

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 15 August 2022

J. Preuß Mattsson  
G. Selander  
Ericsson  
C. Amsüss  
Energy Harvesting Solutions  
11 February 2022

Amplification Attacks Using the Constrained Application Protocol (CoAP)  
[draft-mattsson-t2trg-amplification-attacks-00](#)

Abstract

Protecting Internet of Things (IoT) devices against attacks is not enough. IoT deployments need to make sure that they are not used for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks are typically done with compromised devices or with amplification attacks using a spoofed source address. This document gives examples of different theoretical amplification attacks using the Constrained Application Protocol (CoAP). The goal with this document is to raise awareness and to motivate generic and protocol-specific recommendations on the usage of CoAP. Some of the discussed attacks can be mitigated by not using NoSec or by using the Echo option.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 August 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

CoAP Amplification Attacks

February 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Amplification Attacks using CoAP . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	Simple Amplification Attacks . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Amplification Attacks using Observe . . . . .	<a href="#">5</a>
<a href="#">2.3.</a>	Amplification Attacks using Group Requests . . . . .	<a href="#">7</a>
<a href="#">2.4.</a>	MITM Amplification Attacks . . . . .	<a href="#">8</a>
<a href="#">3.</a>	Summary . . . . .	<a href="#">10</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">11</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">11</a>
<a href="#">6.</a>	Informative References . . . . .	<a href="#">11</a>
	Acknowledgements . . . . .	<a href="#">14</a>
	Authors' Addresses . . . . .	<a href="#">14</a>

## [1.](#) Introduction

One important protocol used to interact with Internet of Things (IoT) sensors and actuators is the Constrained Application Protocol (CoAP) [[RFC7252](#)]. CoAP can be used without security in the so called NoSec mode but any Internet-of-Things (IoT) deployment valuing security and privacy would use a security protocol such as DTLS [[I-D.ietf-tls-dtls13](#)], TLS [[RFC8446](#)], or OSCORE [[RFC8613](#)] to protect CoAP, where the choice of security protocol depends on the transport protocol and the presence of intermediaries. The use of CoAP over UDP and DTLS is specified in [[RFC7252](#)] and the use of CoAP over TCP and TLS is specified in [[RFC8323](#)]. OSCORE protects CoAP end-to-end with the use of COSE [[RFC8152](#)] and the CoAP Object-Security option [[RFC8613](#)] and can therefore be used over any transport. Group OSCORE [[I-D.ietf-core-oscore-groupcomm](#)] can be used to protect CoAP Group Communication [[I-D.ietf-core-groupcomm-bis](#)].

Protecting Internet of Things (IoT) devices against attacks is not enough. IoT deployments need to make sure that they are not used for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks are typically done with compromised devices or with amplification attacks using a spoofed source address. DDoS attacks is a huge and growing

problem for services and critical infrastructure [[DDoS-Infra](#)].

The document gives examples of different theoretical amplification attacks using CoAP. When transported over UDP, the CoAP NoSec mode is susceptible to source IP address spoofing and as a single request

can result in multiple responses from multiple servers, CoAP can have very large amplification factors. The goal with this document is to raise awareness and to motivate generic and protocol-specific recommendations on the usage of CoAP.

Some of the discussed attacks can be mitigated by not using NoSec or by using the Echo option [[I-D.ietf-core-echo-request-tag](#)].

## [2.](#) Amplification Attacks using CoAP

In a Denial-of-Service (DoS) attack, an attacker sends a large number of requests or responses to a target endpoint. The denial-of-service might be caused by the target endpoint receiving a large amount of data, sending a large amount of data, doing heavy processing, or using too much memory, etc. In a Distributed Denial-of-Service (DDoS) attack, the request or responses come from a large number of sources.

In an amplification attack, the amplification factor is the ratio between the total size of the data sent to the target and the total size of the data sent by the attacker. In the attacks described in this section, the attacker sends one or more requests, and the target receives one or more responses. An amplification attack alone can be a denial-of-service attack on a CoAP server by making it send a large amount of data. But often amplification attacks are combined with the attacker spoofing the source IP address of the targeted victim. By requesting as much information as possible from several servers an attacker can multiply the amount of traffic and create a distributed denial-of-service attack on the target. When transported over UDP, the CoAP NoSec mode is susceptible to source IP address spoofing.

Amplification attacks with CoAP are unfortunately not only theory. Powerful CoAP amplification attacks made headlines in 2018, reaching 55 Gbps on average, and with the largest one clocking at 320 Gbps [[DDoS-ZDNET](#)]. But in 2019, they were hardly seen anymore [[DDoS-2019](#)]. In 2020, the FBI cyber division mentioned CoAP in a

public notification warning that cyber actors are increasingly likely to abuse network protocols for DDoS attacks [[DDoS-FBI](#)]. CoAP amplification attacks made a comeback in 2020 and CoAP was behind a significant part of global DDoS attacks in Q4 2020 and Q1 2021, but not at all in Q2 and Q3 of 2021 [[DDoS-2021](#)]. It seems unclear exactly how the attacks were done, why they stopped, and how likely CoAP amplifications attacks are to come back in the future.

The following sections give examples of different theoretical amplification attacks using CoAP.

## 2.1. Simple Amplification Attacks

An amplification attack using a single response is illustrated in Figure 1. If the response is  $c$  times larger than the request, the amplification factor is  $c$ .

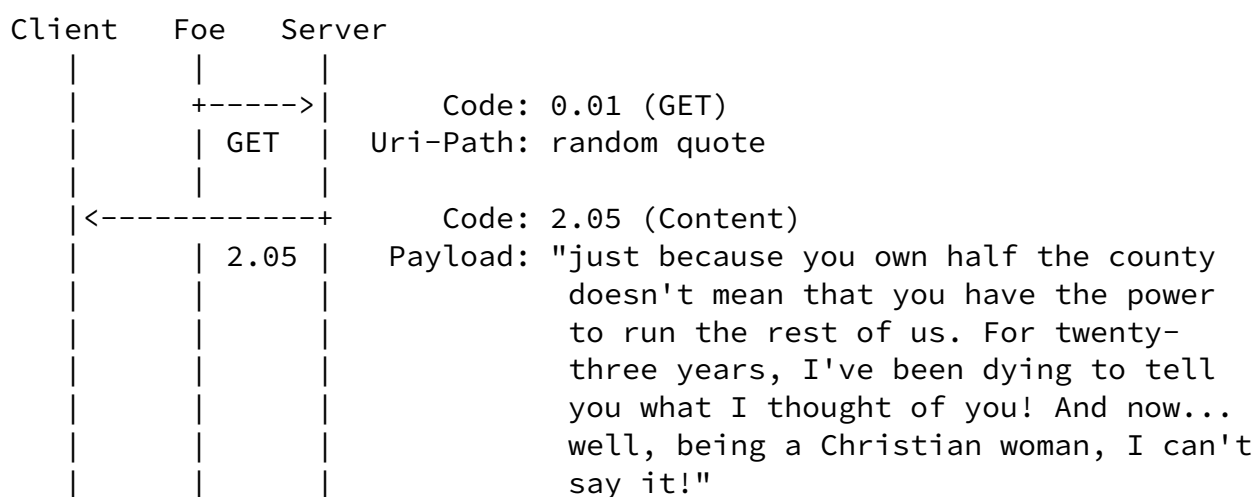


Figure 1: Amplification attack using a single response

An attacker can increase the bandwidth by sending several GET requests. An attacker can also increase or control the amplification factor by creating or updating resources. By creating new resources, an attacker can increase the size of /.well-known/core. An amplification attack where the attacker influences the amplification factor is illustrated in Figure 2.

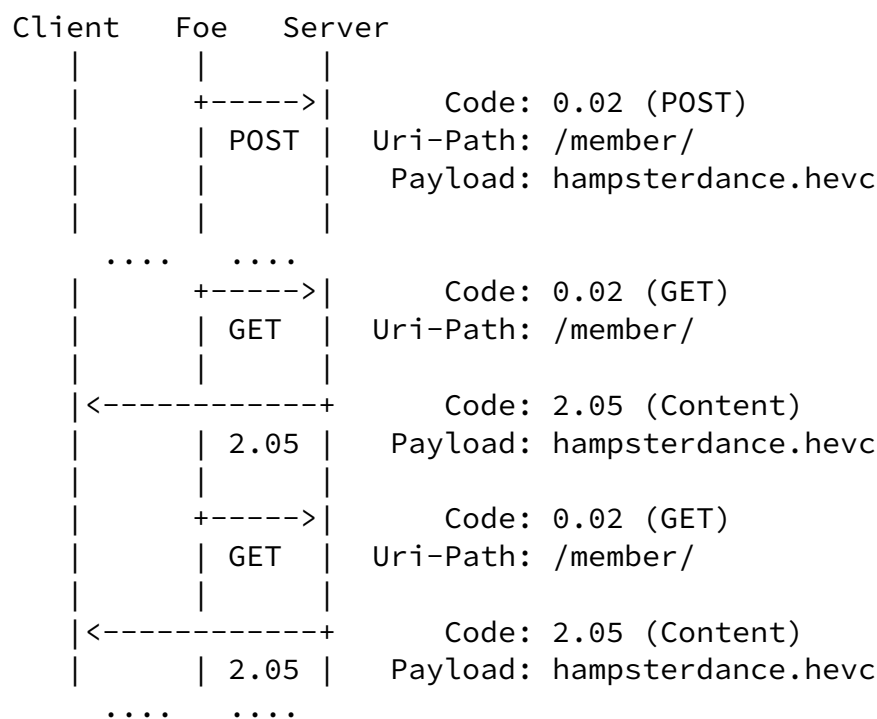


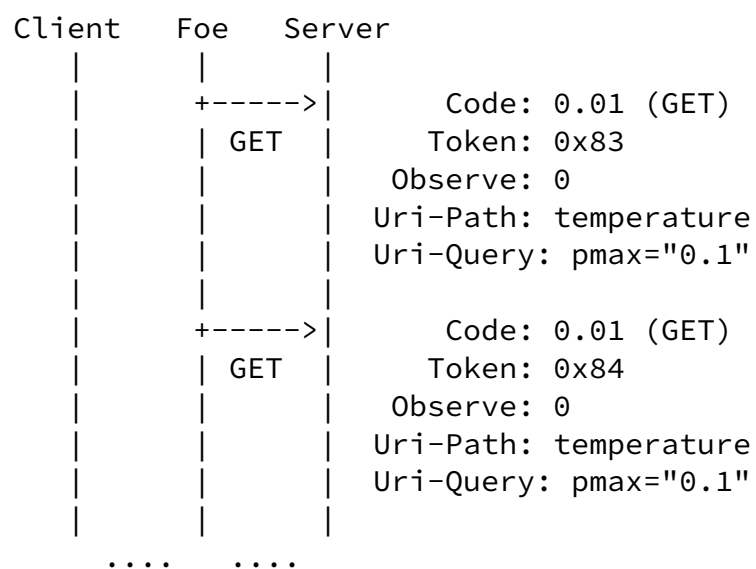
Figure 2: Amplification attack using several requests and a chosen amplification factor

## 2.2. Amplification Attacks using Observe

Amplification factors can be significantly worse when combined with observe [[RFC7641](#)] and group requests [[I-D.ietf-core-groupcomm-bis](#)]. As a single request can result in multiple responses from multiple servers, the amplification factors can be very large.

An amplification attack using observe is illustrated in Figure 3. If each notification response is  $c$  times larger than the registration request and each request results in  $n$  notifications, the amplification factor is  $c * n$ . By registering the same client several times using different Tokens or port numbers, the bandwidth can be increased. By updating the observed resource, the attacker may trigger notifications and increase the size of the notifications. By using conditional attributes [[I-D.ietf-core-conditional-attributes](#)] an attacker may increase the frequency of notifications and therefore the amplification factor. The maximum period attribute  $p_{max}$  indicates the maximum time, in seconds, between two consecutive notifications (whether or not the

resource state has changed). If it is predictable when notifications are sent as confirmable and which Message ID are used the acknowledgements may be spoofed.



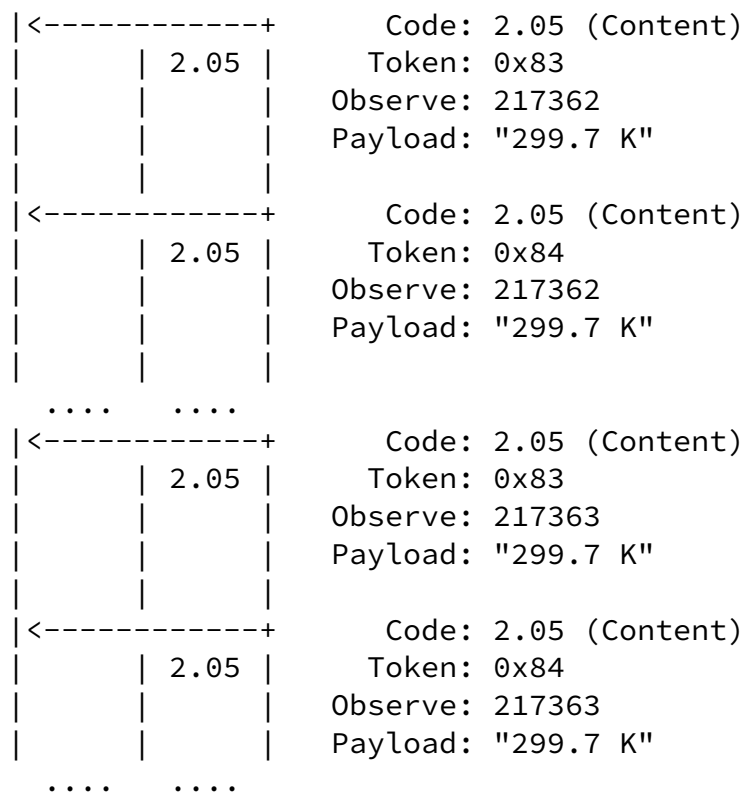


Figure 3: Amplification attack using observe, registering the same client several times, and requesting notifications at least 10 times every second

### [2.3.](#) Amplification Attacks using Group Requests

An amplification attack using a group request is illustrated in Figure 4. The group request is sent over multicast or broadcast and in this case a single request results in  $m$  responses from  $m$  different servers. If each response is  $c$  times larger than the request, the amplification factor is  $c * m$ . Note that the servers usually do not know the variable  $m$ .

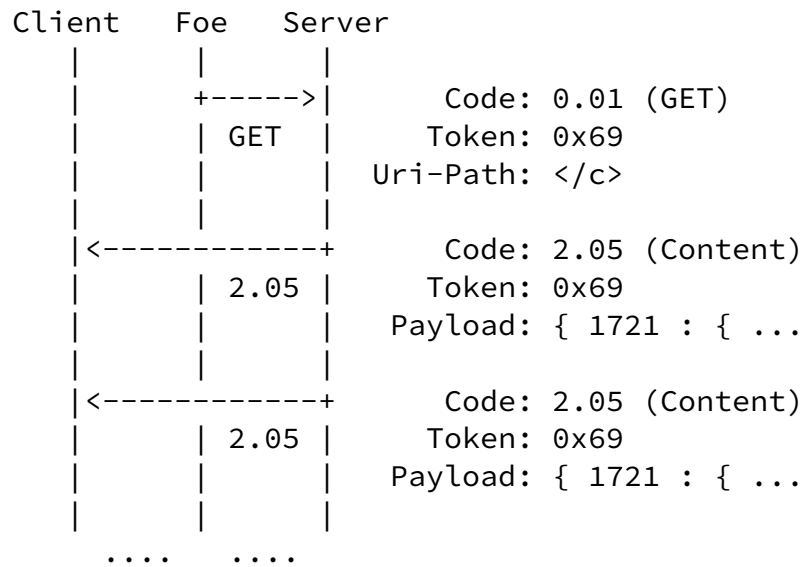


Figure 4: Amplification attack using multicast

An amplification attack using a multicast request and observe is illustrated in Figure 5. In this case a single request results in  $n$  responses each from  $m$  different servers giving a total of  $n * m$  responses. If each response is  $c$  times larger than the request, the amplification factor is  $c * n * m$ .



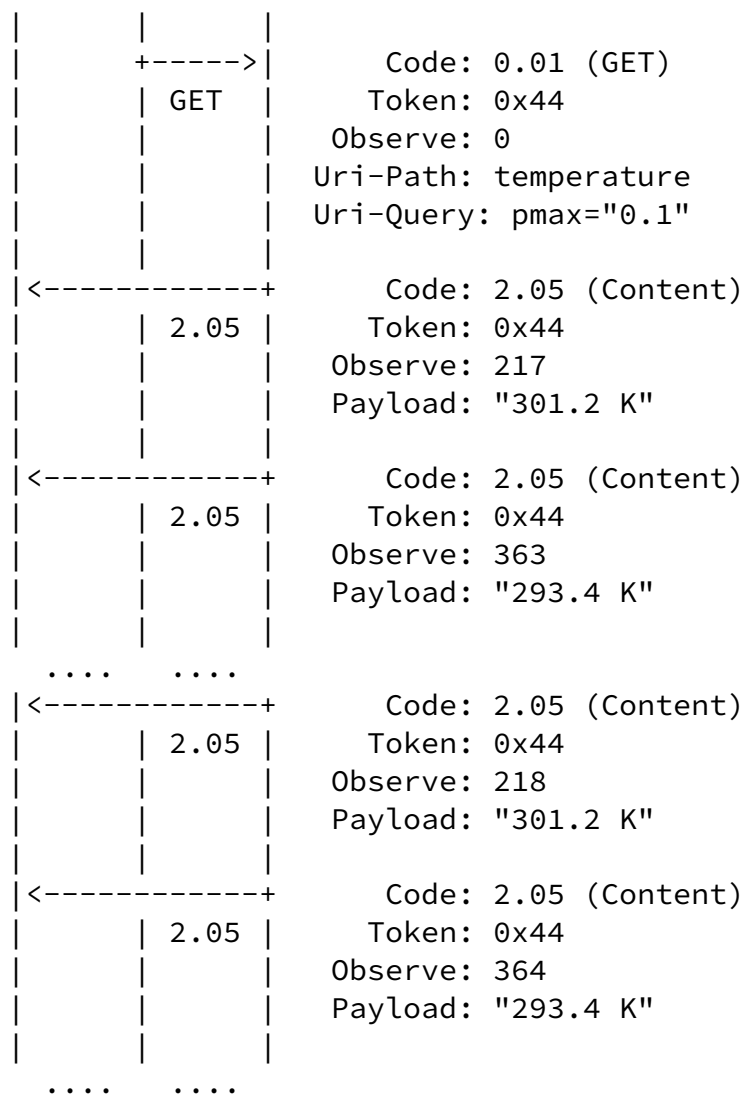


Figure 5: Amplification attack using multicast and observe

#### 2.4. MITM Amplification Attacks

TLS and DTLS without Connection ID [[I-D.ietf-tls-dtls-connection-id](#)] validate the IP address and port of the other peer, binds them to the connection, and do not allow them to change. DTLS with Connection ID allows the IP address and port to change at any time. As the source address is not protected, an MITM attacker can change the address. Note that an MITM attacker is a more capable attacker than an attacker just spoofing the source address. It can be discussed if and how much such an attack is reasonable for DDoS, but DTLS 1.3 states that "This attack is of concern when there is a large asymmetry of request/response message sizes." [[I-D.ietf-tls-dtls13](#)].

DTLS 1.2 with Connection ID [[I-D.ietf-tls-dtls-connection-id](#)] requires that "the receiver MUST NOT replace the address" unless "there is a strategy for ensuring that the new peer address is able to receive and process DTLS records" but does not give more details than that. It seems like the receiver can start using the new peer address and test that it is able to receive and process DTLS records at some later point. DTLS 1.3 with Connection ID requires that "implementations MUST NOT update the address" unless "they first perform some reachability test" but does not give more details than that. OSCORE [[RFC8613](#)] does not discuss address updates, but it can be assumed that most servers send responses to the address it received the request from without any reachability test. A difference between (D)TLS and OSCORE is that in DTLS the updated address is used for all future records, while in OSCORE a new address is only used for responses to a specific request.

An MITM amplification attack updating the client's source address in an observe registration is illustrated in Figure 6. This attack is possible in OSCORE and DTLS with Connection ID. The server will send notifications to the Victim until it at some unspecified point requires an acknowledgement [[RFC7641](#)]. In DTLS 1.2 the reachability test might be done at a later point. In OSCORE a reachability test is likely not done.

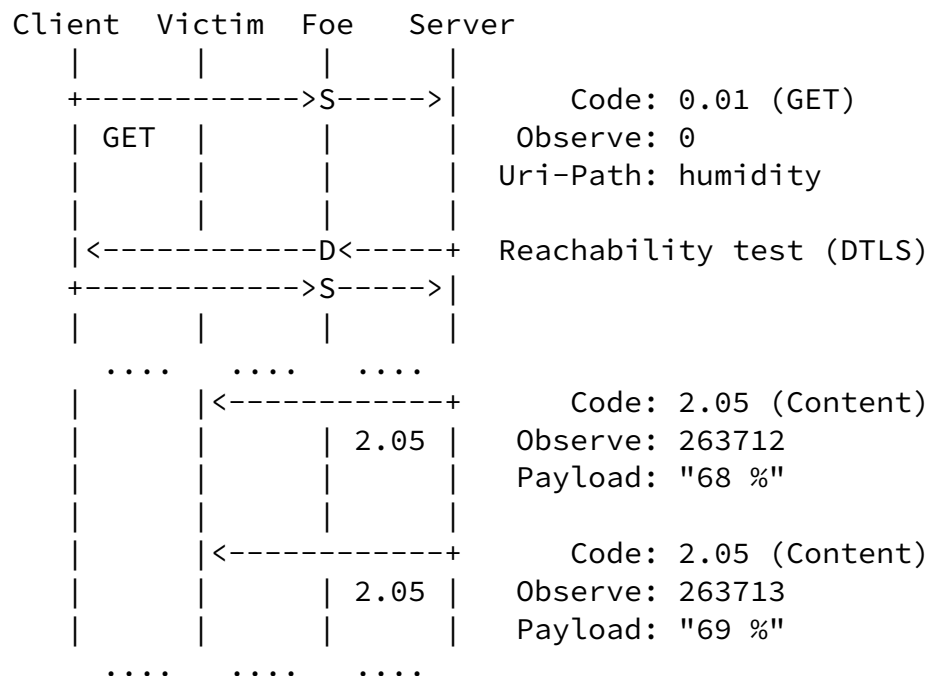


Figure 6: MITM Amplification attack by updating the client's source address in a observe registration request

Where 'S' means the MITM attacker is changing the source address of the message and 'D' means the MITM attacker is changing the destination address of the message.

An MITM amplification attack updating the server's source address is illustrated in Figure 7. This attack is possible in DTLS with Connection ID. In DTLS 1.2 the reachability test might be done at a later point.

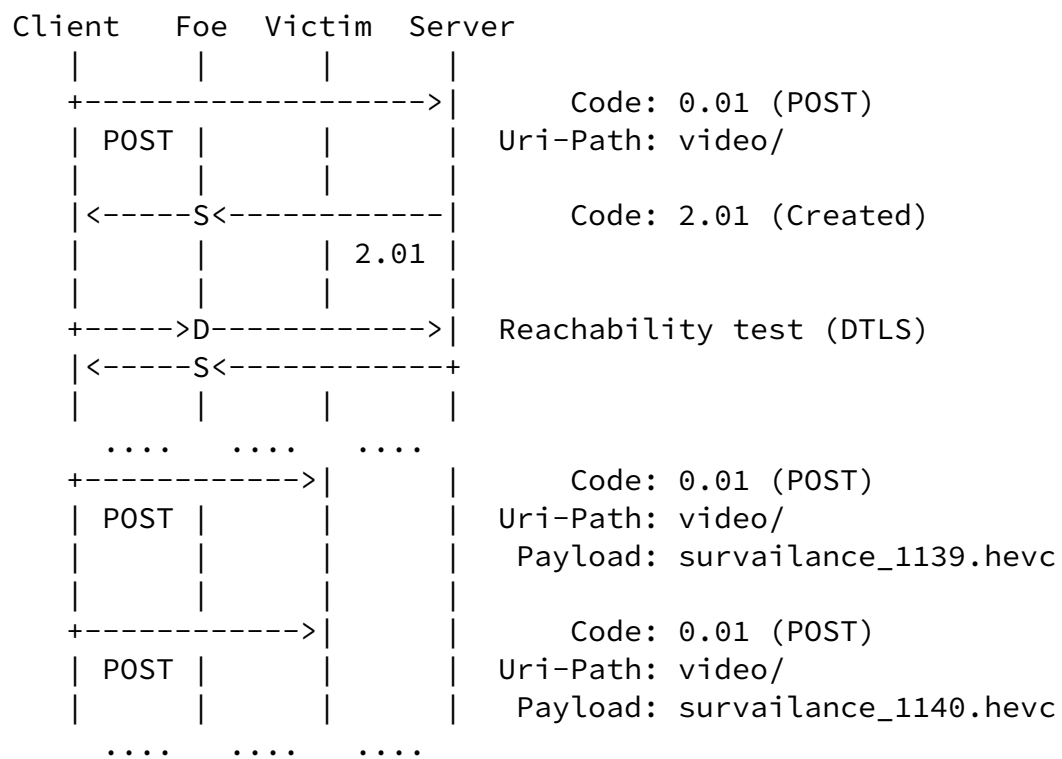


Figure 7: MITM Amplification attack by updating the server's source address in a response

### 3. Summary

CoAP has always considered amplification attacks, but most of the requirements in [\[RFC7252\]](#), [\[RFC7641\]](#), [\[I-D.ietf-core-echo-request-tag\]](#), and [\[I-D.ietf-core-groupcomm-bis\]](#) are "SHOULD" instead of "MUST", it is undefined what a "large

amplification factor" is, [\[RFC7641\]](#) does not specify how many notifications that can be sent before a potentially spoofable acknowledgement must be sent, and in several cases the "SHOULD" level is further softened by "If possible" and "generally". [\[I-D.ietf-core-conditional-attributes\]](#) does not have any amplification attack considerations.

QUIC [\[RFC9000\]](#) mandates that "an endpoint MUST limit the amount of data it sends to the unvalidated address to three times the amount of data received from that address" without any exceptions. This approach should be seen as current best practice.

While it is clear when a QUIC implementation violates the requirement in [\[RFC9000\]](#), it is not clear when a CoAP implementation violates the requirement in [\[RFC7252\]](#), [\[RFC7641\]](#), [\[I-D.ietf-core-echo-request-tag\]](#), and [\[I-D.ietf-core-groupcomm-bis\]](#).

In CoAP, an address can be validated with a security protocol or by using the Echo Option [\[I-D.ietf-core-echo-request-tag\]](#). Restricting the bandwidth per server is not enough as the number of servers the attacker can use is typically unknown. For multicast requests, anti-amplification limits and the Echo Option do not really work unless the number of servers sending responses is known. Even if the responses have the same size as the request, the amplification factor from  $m$  servers is  $m$ , where  $m$  is typically unknown. While DoS attacks from CoAP servers accessible over the Internet pose the largest threat, an attacker on a local network (e.g, a compromised node) might use local CoAP servers to attack targets on the Internet or on the local network.

#### [4.](#) Security Considerations

The whole document can be seen as security considerations for CoAP.

#### [5.](#) IANA Considerations

This document has no actions for IANA.

#### [6.](#) Informative References

[DDoS-2019]

"DDoS Attacks 2019: A look back at the Developments over the Year", Link11 , December 2019,  
<<https://www.link11.com/en/blog/threat-landscape/ddos-attacks-2019-a-look-back-at-the-developments-over-the-year/>>.

[DDoS-2021]

"Quarterly DDoS and Application Attack Report", Radware , October 2021,  
<<https://www.radware.com/2021q3-ddos-report/>>.

[DDoS-FBI] "Private Industry Notification", FBI Cyber Division , July 2020, <<https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+7.21.2020.pdf>>.

[DDoS-Infra]

"Critical Infrastructure Under Attack", Dark Reading , November 2021, <<https://www.darkreading.com/attacks-breaches/critical-infrastructure-under-attack-/a/d-id/1340960>>.

[DDoS-ZDNET]

"The CoAP protocol is the next big thing for DDoS attacks", ZDNet , December 2018,  
<<https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/>>.

[I-D.ietf-core-conditional-attributes]

Koster, M., Soloway, A., and B. Silverajan, "Conditional Attributes for Constrained RESTful Environments", Work in Progress, Internet-Draft, [draft-ietf-core-conditional-attributes-01](#), 13 January 2022,  
<<https://www.ietf.org/archive/id/draft-ietf-core-conditional-attributes-01.txt>>.

[I-D.ietf-core-echo-request-tag]

Amsüss, C., Mattsson, J. P., and G. Selander, "CoAP: Echo, Request-Tag, and Token Processing", Work in Progress, Internet-Draft, [draft-ietf-core-echo-request-tag-14](#), 4 October 2021, <<https://www.ietf.org/archive/id/draft-ietf->

[core-echo-request-tag-14.txt](#)>.

[I-D.ietf-core-groupcomm-bis]

Dijk, E., Wang, C., and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, [draft-ietf-core-groupcomm-bis-05](#), 25 October 2021, <<https://www.ietf.org/archive/id/draft-ietf-core-groupcomm-bis-05.txt>>.

[I-D.ietf-core-oscore-groupcomm]

Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and J. Park, "Group OSCORE - Secure Group Communication for CoAP", Work in Progress, Internet-Draft, [draft-ietf-core-oscore-groupcomm-13](#), 25 October 2021, <<https://www.ietf.org/archive/id/draft-ietf-core-oscore-groupcomm-13.txt>>.

[I-D.ietf-lake-edhoc]

Selander, G., Mattsson, J. P., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", Work in Progress, Internet-Draft, [draft-ietf-lake-edhoc-12](#), 20 October 2021, <<https://www.ietf.org/archive/id/draft-ietf-lake-edhoc-12.txt>>.

[I-D.ietf-tls-dtls-connection-id]

Rescorla, E., Tschofenig, H., Fossati, T., and A. Kraus, "Connection Identifiers for DTLS 1.2", Work in Progress, Internet-Draft, [draft-ietf-tls-dtls-connection-id-13](#), 22 June 2021, <<https://www.ietf.org/archive/id/draft-ietf-tls-dtls-connection-id-13.txt>>.

[I-D.ietf-tls-dtls13]

Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, [draft-ietf-tls-dtls13-43](#), 30 April 2021, <<https://www.ietf.org/archive/id/draft-ietf-tls-dtls13-43.txt>>.

[RFC6347]

Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.

- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", [RFC 7252](#), DOI 10.17487/RFC7252, June 2014, <<https://www.rfc-editor.org/info/rfc7252>>.
- [RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", [RFC 7641](#), DOI 10.17487/RFC7641, September 2015, <<https://www.rfc-editor.org/info/rfc7641>>.
- [RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", [RFC 8152](#), DOI 10.17487/RFC8152, July 2017, <<https://www.rfc-editor.org/info/rfc8152>>.
- [RFC8323] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, Ed., "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", [RFC 8323](#), DOI 10.17487/RFC8323, February 2018, <<https://www.rfc-editor.org/info/rfc8323>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [RFC 8446](#), DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", [RFC 8613](#), DOI 10.17487/RFC8613, July 2019, <<https://www.rfc-editor.org/info/rfc8613>>.

- [RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", [RFC 9000](#), DOI 10.17487/RFC9000, May 2021, <<https://www.rfc-editor.org/info/rfc9000>>.

## Acknowledgements

The authors would like to thank Carsten Bormann, Klaus Hartke, Jaime Jiménez, Ari Keränen, Matthias Kovatsch, Achim Kraus, Sandeep Kumar, and András Méhes for their valuable comments and feedback.

## Authors' Addresses

John Preuß Mattsson  
Ericsson AB  
SE-164 80 Stockholm  
Sweden

Email: [john.mattsson@ericsson.com](mailto:john.mattsson@ericsson.com)

Göran Selander  
Ericsson AB  
SE-164 80 Stockholm  
Sweden

Email: [goran.selander@ericsson.com](mailto:goran.selander@ericsson.com)

Christian Amsüss  
Energy Harvesting Solutions

Email: [c.amsuess@energyharvesting.at](mailto:c.amsuess@energyharvesting.at)