US 20170374051A1

(19) **United States**

(12) **Patent Application Publication**

Bifulco et al.

(10) **Pub. No.: US 2017/0374051 A1**

(43) **Pub. Date: Dec. 28, 2017**

(54) **METHOD FOR OPERATING A NETWORK AND A NETWORK**

(71) Applicant: **NEC EUROPE LTD.**, Heidelberg (DE)

(72) Inventors: **Roberto Bifulco**, Heidelberg (DE); **Ghassan Karame**, Heidelberg (DE)

(21) Appl. No.: **15/698,703**

(22) Filed: **Sep. 8, 2017**

Related U.S. Application Data

(63) Continuation of application No. 14/904,951, filed on Jan. 14, 2016, now Pat. No. 9,794,244, filed as application No. PCT/EP2013/066435 on Aug. 6, 2013.

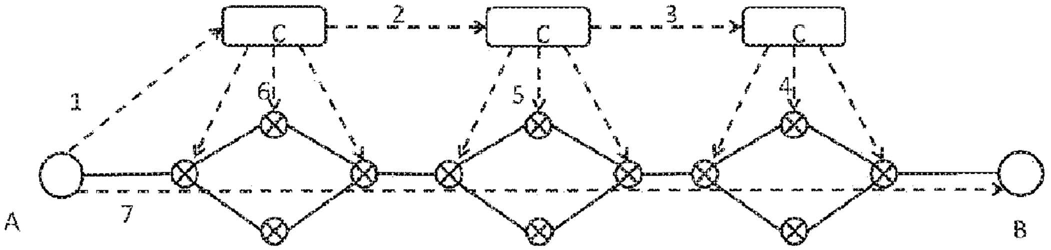
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/08*** (2013.01); ***H04L 63/0823*** (2013.01); ***H04L 63/102*** (2013.01)

(57) **ABSTRACT**

A method for providing a guarantee of a network property includes receiving, from a network user, a signature and a request for the network property, wherein the request for the network property includes a public key of the network user; verifying that the signature received from the network user matches the public key of the network user; demonstrating the capability of providing the network property by determining policies to be installed on nodes of the network so as to enable the network property to be provided; generating, in response to the demonstrating the capability of providing the network property, a secure certificate that contains a secure acknowledgment (ACK) of a commitment to provide the network property; and providing the secure certificate to the network user as a guarantee of the network property.



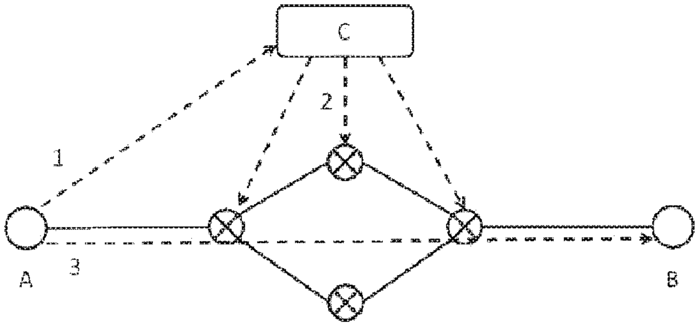


Fig. 1

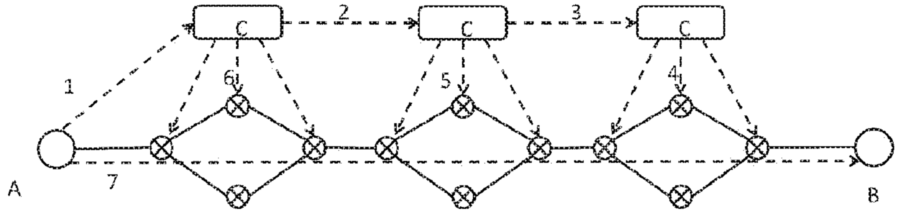


Fig. 2

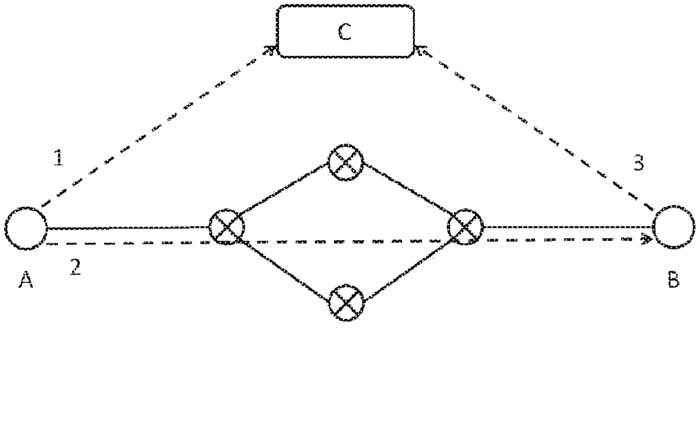


Fig. 3

METHOD FOR OPERATING A NETWORK AND A NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation application of U.S. application Ser. No. 14/904,951, filed on Jan. 14, 2016, which is a continuation of U.S. National Stage Application under 35 U.S.C. §371 of International Application No. PCT/EP2013/066435 filed on Aug. 6, 2013, which was published in English on Feb. 12, 2015 as WO 2015/018436 A1 under PCT Article 21(2). The entire contents of these applications are incorporated by reference herein.

FIELD

[0002] The present invention relates to a method for operating a network, wherein a Software-defined Networking (SDN) functionality between at least some of a plurality of elements of the network is realized by at least one controller and wherein a secure proof of at least one network property is provided.

[0003] Further, the present invention relates to a network, wherein an SDN functionality between at least some of a plurality of elements of the network is realized by at least one controller and wherein a secure proof of at least one network property is provided.

BACKGROUND

[0004] In current internet, end-users consider the network like a black-box that provides connectivity between two endpoints. The security properties, e.g. path guarantees, accountability, properties of connecting hosts, etc., of a communication must be enforced by the endpoints through e.g., encryption/authentication primitives.

[0005] An interesting case is when an endpoint does not trust the claims of the machine at the other end of the communication; this could include the location of the machine, among others. In these cases, the network operator could provide a proof that the untrusted endpoint, e.g., is actually located where it claims to be.

[0006] For simplicity and without loss of generality, assume that an online banking service is provided by endpoint B, and consider the case where a user located at endpoint C wishes to access the online banking service. Here, we consider the case where B allows connections only to endpoints located in a given country, e.g. due to legislations, liability, etc.

[0007] Whenever C is accessing the banking service, B would like to ensure that C is indeed located within a given country. In typical cases, the only way for C to provide a proof of location is to contact its network administrator and acquire such guarantee. While the network itself could in theory provide for such guarantees, this process is quite cumbersome in traditional networks, since it requires a manual intervention, and/or a number of mail exchanges in order to set up such guarantees in practice.

SUMMARY

[0008] In an embodiment, the present invention provides a method for providing a guarantee of a network property from a network in which a domain governing controller governing a domain of a network user provides a Software-Defined Networking (SDN) functionality between a plurality of nodes. The method includes receiving, from a network user, a signature and a request for the network property, wherein the request for the network property includes a public key of the network user; verifying that the signature received from the network user matches the public key of the network user; demonstrating the capability of providing the network property by determining policies to be installed on nodes of the network so as to enable the network property to be provided; generating, in response to the demonstrating the capability of providing the network property, a secure certificate that contains a secure acknowledgment (ACK) of a commitment to provide the network property; and providing the secure certificate to the network user as a guarantee of the network property.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The present invention will be described in even greater detail below based on the exemplary figures. The invention is not limited to the exemplary embodiments. All features described and/or illustrated herein can be used alone or combined in different combinations in embodiments of the invention. The features and advantages of various embodiments of the present invention will become apparent by reading the following detailed description with reference to the attached drawings which illustrate the following:

[0010] FIG. **1** depicts trustworthy network paths for a single SDN domain;

[0011] FIG. **2** depicts trustworthy network paths for multiple SDN domains; and

[0012] FIG. **3** depicts a proof of network location.

DETAILED DESCRIPTION

[0013] Generally, by separating the control plane and data plane, SDNs promise one of the few workable possibilities to automatically and dynamically control network paths.

[0014] An embodiment of the present invention provides a method for operating a network and an according network for allowing a very simple and resource saving provision of secure proofs of network properties.

[0015] According to an embodiment, a method is characterized in that the secure proof of the at least one network property is provided by the SDN functionality.

[0016] According to an embodiment, a network is characterized in that the SDN functionality is enhanced for providing the secure proof of the at least one network property.

[0017] According to an embodiment of the invention, it has been recognized that it is possible to simply use already present functionalities for solving the above object. Concretely, the present SDN functionality will be used for providing the secure proof of at least one network property. This inventive solution is very simple and resource saving only incurring minimal overhead on a SDN controller.

[0018] A secure proof of various network properties is possible and within a preferred embodiment the network property can be network location and/or path property and/or path guarantee. This includes the establishment of "trustworthy paths" that traverse only a selected number of routers or switches, e.g., or that exhibit a given quality metric, providing a proof of location, among other services etc.

[0019] The leveraged SDN functionality can preferably automatically and securely establish provable network guarantees to its clients or users.

[0020] Within a further preferred embodiment a federation of OpenFlow domains can be realized. Within a further concrete embodiment a PM, Public Key Infrastructure, can be provided within the network. Further preferred, all controllers or a definable number of controllers know each other's public key.

[0021] Where appropriate a trusted computing base can be provided within the network. In this case a tamper-resistant hardware, e.g. Trusted Platform Modules, can be realized that populates at least one controller.

[0022] Within a further preferred embodiment at least one network user or each network user can be equipped with a public key and private key pair. Such a pair can be denoted in the sequel by pku, sku for user u.

[0023] Within preferred embodiments proof of path guarantees, proof of location and/or immediate detection of Sybil attacks in the network can be enabled.

[0024] Within a preferred realization of the invention a network user can connect to the controller that governs its own domain using a secure ENI, Endpoint-to-Network Interface, for requesting a network property. The ENI can be predefined. In this way, the ENI enables the user to directly ask for the provisioning of a path with some security properties or for proofs of network guarantees or other network properties.

[0025] If the requested network property extends outside the scope of the network user's domain the network user's domain governing controller can contact at least one other controller using a NNI, Network-to-Network Interface, for transmitting the requested network property.

[0026] If the requested network property can be provided within a network element or network elements controlled by the at least one other controller, the at least one other controller can provide a secure ACK to the network user's domain governing controller.

[0027] Within a further preferred embodiment the network user's domain governing controller generates a secure certificate that contains a secure commitment to the ACK or ACKs sent by the at least one other controller and/or contains a proof of correctness of said network user's domain governing controller and/or contains a statement certifying that the requested network property will be provided and/or contains a signature encapsulating this secure certificate. Such a resulting signed certificate can be called: proof of network guarantee. The encapsulated commitments can be used for liability/accountability purposes by the network user's domain governing controller, e.g., in case other controllers do misbehave.

[0028] With regard to an effective realization of the inventive concept the network user's domain governing controller and/or the at least one other controller can install a forwarding rule on its controlled network element or network elements to enable the requested network property. Within a further preferred embodiment the installed forwarding rule can include a secure tag derived from the secure certificate used to check the presence of said tag in network packets. Such a secure tag can be a packet header tag or a keyed-hash tag.

[0029] With regard to a very effective realization the secure tag taints all packets sent by the network user. Those packets that are tainted with this tag and that abide by installed rule will be treated specially in the network, thus satisfying the user's request.

[0030] If the requested network property is bound by time and/or size and/or by packet count, the network user's domain governing controller and/or the at least one other controller can install a temporary rule on its controlled network element or network elements, wherein said temporary rule will be deleted, once time, size and packet count, respectively, has been reached. This will result in minimum overhead on the controller in maintaining these rules.

[0031] The entire method can be overloaded with an attestation of the controller. Concretely, an attestation of the network user's domain governing controller and/or the at least one other controller can be performed for establishing a correctness of the network user's domain governing controller and/or the at least one other controller.

[0032] Concretely, the requested network property can comprise the guarantee that a data transmission or communication over a path is performed over defined nodes or switches and/or is performed under consideration of a set of constraints on a paths length and/or on a Quality of Service on the path. Additionally or alternatively the requested network property can comprise the guarantee that a data transmission or communication over a path is performed under consideration of a set of constraints on the nodes or switches that the path traverses.

[0033] Various constraints on the nodes or switches could be considered.

[0034] Within a further preferred embodiment the SDN can be realized by OpenFlow.

[0035] Embodiments of the present invention can provide the construction of self-verifiable, secure and accountable receipts that can be used to prove various network properties, e.g., network location, path guarantees, while incurring minimum overhead on the controllers.

[0036] Further, embodiments of the invention can enable the tainting of "differentiated" packets with secure tags that can only be used by users equipped with a genuine certificate/receipt of network property originating from the controllers. These tags ensure minimum overhead on the controllers with regard to rule maintenance and policy compliance checks.

[0037] Further, embodiments of the invention can provide the combination of proofs of network properties with attestation protocols in order to establish guarantees on the correctness of the network.

[0038] Embodiments of the invention can provide:

[0039] 1) Leveraging OpenFlow to enable differentiated services such as proof of location, or proofs of network/path guarantees.

[0040] 2) Achieving verifiable, fully accountable, and unforgeable guarantees while minimizing the efforts required to detect possible misbehavior by malicious users.

[0041] 3) A scalable and secure architecture that supports proofs of network guarantees.

[0042] Embodiments of the invention enable the acquisition of secure proofs of network guarantees or network properties be leveraging the OpenFlow functionality. Respective protocols can be implemented as part of an OpenFlow controller application and do not require any modification to the existing OpenFlow protocol specification.

[0043] Within a preferred embodiment we assume that a network user is interested in acquiring proofs of network guarantees from the operator in order to use it subsequently to access other online services. We further assume the existence of one or more colluding malicious users who wish to forge such proofs of network characteristics in order to fool existing online services. We additionally assume, however, that these users are computationally bounded, and as such cannot forge signatures, break encryption schemes, etc.

[0044] Within the preferred embodiments secure proofs of network properties, such as proof of network location or proof of path properties, are provided, while incurring minimal overhead on the SDN controllers. One solution requires the embedding of secure and unforgeable packet header tags that are tightly coupled with the contract that users signed with an operator.

[0045] The numbers **1** to **3** within FIGS. **1** and **3** and numbers **1** to **7** within FIG. **2** represent the order in which messages between the entities are exchanged.

[0046] With regard to FIGS. **1** and **2**, which are showing trustworthy network paths for a single SDN domain and for multiple SDN domains, the following embodiment of the method is preferred.

[0047] 1. The user A connects to the controller C that governs its own domain using a secure pre-defined Endpoint-to-Network Interface, ENI. This interface enables A to directly ask for the provisioning of a path with some security properties, or for proofs of network guarantees, etc.

[0048] 2. Upon receipt of the request, the controller derives the requirements/policies that need to be set/installed on the switches of the network. In case these policies extend outside the scope of its domain, the controller contacts other controllers using a Network-to-Network Interface (NNI) and informs them of the user requests. These controllers will also investigate the feasibility of the requested rules on their switches and will provide a secure and unforgeable ACK to the original controller that the appropriate rules can be indeed installed.

[0049] 3. The controller will generate an unforgeable and secure certificate that contains a secure commitment to the ACKs sent by other controllers, a proof of correctness of the controller, a statement certifying that what the user requested will be provided, and a signature encapsulating this certificate. We call the resulting signed certificate: proof of network guarantee. Note that the encapsulated commitments can be used for liability/accountability purposes by the original controller, e.g., in case other controllers do misbehave.

[0050] 4. If any controller needs to install any rule on the switches to enable the user request, the rule will check for the presence of a secure tag in the packets sent by the user. The secure tag is derived using a one way transformation solely from the proof of network guarantee, which will taint all packets sent by the user. Those packets that are tainted with this tag, and that abide by installed rule will be treated specially in the network, thus satisfying the user's request. Note that in case the user request is bound by size, or by packet count, the controller will install temporary rules that will be automatically deleted once time, or packet count, has been reached. As we show later, this entire process ensures the security of the entire scheme, while resulting in minimum overhead on the controller in maintaining these rules and verifying compliance. Indeed, in case of any violation, any controller can request from the users the proof of network guarantee and see whether it matches with the tag. The controller can then directly eliminate fake/forged packets by illegitimate users without the need to invest considerable resources.

[0051] 5. This entire process can be overloaded with an attestation of the controller. This can be used to establish the correctness of the controller, and hence the correctness of the SDN or OpenFlow domain.

Embodiment 1: Trustworthy Network Paths

[0052] An exemplary property that can be required by a given user is to guarantee that the communication flow over a path satisfies some conditions. These conditions could be in the form of:

[0053] 1. The ID of the nodes or switches on the path

[0054] 2. A set of constraints on the path length/quality of service

[0055] 3. A set of constraints on the nodes or switches that the path traverses, e.g., location.

[0056] In this case, the user A issues to the controller CONT over the ENI interface the following message:

[0057] M1: IP of A||pka||IP of end-node on the path||CONSTRAINTS||Duration of contract||Timestamp||R

[0058] Here, || denotes message concatenation. A also appends the corresponding signature Sig(M1). Pka is included in this message in order to prevent IP spoofing, in case the spoofer is co-located with the user machine. R is a random fresh nonce used for attestation purposes. R could be computed as h(Timestamp).

[0059] Upon receipt of M1||Siga(M1), CONT checks the feasibility of the user's request given in the network topology. In case this request requires the cooperation of another collaborating domain, CONT forwards (M1||Siga(M1)||SigCONT(M1||Siga(M1)||Timestamp) to the collaborating controller CONT2. These controllers would then check the feasibility of installing the request in M1 on their domains and will issue an ACK: OK||M1||Siga(M1)||SigCONT (M1||Siga(M1)||Timestamp||ATTcont2, along with the signature SigCONT2(ACK). Here ATTcont2 is an attestation response by CONT2. Upon reception of the ACK, CONT issues a final ACK to A in the form:

[0060] RECEIPT: OK: IP of A||IP of end-node on the path||CONSTRAINTS||Duration of contract||Timestamp||h (ACK)||ATTcont, along with the signature on the RECEIPT.

[0061] The h(ACK) acts as a commitment that could be revealed anytime when challenged. In fact, in the case that the quality of service degrades, or the user is not satisfied, CONT can prove by showing ACK that CONT did its due diligence in satisfying the user's request. This also can be used to held another controller liable. Note that this entire process is recursive e.g., if CONT2 needs to involve another controller.

[0062] CONT also installs a rule matching to the request M1 and asks that all packets originating from IP of A destined to IP of end-node on the path that are tagged with the header filed h(RECEIPT) will undergo that rule.

[0063] This technique prevents forgery. Any other user cannot benefit from the rule. This is the case since any packet containing the same tag and originating from a malicious user will cause the message to be forwarded to the controller. The controller simply asks for the RECEIPT and checks if the receipt does indeed match the hash. If so, then the controller invests resources in resolving the problem. Otherwise, the connection is banned.

Alternative Variant:

[0064] Another way to achieve a similar functionality would be to rely on keyed-hashed tags. Here, the users would keep on updating the tags following the output of a keyed-hash function. However, this requires an additional functionality to be installed at the switches; indeed, these switches need to also be able to verify these tags and therefore require an algorithm that implements a keyed-hash.

Tag Implementation Strategy:

[0065] Several strategies can be exploited for the implementation of the TAG required in the network packets. In particular, any current protocol header can work as a TAG, provided that it is compatible with the properties of the network protocols. For example, the TOS field of IP header, VLAN or MPLS tags, are all candidates to this purpose. Another example is using an IPv6 source address that contains the TAG in the part defined by the end-point.

Sybil Attacks/Forgery Detection:

[0066] Given that A is connected to PORTa of switch SW1, during the A request for the path, CONT can store the knowledge that A is located at PORTa-SW1. Any tag h(RECEIPT) located at a different port/switch has to be immediately discarded or proper actions can be taken, e.g., asking for a new receipt.

[0067] When involving multiple domains and controllers, the procedure is recursive. A controller, when contacting another controller for setting up the trustworthy path, declares the entering port/switch to the next controller whose managed domain is on the path.

[0068] From this port/switch only correctly tagged packets are allowed to flow, since the transmitting domain has applied already filtering at its borders. Hence, a chain of controller collaborating for the provisioning of the path can actually guarantee that the path is taken only by allowed traffic, provided that each controller enforces the check on the starting point of the flow for its managed domain.

Embodiment 2: Proof of Network Location

[0069] We now propose another embodiment in which a user can obtain a verifiable proof of location certificate that he can present to any other service, thus proving that he has a machine operating from a given location.

[0070] Consider FIG. **3** where the endpoint A wants to establish a connection with B, but B requires A to prove that it is in a given location. A asks in first place a certification token to C, who is charge of controlling the network between A and B. C is the controller of the domain of A.

[0071] Here, A issues the following request:

M1: IP of A||pka||LocationRequest||Timestamp||R

[0072] Along with the signature Sig(M1).

[0073] Upon request of M1, the controller, then verifies Sig(M1) matches with pka, verifies the IP of A, and then issues the following proof of location (POL) response:

POL: IP of A||pka||Country/city/area||Timestamp||ATTb||R||h(M1)

[0074] Along with its signature Sig(POL). A then forwards POL||Sig(POL) to B who can verify the authenticity of POL.

Another Variant:

[0075] A variant protocol can be established to allow B to directly query the location of A. Here, if B and A are not in the same OpenFlow domain, then the controller of the domain of B will forward B's request to the corresponding controller.

[0076] While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplary and not restrictive. It will be understood that changes and modifications may be made by those of ordinary skill within the scope of the following claims. In particular, the present invention covers further embodiments with any combination of features from different embodiments described above and below.

[0077] The terms used in the claims should be construed to have the broadest reasonable interpretation consistent with the foregoing description. For example, the use of the article "a" or "the" in introducing an element should not be interpreted as being exclusive of a plurality of elements. Likewise, the recitation of "or" should be interpreted as being inclusive, such that the recitation of "A or B" is not exclusive of "A and B," unless it is clear from the context or the foregoing description that only one of A and B is intended. Further, the recitation of "at least one of A, B and C" should be interpreted as one or more of a group of elements consisting of A, B and C, and should not be interpreted as requiring at least one of each of the listed elements A, B and C, regardless of whether A, B and C are related as categories or otherwise. Moreover, the recitation of "A, B and/or C" or "at least one of A, B or C" should be interpreted as including any singular entity from the listed elements, e.g., A, any subset from the listed elements, e.g., A and B, or the entire list of elements A, B and C.

What is claimed is:

1. A method for providing a guarantee of a network property from a network in which a domain governing controller governing a domain of a network user provides a Software-Defined Networking (SDN) functionality between a plurality of nodes, the method comprising:

receiving, from the network user, a signature and a request for the network property, wherein the request for the network property includes a public key of the network user;

verifying that the signature received from the network user matches the public key of the network user;

demonstrating the capability of providing the network property by determining policies to be installed on nodes of the network so as to enable the network property to be provided;

generating, in response to the demonstrating the capability of providing the network property, a secure certificate that contains a secure acknowledgment (ACK) of a commitment to provide the network property; and

providing the secure certificate to the network user as a guarantee of the network property.

2. The method according to claim **1**, wherein the network property is at least one of a network location, a path property, or a path guarantee.

3. The method according to claim **1**, wherein a Public Key Infrastructure (PM) is provided within the network.

4. The method according to claim **3**, wherein each controller in a group of a definable number of controllers know a public key of the other controllers.

5. The method according to claim **1**, wherein a trusted computing base is provided within the network.

6. The method according to claim **1**, wherein a tamper-resistant hardware populates the at least one controller.

7. The method according to claim **1**, wherein the network user is equipped with a public key and private key pair.

8. The method according to claim **1**, wherein the signature and the request for the network property are received by the domain governing controller via a secure Endpoint-to-Network Interface (ENI).

9. The method according to claim **8**, further comprising contacting, by the domain governing controller, at least one other controller via a Network-to-Network Interface (NNI); and

transmitting the network property to the at least one other controller using the NNI.

10. The method according to claim **9**, wherein the at least one other controller provides a secure acknowledgement (ACK) of a commitment to provide the network property to the domain governing controller in response to a determination, by the at least one other controller, that one or more network nodes controlled by the at least one other controller are capable of providing the network property.

11. The method according to claim **10**, wherein the secure certificate at least one of: includes the secure acknowledgment (ACK) of the commitment to provide the network property provided by the at least one other controller, contains a proof of correctness of the domain governing controller, or contains a statement certifying that the requested network property will be provided.

12. The method according to claim **1**, further comprising installing the policies to be installed on nodes of the network so as to enable the network property to be provided.

13. The method according to claim **12**, wherein the installed policies include a forwarding rule that determines whether network packets include a secure tag derived from the secure certificate provided to the network user.

14. The method according to claim **13**, wherein the secure tag is a packet header tag.

15. The method according to claim **13**, wherein the secure tag is a keyed-hash tag.

16. The method according to claim **13**, wherein the secure tag taints all packets sent by the network user.

17. The method according to claim **12**, wherein if the requested network property is bound by at least one of time, size, or packet count, the installed policies include a temporary rule that will be deleted once reaching a bound of at least one of time, size, or packet count.

18. The method according to claim **1**, further comprising performing an attestation of the domain governing controller for establishing a correctness of the domain governing controller.

19. The method according to claim **1**, wherein the requested network property comprises a guarantee that a data transmission or communication over a path is performed over defined nodes or switches.

20. The method according to claim **1**, wherein the requested network property comprises a guarantee that a data transmission or communication over a path is performed under consideration of a set of constraints on at least one of a path length or a Quality of Service (QoS) on the path.

21. The method according to claim **1**, wherein the requested network property comprises a guarantee that a data transmission or communication over a path is performed under consideration of a set of constraints on the nodes or switches that the path traverses.

22. The method according to claim **1**, wherein the SDN is realized by OpenFlow.

23. A network for providing a guarantee of a network property, the network comprising:

a domain governing controller governing a domain of a network user configured to:

provide a Software-Defined Networking (SDN) functionality between a plurality of nodes,

receive, from the network user, a signature and a request for the network property, wherein the request for the network property includes a public key of the network user;

verify that the signature received from the network user matches the public key of the network user;

demonstrate the capability of providing the network property by determining policies to be installed on nodes of the network so as to enable the network property to be provided

generate, in response to demonstrating the capability of providing the network property, a secure certificate that contains a secure acknowledgment (ACK) of a commitment to provide the network property; and

provide the secure certificate to the network user as a guarantee of the network property.

* * * * *