September 18, 2018

INFORMATION CENTRIC NETWORKING INTEREST SIGNALED DYNAMIC DATA INTEGRITY VALIDATION OFFLOAD TO FOG NODE OR MOBILE EDGE COMPUTING NODE

Nagendra Kumar Nainar

Carlos M. Pignataro

Luca Muscariello

INFORMATION CENTRIC NETWORKING INTEREST SIGNALED DYNAMIC DATA INTEGRITY VALIDATION OFFLOAD TO FOG NODE OR MOBILE EDGE COMPUTING NODE

AUTHORS:
Nagendra Kumar Nainar
Carlos M. Pignataro
Luca Muscariello

ABSTRACT

Techniques are described herein for offloading the responsibility of validation to an edge node such as a fog router or Mobile Edge Computing (MEC) platform by signaling the same in an Interest packet or using another Out-of-Band (OOB) mechanism. Upon receiving the Interest packet, the edge node creates the local state entry in a Pending Interest Table (PIT) and marks the entry for local integrity validation. The edge node uses any mechanism to retrieve the public key and perform the validation on behalf of the sensors/end-users.

DETAILED DESCRIPTION

Data integrity validation is one of the basic and mandatory requirements in Information Centric Networking (ICN) / hybrid ICN (hICN).

While there are various proposals available in the industry on how the Public Key Infrastructure (PKI) should be implemented for ICN/hICN, most involve base machinery where each data chunk is digitally signed using a data producer's private key and the data consumers use the associated public key to validate the data integrity. How the keys are exchanged between producer and consumer varies depending on the proposal.

With any of these options, the need to maintain the flow specific to the public key and perform the data integrity validation consumes additional power and other resource cycles that is very costly in the Internet of Things (IoT) and mobile world.

The cost of validation is twofold: integrity hash computation and signature computation.

Figures 1-3 below illustrate the goodput of an application using the hICN stack implemented in Vector Packet Processing (VPP) in different cases. A producer computes integrity SHA-256 hashes and a signature over a block of hashes contained in a manifest

packet using RSA-2014 or ECDSA-192. The cost of verifications brings the goodput from about 3Gbps down to 1Gbps in the best case (RSA) or 300Mbps (ECDSA). If the applications cannot perform computation on blocks of data but only on a per-packet basis (e.g., small IoT sensors sending temperature measurements) the cost of cryptography becomes very high as the goodput drops to about 30 Mbps.

Offloading to hardware is always a good option for cryptographic operations but in most cases is very expensive in the IoT in terms of power consumption.

Offloading these computations to a trusted compute appliance is an opportunity to optimize IoT use cases without trading it off with security.

Type of test	Average	99% CI
(h)ICN Asynchronous Publication		
Manifest RSA-1024	928Mbps	[919 936]
Packet-wise RSA-1024	290Mbps	[283 297]
Manifest ECDSA-192	531Mbps	[523 538]
Packet-wise ECDSA-192	28Mbps	[27 28]
(h)ICN Synchronous Publication		
Manifest RSA-1024	525Mbps	[518 532]
Packet-wise RSA-1024	26Mbps	[26 27]
Manifest ECDSA-192	530Mbps	[522 537]
Packet-wise ECDSA-192	28Mbps	[28 29]
(h)ICN Crypto Operations disabled		
No signature	2.45Gbps	[2.43 2.46]
No signature, 2 transfers	3.16Gbps	[3.13 3.19] Jain=0.99
No signature, 3 transfers	3.69Gbps	[3.43 3.95] Jain=0.98
TCP - Iperf		
Linux TCP (w/ TSO)	9.19Gbps	[9.09 9.30]
Linux TCP (w/o TSO)	5.00Gbps	[4.88 5.12]
VPP TCP stack	9.24Gbps	[9.22 9.26]

Figure 1

	Vector of packets		Single packet	
Consumer: Signature verification				
RSA-1024	52.2us	[51.5 52.9]	140us	[132 149]
ECDSA-192	412us	[406 417]	757us	[697 817]
Producer: Signature computation				
RSA-1024	440us	[437 443]	775us	[733 818]
ECDSA-192	380us	[377 383]	701us	[661 740]
SHA-256 hash computation on MTU packet				
1.5kB	9.44us	[9.38 9.50]	28.62us	[31.03 32.08]
9kB	31.55us	[31.03 32.08]	68.26us	[63.63 72.89]

Figure 2

Type of test	Average	99% CI
No signature	145us	[136 155]
RSA-1024	1173us	[1142 1205]
ECDSA-192	1667us	[1621 1712]

Figure 3

Accordingly, described herein is a hICN dataplane (Interest) signaled dynamic mechanism to offload the ICN data integrity validation to a fog router or Mobile Edge Computing (MEC) platform if the IoT sensors are connected over a 5G environment. This machinery leverages the computing capability of fog routers / MEC platforms and dynamically signals the interest of offloading the public key retrieval and data validation on the ICN data before forwarding the data packets to the end user (sensor or 5G user equipment).

Any ICN/hICN consumers may be provisioned to offload the data integrity validation to the edge device. The consumers that are provisioned to offload the integrity validation may signal the same to the edge node. There are at least two potential ways of achieving this: ICN interest based signaling and ICN data integrity validation.

Figure 4 below illustrates ICN interest based signaling.

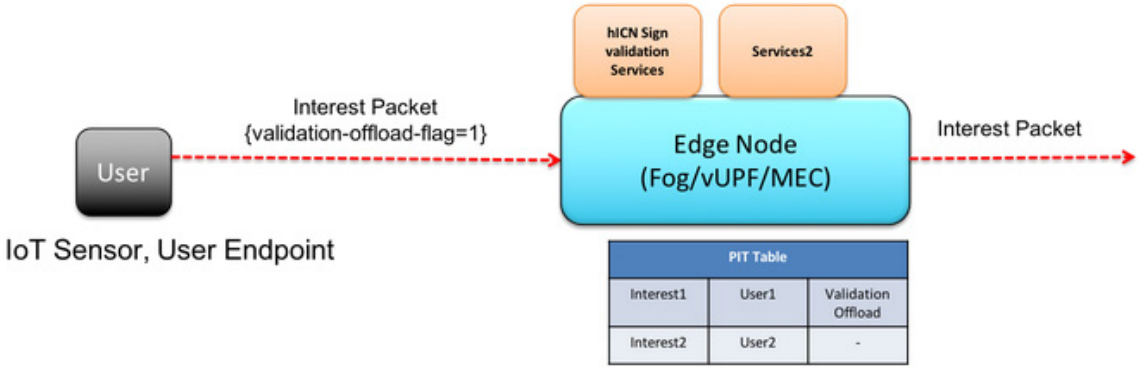

Figure 4

In this approach, the user may send the ICN/hICN Interest packet towards the fog router, which is expected to create a state entry in the local Pending Interest Table (PIT). The edge node may run a local service referred to herein as the ICN-Signature Validation service (ICN-SV). This service may be enabled as a local process on the edge node, a virtual service function that is running on an edge computing device (e.g., fog router, MEC platform, etc.), or a virtual Network Function (vNF) as part of a service chain positioned anywhere in the domain in a bidirectional manner.

When the user/consumer sends the Interest packet for any data chunk, the user may include a metadata (or a flag) that signals the Interest to offload the integrity validation. Upon receiving it, the ICN-SV may create relevant state entries in the PIT and mark a flag in the local table for validation. The ICN-SV may use the content name in the received Interest packet to retrieve the relevant public key details and maintain the keys for different Interest/data packets to the respective user/sensor.

There are two modes for the user to delegate the signature validation depending on the mechanism used for validation. First, the user may insert the public key of the producer in the interest payload field so that the MEC node, which is a trusted/authenticated entity, can very quickly verify the signature as soon as the data comes back. Second, the user equipment may not insert the public key and allow the MEC node to use the key locator to retrieve the key first and perform the validation service.

The first mode allows higher scaling at the MEC, which only offers Central Processing Unit (CPU) power while the second mode offloads public key retrieval, key storage, and CPU processing. But it consumes more resources at the MEC node.

Figure 5 below illustrates ICN data integrity validation. As shown, ICN-SV may clear the metadata before forwarding the Interest packet further upstream towards the content store or the producer.

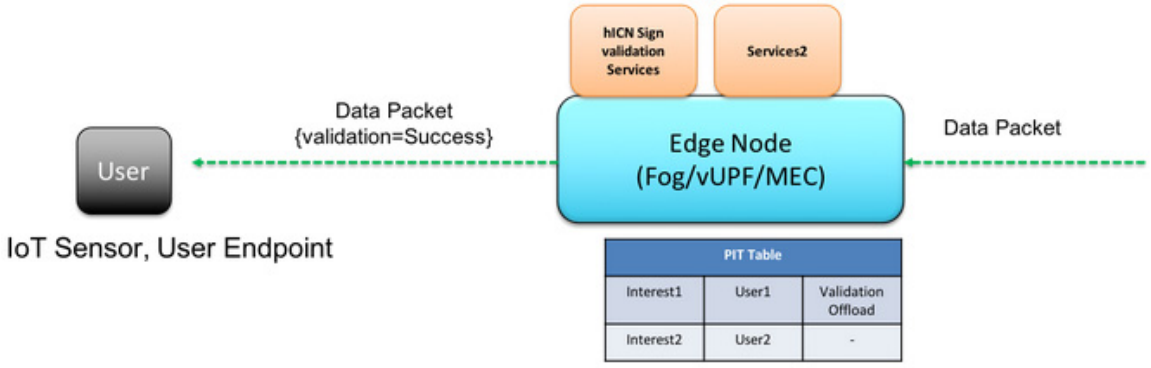

Figure 5

Upon receiving the data traffic for the Interest packet, the ICN-SV may identify that the packet needs offloaded validation based on the table lookup.

It may use the relevant public key and verify the digital signature on the received data chunk before forwarding to the user. Additionally, it may include minimal details in the metadata field of the data packet with a flag to signal the successful validation of the signature.

In case of validation failure, ICN-SV may send a null data packet with the relevant error message (or an equivalent to Internet Control Message Protocol (ICMP) for error signaling).

While the techniques provided herein are described in the context of IoT sensors, they are broadly applicable in other environments such as connectivity vehicles, 5G mobile users, etc.

A dynamic approach is described herein that leverages a dataplane based signaling approach and “signals” the intent to offload the data integrity validation on a per data request basis by including the intent directly in the ICN Interest packet. The successful data integrity validation may be signaled back in the ICN data packet, thereby leveraging the dataplane for reliable signaling of ICN data integrity offload in a connectionless (yet reliable) manner.

This concerns authenticity and integrity validation, which is mandatory in ICN, while confidentiality is optional and left to the upper layers. Moreover, the validation process may not require trust delegation of any sort, but only validation offload.

The mechanisms described herein may be agnostic to the type of data/content exchanges between producer/consumer. The nature of ICN requires a robust, scalable manner of signaling and offloading the integrity validation. This is achieved using dataplane based signaling by leveraging the existing/defined Interest/data packet header itself.

In summary, techniques are described herein for offloading the responsibility of validation to an edge node such as a fog router or MEC platform by signaling the same in an Interest packet or using another Out-of-Band (OOB) mechanism. Upon receiving the Interest packet, the edge node creates the local state entry in a PIT and marks the entry for local Integrity validation. The edge node uses any mechanism to retrieve the public key and perform the validation on behalf of the sensors/end-users.