

UDP-Lite

Johannes Hamfler
KMI12
johannes.hamfler@hft-leipzig.de

ABSTRACT

In diesem Dokument wird das Lightweight User Datagram Protokoll (UDP-Lite) beschrieben, welches ähnlich UDP ist. Der Focus dieses Dokuments liegt in der Beschreibung der Vorteile, die UDP-Lite gegenüber UDP aufweisen kann. Des Weiteren wird das Protokoll in das ISO OSI-Referenzmodell eingeordnet und die Auswirkungen auf andere Schichten in diesem beschrieben. Dieses Dokument orientiert sich stark am RFC.

Categories and Subject Descriptors

Ausarbeitung [Protokolle]: RFC-Protokolle

General Terms

Beschreibung von UDP-Lite

Keywords

UDP-Lite

1. EINLEITUNG

UDP, welches im RFC 768 beschrieben ist, wird seit Jahren als verbindungsloses Protokoll verwendet und ist weit verbreitet. Auch heute hat dieses große Bedeutung für Sprachdienste, Videokommunikation und Echtzeitübertragung. Der Vorteil des Protokolls gegenüber TCP liegt vor allem bei der Sprachkommunikation darin, dass verlorene und fehlerhafte Datenpakete nicht erneut übertragen werden, da diese nach wenigen Millisekunden schon nicht mehr von Bedeutung sind.

In RFC 3828 findet sich die Beschreibung des UDP-Lite Protokolls. UDP-Lite versucht das Problem der fehlerhaften Pakete, welche beim Empfänger gelöscht werden, zu mindern, indem die Option besteht fehlerhafte Pakete dennoch zu verwenden und an höhere Schichten weiterleiten zu können. Bei Sprachdiensten hätte dies den Vorteil, dass der in

einer höheren Schicht angesiedelte Codec die korrekten Bits auf eine bestimmte Weise verarbeitet, so dass diese nützlich für die Anwendung sind. Fehlerhafte Bits könnten für den Codec ebenfalls einen Nutzen darstellen, so dass UDP-Lite in diesem Zusammenhang einen Vorteil darstellen würde.

2. PROTOKOLLSPEZIFIKATION

2.1 Einordnung in das OSI-Referenzmodell

UDP-Lite befindet sich auf Schicht 4, der Transportschicht des OSI-Referenzmodells. Trotz dass UDP-Lite für eine volle Funktionalität und die Verwendung der Stärken des Protokolls auf andere Schichten angewiesen ist, stellt es eine hohe Kompatibilität mit UDP bereit und befindet sich deshalb wie UDP auf Schicht 4.

2.2 Einteilung des Payloads

Da manche Codecs die Fähigkeit besitzen beschädigten Payload zu behandeln und nützliche Informationen aus diesem zu extrahieren, wurde bei UDP-Lite ein Paket in zwei Teile aufgliedert werden. Ein Teil kann mit einem Fehlerkorrekturwert überprüft werden, um die Integrität der darin enthaltenen Daten zu sichern, ein anderer Teil kann ohne Prüfsumme vorhanden sein.

In dem Teil, in welchem eine Fehlerüberprüfung stattfinden soll, werden üblicherweise Steuerinformationen übertragen, welche unbedingt fehlerfrei vorhanden sein müssen, um die Parameter des Payloads beim Empfänger richtig interpretieren zu können. Sollte der Payload in diesem Teil beschädigt sein, wird das Paket beim Empfänger in der Transportschicht verworfen.

Der andere Teil des Payloads, welcher beim klassischen UDP üblicherweise Daten enthält, welche nicht zwingend neu übertragen werden müssen, kann ohne Fehlerkorrektur übertragen werden, damit die darüber liegenden Schichten auch beschädigte Daten bearbeiten können, um aus diesen ebenfalls nützliche Informationen für eine Anwendung zu extrahieren. Da in diesem Teil nicht überprüft wird ob Fehler vorhanden sind, wird der Payload nicht für die Entscheidung der Weiterleitung an höhere Schichten verwendet.

Wird eine Prüfsumme über das gesamte Paket angewandt, so ist UDP-Lite zwar semantisch identisch zu UDP, wird jedoch unterschiedlich beim Empfänger behandelt.

2.3 Beobachtungen aus dem RFC

Im RFC wurden einige Beobachtungen zu der Datenübertragung erläutert, welche hier kurz erwähnt werden.

Es wurden folgende Codecs als Beispiele genannt, welche mit UDP-Lite eine Verbesserung der decodierten Daten erreichen können:

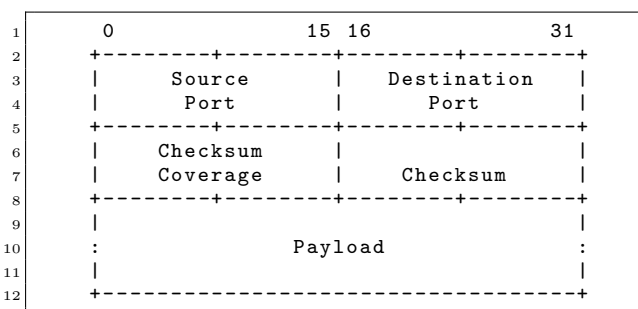
- AMR speech codec [RFC-3267]
- Internet Low Bit Rate Codec [ILBRC]
- error resilient H.263+ [ITU-H.263]
- H.264 [ITU-H.264; H.264]
- MPEG-4 [ISO-14496] video codecs)

Des Weiteren ist es nützlich, wenn niedrigere Schichten beschädigte IP Pakete weiterleiten, wenn dies verlangt wird. Sollten Verbindungen sich ihrer Fehleranfälligkeit bewusst sein, so ist es möglich, dass eine physische Verbindung eine höhere Sicherheit für sensible Daten gewährleistet, was durch verschiedene Fehlerkorrekturverfahren erreicht werden kann.

Außerdem sollte die Transport- und Vermittlungsschicht höher gelegene Applikationen nicht an ihrer Ausführung hindern, weil Pakete beschädigt sind. UDP eignet sich deshalb nur bedingt, da bei diesem die Prüfsumme gesetzt sein muss. Bei IP ist dies nicht der Fall.

2.4 Der UDP-Lite Header

Nachfolgend ist der UDP-Header abgebildet.



[1] Dieser unterscheidet sich von dem UDP-Header nur in der Hinsicht, dass das Length-Feld mit einem Cecksum-Coverage-Feld ausgestattet wurde. Dieses ist dazu da, um die Länge anzugeben, bis wohin die Prüfsumme berechnet wird. Dies war möglich, da die Information über die Länge des Pakets aus IP-Paketen entnommen werden kann.

2.5 Beschreibung der Felder der PDU

Das Source- und Destination-Port-Feld sind dem von UDP gleich, wobei das Checksum-Coverage-Feld die Länge in Bit-Oketetten angibt, die von der Prüfsumme einbezogen werden. Hierbei wird ab dem ersten Oktett mit dem Zählen angefangen.

Der Header muss dabei immer mit einer Prüfsumme gesichert werden. Eine Prüfsumme von 0 bedeutet dabei, dass das

gesamte Paket in die Prüfsumme einbezogen wird. Die Prüfsumme des UDP-Headers muss 0 oder mindestens 8 sein, was bedeutet, dass die 8 Bytes des Headers beinhaltet sein müssen. Ein Paket mit einer Prüfsummenlänge zwischen 1 und 7 muss beim Empfänger verworfen werden, da dieses die Bedingung der Sicherung des Headers nicht erfüllt. Das berechnete Prüfsummenfeld muss den Pseudo-Header von IP enthalten. Zusätzlich müssen UDP-Lite Pakete, die eine größere Prüfsummenlänge als der IP-Header annehmen, ebenfalls verworfen werden. Wäre dies nicht der Fall, könnte die Länge des UDP-Lite-Pakets nicht festgestellt werden.

Da das Prüfsummenfeld ein 16-Bit-Komplement der Summe des Einerkomplements des Pseudo-Headers darstellt, muss das UDP-Lite-Paket im Payload ein vielfaches von 2Byte aufweisen. Notfalls wird dieses mit Nullen aufgefüllt. Die Informationen, aus welchen die Prüfsumme berechnet wird, werden dem IP-Header entnommen. Bevor die Prüfsumme berechnet wird, muss das Prüfsummenfeld jedoch auf 0 gesetzt werden. Sollte nach der Berechnung die Prüfsumme 0 ergeben, so werden 16 Einsen übertragen.

Da manche Anwendungen die UDP-Lite benutzen möglicherweise keine Fehlerbehandlung wünschen, kann hier die Prüfsummenlänge einfach auf 8 gesetzt werden, um den Payload nicht mit einbeziehen zu müssen. Dadurch wird sichergestellt, dass die Steuerinformationen in jedem Fall korrekt ankommen.

2.6 Der Pseudo-Header

Der Pseudo-Header von UDP-Lite unterscheidet sich von dem in UDP insofern, dass der Wert des Längenfeldes nicht vom UDP-Lite-Header genommen wird, sondern von Informationen aus den IP-Paketen. Dabei wird die Berechnung gleich wie bei TCP ausgeführt, was bedeutet, dass nicht nur der Payload, sondern auch der Header von UDP-Lite mit einbezogen wird. Dadurch, dass die Länge auf diese Weise berechnet, muss das Prüfsummenfeld bei 8 beginnen und ermöglicht so einen einfachen softwareseitigen Vergleich.

2.7 Die Anwendungsschnittstelle

Die Anwendungsschnittstelle stellt die gleichen Funktionen wie bei UDP zur Verfügung. Des Weiteren sollte eine Möglichkeit der sendenden Anwendung bestehen, den Prüfsummenlängenwert an UDP-Lite zu übertragen. Zumindest sollte jedoch die Möglichkeit für eine empfangende Anwendung bestehen, die Weiterleitung von Paketen mit Prüfsummenlängen kleiner als eine Festgelegte zu blockieren.

Im RFC wird empfohlen, dass UDP-Lite standardmäßig das Verhalten von UDP imitieren sollte, indem das Prüfsummenlängenfeld der Länge des UDP-Lite-Pakets entsprechen soll, um das gesamte Paket verifizieren zu können. Über einen expliziten Aufruf, einem sogenannten System Call, beim Sender, sollen Anwendungen die fehlertolerant sind UDP-Lite ihre Fehlertoleranz mitteilen. Eine empfangende Anwendung die ebenfalls eine teilweise angewandte Prüfsumme nutzen will, sollte dies ebenfalls über einen solchen Aufruf kund geben.

Da im Internet Pfade variieren und verschiedene Eigen-

schaften aufweisen, können keine pauschalen Aussagen über die Fehlerschemas einer Verbindung gemacht werden. Deshalb sollten Anwendungen die UDP-Lite nutzen keine Annahmen der Fehler in einem UDP-Lite-Paket machen, solange der Bereich nicht in die Berechnung der Prüfsumme mit einbezogen wurde. Anwendungen sollten deshalb wenn nötig ihre eigenen Fehlerprüfmechanismen nutzen.

2.8 Die IP-Schnittstelle

Wie bei UDP muss auch UDP-Lite den Pseudo-Header der IP-Implementierung erhalten, welcher die IP-Adresse und Protokollfelder des IP-Headers beinhaltet, sowie die Länge des IP-Payloads, welche aus dem Längenfeld der IP-Pakete entnommen werden kann. Der Sender darf dabei jedoch nicht den IP-Payload mit Padding-Bytes auffüllen, da die Länge des UDP-Lite-Pakets daraus entnommen werden soll.

2.9 IP-Jumbo-PDUs

Da das Prüfsummenlängenfeld Werte bis 65535 annehmen kann, können genaue Prüfsummenlängen benutzt werden. Dies ist bei Jumbo-PDUs (Jumbogrammen) nicht der Fall. Es kann entweder das gesamte Paket mit der Prüfsummenlänge von 0 oder alle Oktette bis zum 65535ten Oktett einschließen.

2.10 Betrachtung der niedrigeren Schichten

Frames, die UDP-Lite-Pakete enthalten dürfen von niedrigeren Schichten nicht verworfen werden, da die Fehlerbehandlung in einer höheren Schicht erfolgt. Eine Ausnahme wäre der Fall, wenn ein Fehler im sensiblen Datenbereich existiert. Das Prüfsummenlängenfeld könnte für Verbindungen, welche partielle Fehlererkennung ermöglichen, dafür benutzt werden, niedrigeren Schichten mitzuteilen, in welchen Bereichen Fehler auftreten dürfen. Da der sensible Teil des UDP-Lite-Pakets zwischen dem ersten Oktet des IP-Headers und dem letzten Oktett liegt, welcher vom Prüfsummenlängenfeld bekannt gegeben wird, kann der sensible Teil in der gleichen Weise behandelt werden, wie ein UDP-Paket.

Da Verbindungen, welche keine partielle Fehlererkennung ermöglichen, in einem Fehlerfall das Paket verwerfen müssen, wird das UDP-Lite-Paket in gleicher Weise wie ein UDP-Paket behandelt.

Somit lässt sich bei UDP-Lite sagen, dass dieses Protokoll nur eine Verbesserung erwirken kann, wenn in Schicht 2 des OSI-Referenzmodells die Partielle Prüfsumme und die Prüfsummenlänge von UDP-Lite genutzt wird. Dies würde seine Wirkung jedoch erst in Fehleranfälligen Umgebungen entfalten.

2.11 Kompatibilität mit UDP

Da UDP und UDP-Lite eine ähnliche Syntax und Semantik hat, können Anwendungen UDP-Lite anstatt UDP mit der Eigenschaft nutzen, das ganze Paket mit einer Fehlerkorrektur zu sichern. Des Weiteren sind durch die Ähnlichkeit nur geringe Änderungen an Anwendungen vorzunehmen, um UDP-Lite verwenden zu können.

UDP-Lite hat eine eigene IP-Protokoll-Identifikation (136), welche es einem Empfänger erlaubt zu erkennen, ob UDP-Lite oder UDP genutzt wird. Ein Empfänger, welcher das UDP-Lite-Protokoll nicht kennt, wird ein ICMP-Paket mit einer Fehlernachricht zurück senden. Damit kann festgestellt werden, ob anderen Systemen UDP-Lite bekannt ist. Diese Nachrichten können folgende sein:

- ICMP "Protocol Unreachable"
- ICMPv6 "Payload Type Unknown"

Ein Problem würde bei der Verwendung einer gleichen UDP-Identifikation entstehen, da ein UDP-Lite-Payload mit einer partiellen Prüfsumme von UDP-Anwendungen verworfen wird und UDP-Pakete, welche nur teilweise den IP-Payload füllen, nicht an UDP-Lite-Anwendungen weitergeleitet werden können. Das Problem dabei wäre die fehlende Benachrichtigung an den Sender, welches durch folgende Maßnahmen laut dem RFC eingedämmt werden könnte:

- Explizite Nutzung der Signalisierung innerhalb des Payloads ohne die partielle Prüfsumme zu verwenden, um dem Sender das Erkennen der UDP-Lite-Unterstützung zu ermöglichen
- Nutzung eines anderen Protokolls zur Signalisierung, wie zum Beispiel SIP, damit erkannt werden kann, ob der Empfänger UDP-Lite nutzen kann

Da jedoch UDP-Lite eine eigene Identifikation besitzt, müssen diese Varianten nicht verwendet werden.

2.12 Sicherheitsbetrachtungen

Der Sicherheitsaspekt von UDP-Lite hängt von der Interaktion mit Authentifizierungs- und Verschlüsselungsverfahren ab. Da der sensible Teil des Payloads beim Übertragen über verschiedene Netzsegmente variieren kann, würde im Fall einer Beschädigung des Pakets die Authentifizierung oder Verschlüsselung korumpiert werden. Dies gilt besonders wenn IPv6 verwendet wird, da hier eine Fehlerkorrektur im IP-Paket vorhanden sein muss. Sollte ebenfalls IPSec mit ESP genutzt werden, kann eine Verbindung nicht feststellen welches Transportprotokoll verwendet wird. UDP-Lite kann in diesem Fall keinen Vorteil für darüber liegende Codecs oder Anwendungen erwirken.

Stattdessen kann eine Verschlüsselung in der Transportschicht oder auf Anwendungsebene angewandt werden, jedoch haben Verschlüsselungsverfahren, (besonders Block-basierte) die Eigenschaft, dass ein fehlerhaftes Bit den gesamten Block unbrauchbar macht. Deshalb sollten spezielle Stromchiffren verwendet werden, die dieses Verhalten minimieren. Der Nachteil dieser ist jedoch, dass ein Angreifer möglicherweise vorhersagbare Manipulationen am Payload vornehmen kann, ohne den verschlüsselten Payload vollständig entschlüsseln zu müssen.

2.13 IANA Protokollnummer

Die IANA vergab UDP-Lite die Protokollnummer 136, änderte jedoch den Namen auf UDPLite, da somit eine größere Bandbreite an Plattformen mit diesem bedient werden kann, besonders diejenigen, die ein Minus-Zeichen nicht unterstützen.

3. SCHLUSSFOLGERUNG

Abschließend ist zu sagen, dass UDP-Lite zwar Vorteile gegenüber UDP bietet, diese jedoch nur bei fehleranfälligen Verbindungen Ihre Wirkung zeigen. UDP-Lite hat zudem einen etwas höheren Einrichtungsaufwand, dennoch im Fehlerfall einen ungleich großen Nutzen. Deshalb sollte UDP-Lite für vorhersagbar schlechte Verbindungen verwendet werden, muss jedoch bei bestehenden Systemen nicht notwendigerweise zum Einsatz kommen. Bei kryptografischen Anwendungen hat UDP-Lite wenig Vorteile, weshalb UDP für diese gleich oder besser geeignet scheint.

4. REFERENCES

- [1] N. W. Group. The lightweight user datagram protocol (udp-lite). *RFC 3828*, Standards Track(3828):12, Juli 2004.