through the proxy provided by the gateway 602. The gateway 602 includes a security logic 604 that is able to add a security header to a transaction packet issued by the new device 102. The switch 302 is configured to route any transaction packet sent by the new device 102 to the DCID of the gateway 602; this DCID is referred to as the gateway DCID. The gateway 602 receives the transaction packet from the new device 102, and applies one or multiple transformations on the transaction packet before the transaction packet is sent over the communication fabric 104 to the destination device. One type of transformation that is performed is the insertion of the security header 502 into the transaction packet by the security logic 604 in the gateway 602.

[0046] Note that when a transaction packet is received from another device that is targeted to the new device 102, the security logic 604 can perform verification based on the security header 502 of the transaction packet. If the verification is successful, then the security logic 604 can remove the security header 502 from the transaction packet, and can send the modified transaction packet through the switch 302 to the new device 102.

[0047] In some implementations, the gateway 602 also includes a policy enforcement logic 606 that is able to enforce a policy for communications involving any device that does not support one or multiple features of the interconnect protocol

governing communications over the communication fabric 104. For example, the policy enforcement logic 606 can apply any one of or some combination of the following transformations to a transaction packet from the new device 102: insert an access key or change an access key of the transaction packet, change the SCID and/or the DCID in the transaction packet, and restrict the scope of transactions that the new device 102 is allowed to engage in.

[0048] Also, the policy enforcement logic 606 can specify that just certain types of transactions can be performed by the new device 102, while other types of transactions are not allowed to be performed by the new device 102. This restriction can be enforced by specifying restricted operation codes that can be included in the Opcode field 512 of a transaction packet. Also, the restriction can be accomplished by specifying a restriction on addresses that can be accessed by the new device 102, such that the new device 102 is allowed to access just specific locations in an address space. More generally, policy enforcement can include checking for specifically permitted access keys, DCIDs, address ranges, and operation codes. Any transaction packet from a source device that is outside of the enforcement policy (*e.g.* does not include an access key from among the permitted access keys, a DCID from among the permitted DCIDs, an address from among the permitted address ranges, and an operation code from among the permitted operation codes) is dropped by the gateway 602. The gateway 602 can also issue an alert regarding this policy violation.

[0049] The transformation applied by the policy enforcement logic 606 can also include an address translation, where an address in the transaction packet specifying a resource to be accessed can be translated from an original value to a different value.

[0050] Although the gateway 602 is shown as being separate from the switch 302, it is noted that in some implementations, the gateway 602 can be part of the switch 302.

[0051] Although the foregoing refers to using the gateway 602 to enforce restrictions for a device that does not support feature(s) of the interconnect protocol, it is noted that restrictions can be enforced by the gateway 602 for devices that do support all features of the interconnect protocol. In other words, the policy enforcement logic 606 can enforce policy restrictions for any type of device.

[0052] In some examples, to produce the security value for inclusion in the security header 502 by the security logic 604, the gateway 602 first applies any transformations (as part of performance of policy enforcement) on a transaction packet, and the security value is generated based on the transformed transaction packet using the TIK provided by the control device 108.

[0053] Fig. 7 is a block diagram of an example control device 108 in accordance with some implementations. Note that the control device 108 can be a component within a computer (or within an arrangement of computers).

[0054] The control device 108 includes one or multiple processors 702. A processor can include a microprocessor or a core of the microprocessor, a microcontroller, a physical processor module or subsystem, a programmable integrated circuit, a programmable gate array, and so forth.

[0055] In addition, the control device 108 includes one or multiple non-transitory computer-readable or machine-readable storage media 704, which can store machine-readable instructions. As examples, the storage medium (or storage media) 704 can store security feature determining instructions 706 to determine whether a device supports a security feature, admissions control instructions 708 (corresponding to the admissions control logic 106 shown in Fig. 1 or 3), key sending instructions 710 (which can correspond to the key distribution server 306 of Fig. 3) to send a key (*e.g.* TIK) to a device, and gateway configuring instructions 712 to configure the gateway 602 to act as proxy for a device that does not support a security feature according to some implementations.

[0056] Fig. 8 is a block diagram of an example gateway 602 according to some implementations. Note that the gateway 602 can be a component within a computer (or within an arrangement of computers). The gateway 802 includes one or multiple processors 802. In addition, the gateway 602 includes one or multiple non-transitory computer-readable or machine-readable storage media 804, which can store machine-readable instructions, including security instructions 806 (for implementing the security logic 604 of Fig. 6), and policy enforcement instructions 808 (for implementing the policy enforcement logic 606 of Fig. 6).

[0057] The storage medium (or storage media) 704 or 804 can include one or multiple different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; optical media such as compact disks (CDs) or digital video disks (DVDs); or any other types of volatile or non-volatile storage. Note that the instructions discussed above can be provided on one computer-readable or machine-readable storage medium, or alternatively, can be provided on multiple computer-readable or machine-readable storage media distributed in a large system having possibly plural nodes. Such computer-readable or machine-readable storage medium or media is (are) considered to be part of an article (or article of manufacture). An article or article of manufacture can refer to any manufactured single component or multiple components. The storage medium or media can be located either in the machine running the machine-readable instructions, or located at a remote site from which machine-readable instructions can be downloaded over a network for execution.

[0058] In the foregoing description, numerous details are set forth to provide an understanding of the subject disclosed herein. However, implementations may be practiced without some of these details. Other implementations may include modifications and variations from the details discussed above. It is intended that the appended claims cover such modifications and variations.

What is claimed is:

1. A method comprising:

detecting, by a control device, a first device in a communication fabric that supports memory semantic operations between the first device and a second device; and

performing, by the control device, an admissions control process with the first device to determine whether the first device is authorized to communicate over the communication fabric.

2. The method of claim 1, further comprising:

in response to the admissions control process succeeding, enabling, by the control device, communication by the first device over the communication fabric.

3. The method of claim 2, wherein enabling, by the control device, the communication by the first device over the communication fabric comprises instructing a switch to enable routing of packets for the first device.

4. The method of claim 3, wherein detecting the first device comprises detecting the first device that is newly connected to or newly activated in the communication fabric, wherein the switch is to route packets of the newly connected or newly activated first device just to the control device until the admissions control process succeeds.

5. The method of claim 1, further comprising:

in response to the admissions control process succeeding, sending, by the control device, a transaction integrity key to the first device, the transaction integrity key used in providing security for transactions of the first device.

6. The method of claim 1, wherein performing the admissions control process uses a security element to verify the first device.

7. The method of claim 6, wherein the security element is at least one of a public key, a private key, and a certificate.

8. The method of claim 1, further comprising:

determining, by the control device, whether the first device supports a security header in transactions over the communication fabric; and

in response to determining that the first device does not support the security header, configuring, by the control device, a gateway to act as a proxy for the first device, the proxy to insert the security header for a transaction of the first device.

9. The method of claim 8, wherein configuring the gateway further comprises configuring the gateway that performs at least one selected from among: inserting or modifying an access key in a packet on behalf of the first device to access a resource over the communication fabric, changing a component identifier in the packet for communication involving the first device, and restricting transaction types that are allowed for the first device.

10. A control device comprising:

at least one processor to:

determine whether a first device supports a security feature;

in response to determining that the first device supports the security feature,

perform admissions control to determine whether the first device is authorized to communicate over a communication fabric that supports memory semantic operations, and

send a key to the first device to implement the security feature; and

in response to determining that the first device does not support the security feature,

configure a gateway to act as a proxy for the first device to implement the security feature.

11. The control device of claim 10, wherein the key is for generating a security value to include in a transaction packet sent by the first device over the communication fabric.

12. The control device of claim 10, wherein the admissions control comprises performing a challenge-response process or retrieving a certificate from the first device.

13. The control device of claim 10, wherein the at least one processor is to further, in response to determining that the first device supports the security feature, configure the switch to enable routing of packets between the first device and other devices connected to the communication fabric.

14. The control device of claim 10, wherein the configuring of the gateway further comprises configuring the gateway that performs at least one selected from among: inserting or modifying an access key in a packet on behalf of the first device to access a resource over the communication fabric, changing a component identifier in the packet for communication involving the first device, and restrict transaction types that are allowed for the first device.

15. An article comprising at least one non-transitory machine-readable storage medium storing instructions that upon execution cause a gateway to:

in response to an admissions control process authorizing a first device to communicate over a communication fabric that supports memory semantic operations, implement a security feature on behalf of the first device, wherein the security feature includes generating a security value and inserting the security value into a security header of a packet received from the first device; and

perform policy enforcement comprising at least one selected from among: inserting or modifying an access key in a packet on behalf of the first device to access a resource over the communication fabric, changing a component identifier in the packet for communication involving the first device, and restricting transaction types that are allowed for the first device.

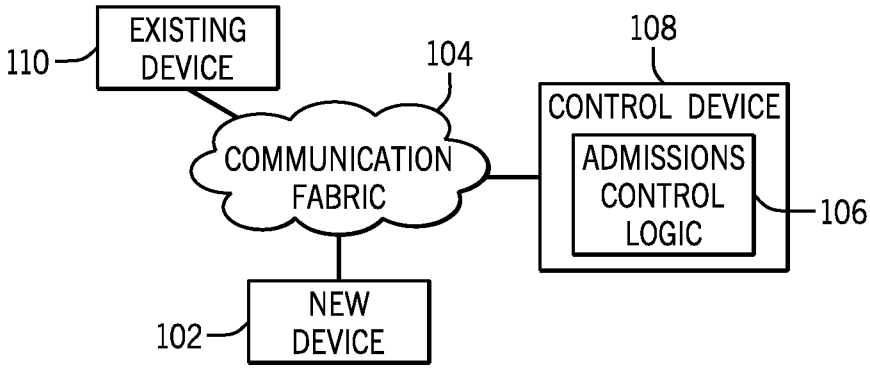
EXISTING DEVICE
110
104
108
CONTROL DEVICE
ADMISSIONS CONTROL LOGIC
106
COMMUNICATION FABRIC
NEW DEVICE
102

FIG. 1

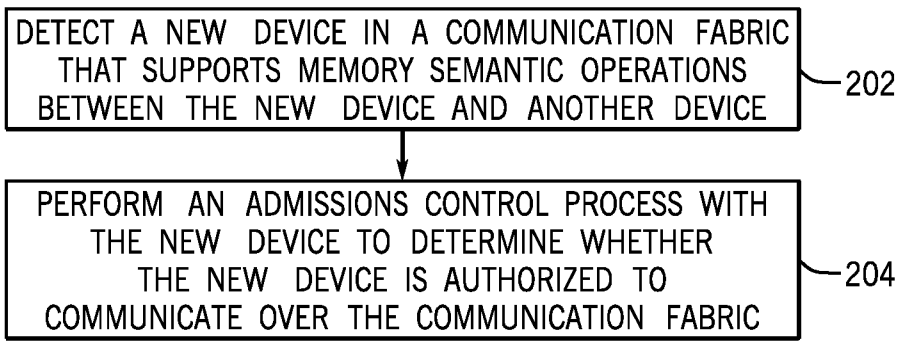
DETECT A NEW DEVICE IN A COMMUNICATION FABRIC THAT SUPPORTS MEMORY SEMANTIC OPERATIONS BETWEEN THE NEW DEVICE AND ANOTHER DEVICE
202
PERFORM AN ADMISSIONS CONTROL PROCESS WITH THE NEW DEVICE TO DETERMINE WHETHER THE NEW DEVICE IS AUTHORIZED TO COMMUNICATE OVER THE COMMUNICATION FABRIC
204

FIG. 2

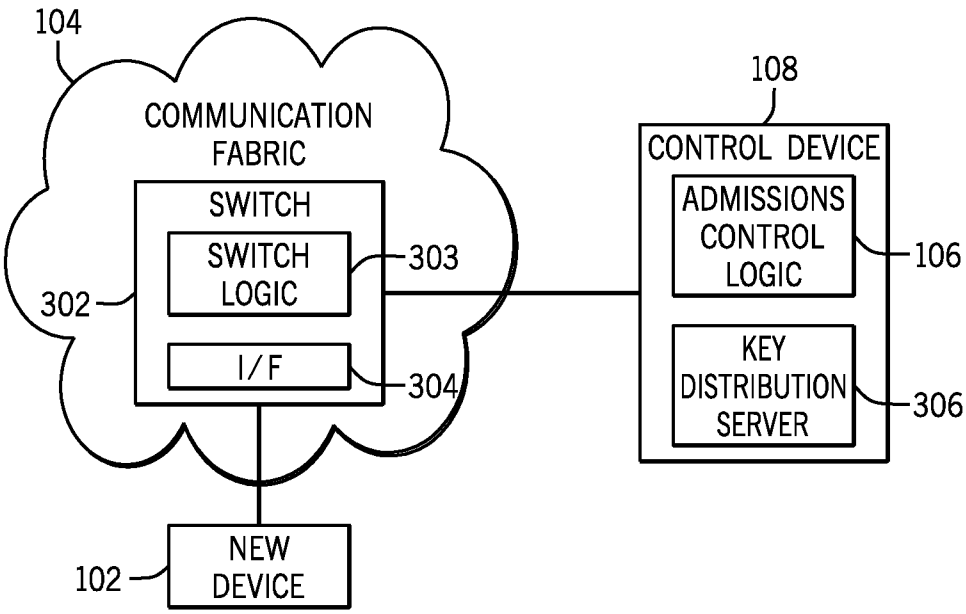
104
COMMUNICATION FABRIC
SWITCH
SWITCH LOGIC
303
302
I/F
304
108
CONTROL DEVICE
ADMISSIONS CONTROL LOGIC
106
KEY DISTRIBUTION SERVER
306
NEW DEVICE
102

FIG. 3

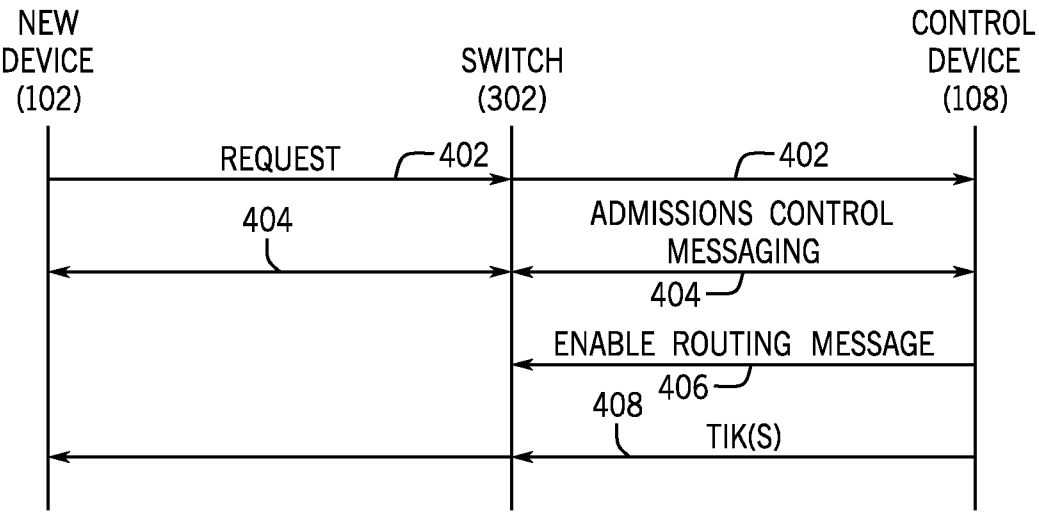
NEW DEVICE (102)
SWITCH (302)
CONTROL DEVICE (108)
REQUEST
402
402
404
ADMISSIONS CONTROL MESSAGING
404
ENABLE ROUTING MESSAGE
406
408
TIK(S)

FIG. 4

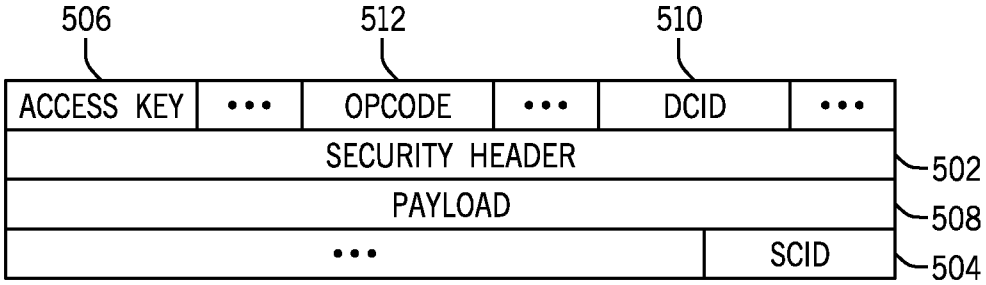
506
512
510
ACCESS KEY
OPCODE
DCID
SECURITY HEADER
PAYLOAD
SCID
502
508
504

FIG. 5

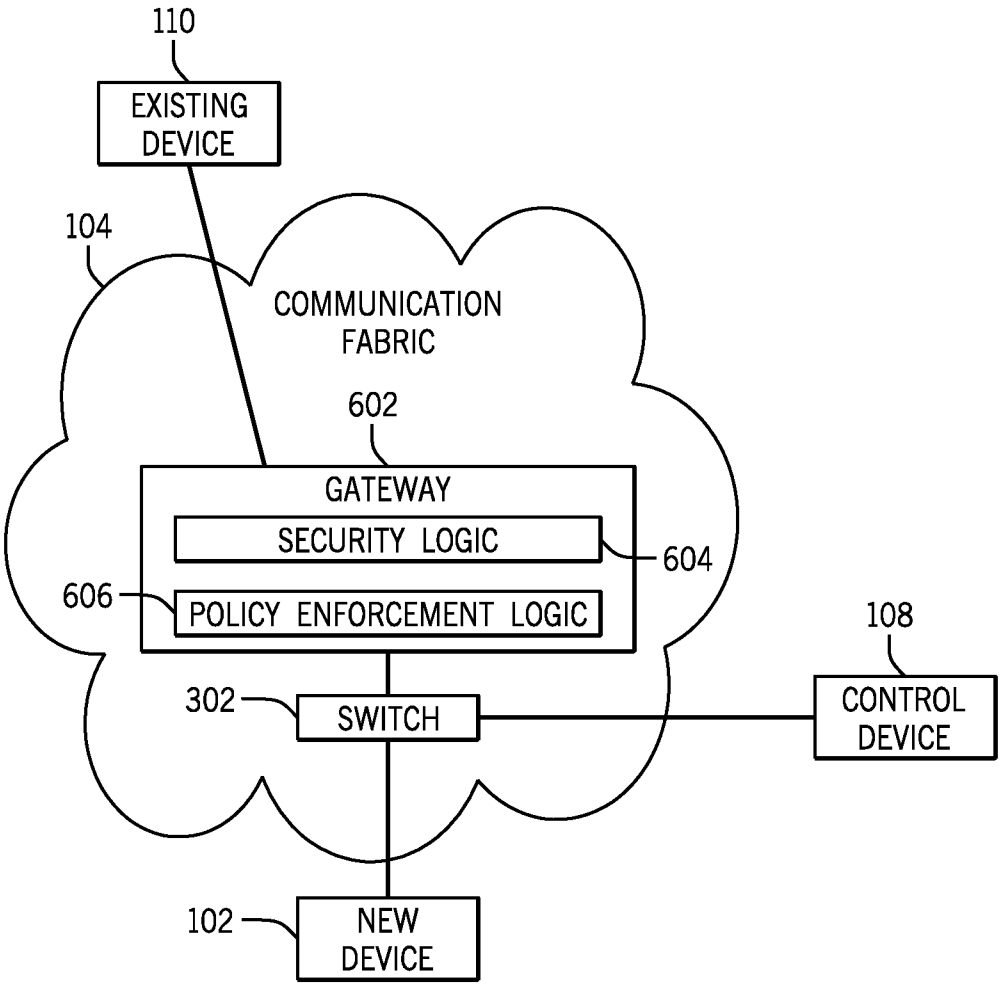
110
EXISTING DEVICE
104
COMMUNICATION FABRIC
602
GATEWAY
SECURITY LOGIC
604
606
POLICY ENFORCEMENT LOGIC
108
302
SWITCH
CONTROL DEVICE
102
NEW DEVICE

FIG. 6

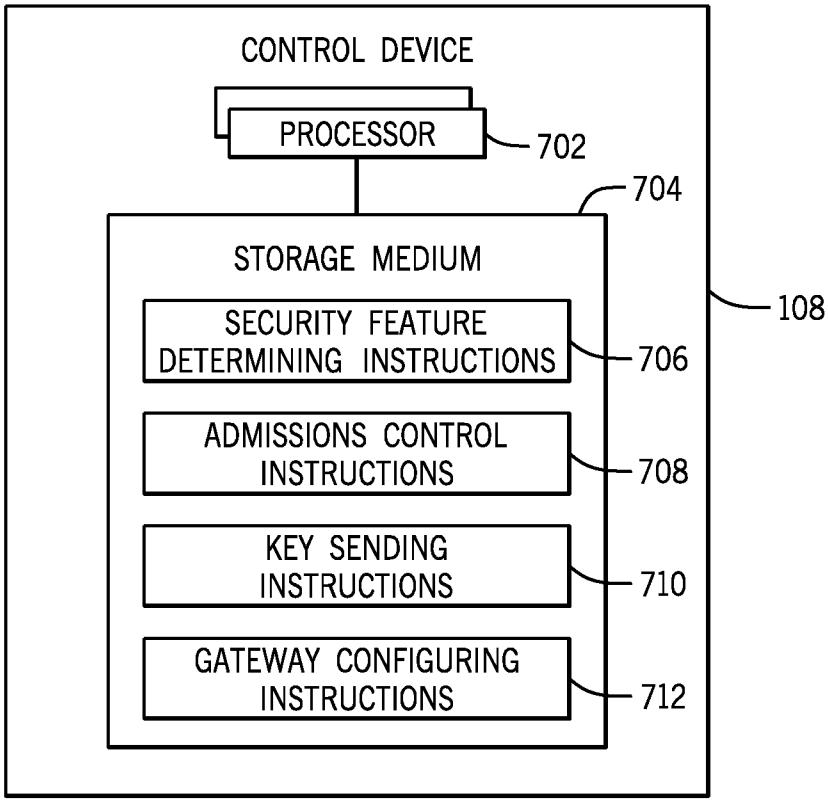
CONTROL DEVICE
PROCESSOR
702
704
STORAGE MEDIUM
SECURITY FEATURE DETERMINING INSTRUCTIONS
706
ADMISSIONS CONTROL INSTRUCTIONS
708
KEY SENDING INSTRUCTIONS
710
GATEWAY CONFIGURING INSTRUCTIONS
712
108

FIG. 7

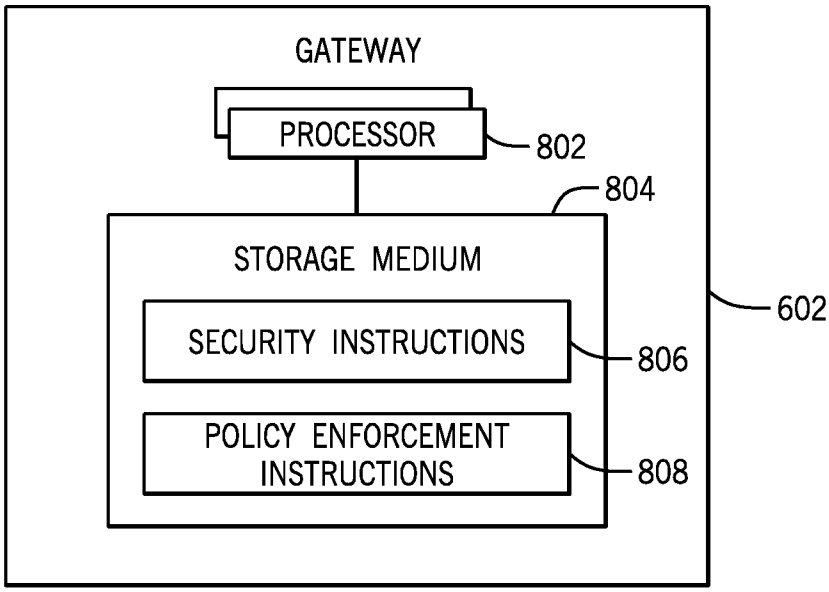
GATEWAY
PROCESSOR
802
804
STORAGE MEDIUM
SECURITY INSTRUCTIONS
806
POLICY ENFORCEMENT INSTRUCTIONS
808
602

FIG. 8

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/US2014/061934**

**A. CLASSIFICATION OF SUBJECT MATTER**

**H04L 9/32(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
H04L 9/32; G06F 13/40; H04J 14/00; H04L 12/50; G06F 9/46; G06F 15/167; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: memory semantic operation, communication fabric, switch, security feature, gateway

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2012-0265840 A1 (ALAN F. BENNER et al.) 18 October 2012<br>See paragraphs [0057]-[0137]; and figures 1-11. | 1-7 |
| Y | | 8-15 |
| Y | US 2009-0073992 A1 (DENNIS HIDEO MAKISHIMA et al.) 19 March 2009<br>See paragraphs [0218]-[0237]; and figures 20-24. | 8-15 |
| A | US 2010-0232793 A1 (MICHAEL W. ATKINSON) 16 September 2010<br>See paragraphs [0026]-[0060]; and figures 1-6. | 1-15 |
| A | US 2004-0049774 A1 (WILLIAM TODD BOYD et al.) 11 March 2004<br>See paragraphs [0079]-[0104]; and figures 6-10. | 1-15 |
| A | US 2014-0115219 A1 (JASMIN AJANOVIE et al.) 24 April 2014<br>See paragraphs [0069]-[0152]; and figures 1-5. | 1-15 |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 10 July 2015 (10.07.2015) | **13 July 2015 (13.07.2015)** |


Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
KIM, Do Weon
Telephone No. +82-42-481-5560

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.
**PCT/US2014/061934**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2012-0265840 A1 | 18/10/2012 | US 2009-0106771 A1 | 23/04/2009 |
| | | US 8244826 B2 | 14/08/2012 |
| | | US 8370447 B2 | 05/02/2013 |
| US 2009-0073992 A1 | 19/03/2009 | US 2006-0023707 A1 | 02/02/2006 |
| | | US 7466712 B2 | 16/12/2008 |
| | | US 8125992 B2 | 28/02/2012 |
| US 2010-0232793 A1 | 16/09/2010 | US 2007-0091903 A1 | 26/04/2007 |
| | | US 2015-0036682 A1 | 05/02/2015 |
| | | US 7760717 B2 | 20/07/2010 |
| | | US 8897294 B2 | 25/11/2014 |
| US 2004-0049774 A1 | 11/03/2004 | AU 2003-255752 A1 | 29/03/2004 |
| | | CN 1679003 A | 05/10/2005 |
| | | CN 1679003 C | 09/04/2008 |
| | | EP 1543422 A1 | 22/06/2005 |
| | | EP 1543422 B1 | 26/02/2014 |
| | | JP 04012545 B2 | 21/11/2007 |
| | | JP 2005-538588 A | 15/12/2005 |
| | | KR 10-0754308 B1 | 03/09/2007 |
| | | KR 10-2005-0057185 A | 16/06/2005 |
| | | MY 127786 A | 29/12/2006 |
| | | US 6721806 B2 | 13/04/2004 |
| | | WO 2004-023305 A1 | 18/03/2004 |
| US 2014-0115219 A1 | 24/04/2014 | US 2014-0304448 A9 | 09/10/2014 |