



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.

H04L 29/06 (2006.01)
H04L 12/56 (2006.01)
G06F 15/16 (2006.01)

(45) 공고일자 2007년03월20일
(11) 등록번호 10-0697355
(24) 등록일자 2007년03월13일

(21) 출원번호 10-2005-7002822

(65) 공개번호 10-2005-0058371

(22) 출원일자 2005년02월18일

(43) 공개일자 2005년06월16일

심사청구일자 2005년02월18일

번역문 제출일자 2005년02월18일

(86) 국제출원번호 PCT/IB2003/002589

(87) 국제공개번호 WO 2004/019586

국제출원일자 2003년07월02일

국제공개일자 2004년03월04일

(30) 우선권주장 10/223,318 2002년08월20일 미국(US)

(73) 특허권자 노키아 코포레이션
핀란드 핀-02150 에스푸 케이라라덴티에 4

(72) 발명자 장 안지
중국 100029 베이징 차오 양 디스트릭트 넘버 20 샤오야오 주 로드 지
리 가든 하우스 2 15 플로어 플랫07

하주 케이조
핀란드 핀-33580 탐페르 툴루스카투 1 비 20

(74) 대리인 박장원

심사관 : 이동환

전체 청구항 수 : 총 13 항

(54) 확장 헤더 압축

(57) 요약

본 발명은 패킷 데이터 네트워크의 링크에 대한 헤더 압축과 복원을 제어하기 위한 방법 및 장치에 관한 것으로, 여기서, 상기 링크에 대한 소정 헤더 확장 사이즈는 초기적으로 설정되고, 만약 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신된다면, 차후 복원에 대하여 참조로서 사용되지 않은 패킷은 압축기(201)에서 복원기(301)로 전송된다. 복원하는 측면(301)에서, 만약 복원기에 형성된 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신된다면 확인의 전송이 억제된다. 그에 따라, 압축기(201)와 복원기(301) 사이에서 압축 문맥의 비밀관성이 방지되고, 상기 문맥을 복구할 필요가 없기 때문에 더 높은 압축 효율이 이루어지고, 정확하게 복원된 패킷들이 임의의 패킷들의 버려짐 없이 상위 네트워크 레이어들로 전달될 수 있다.

대표도

도 5

특허청구의 범위

청구항 1.

패킷 데이터 네트워크의 링크에 대하여 헤더 압축을 제어하는 방법으로서,

- a) 상기 링크에 대하여 소정 헤더 확장 사이즈를 설정하는 단계와; 그리고
- b) 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신되는 경우, 차후의 복원을 위한 참조로서 사용되지 않을 비참조 패킷을 압축기(201)로부터 복원기(301)로 전송하는 단계를 포함하는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 2.

제 1항에 있어서, 상기 헤더 압축은 ROHC 방식을 토대로 하는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 3.

제 2항에 있어서, 상기 비참조 패킷은 동작 모드가 U 모드 또는 O 모드인 경우 발생 식별자가 없는 패킷이며, 여기서, 상기 발생 식별자는 헤더 확장 리스트들의 동일한 발생을 나타내는데 이용되는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 4.

제 2항 또는 제 3항에 있어서, 상기 비참조 패킷은 동작 모드가 R 모드인 경우 복원 문맥을 업데이트 하지 않는 ROHC-신뢰 모드 패킷인 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 5.

제 4항에 있어서, 상기 신뢰 모드 패킷은 R1 패킷인 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 6.

패킷 데이터 네트워크의 링크에 대하여 헤더 복원을 제어하는 방법으로서,

- a) 상기 링크에 대하여 소정 헤더 확장을 설정하는 단계와; 그리고
- b) 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신되는 경우 확인의 전송을 억제하는 단계를 포함하는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 7.

제 6항에 있어서, 상기 헤더 복원은 ROHC 방식을 토대로 하고, 상기 큰 확장 헤더 리스트의 수신에 응답하여 신뢰 모드로의 변환이 수행되는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 8.

제 6항 또는 제 7항에 있어서, 상기 억제는 상기 소정 헤더 확장 사이즈와 동일하거나 더 작은 사이즈의 확장 헤더 리스트가 수신될 때까지 유지되는 것을 특징으로 하는 헤더 압축 제어 방법.

청구항 9.

패킷 데이터 네트워크의 링크에서 헤더 압축을 제어하기 위한 압축 장치로서,

- a) 상기 링크에 대하여 소정 헤더 압축 사이즈를 설정하기 위한 제어 수단들(202)과; 그리고
- b) 상기 소정 헤더 확장 사이즈보다 큰 사이즈의 확장 헤더 리스트가 수신되는 경우, 차후의 복원을 위해 참조로서 사용될 비참조 패킷을 발생시키기 위한 헤더 압축 수단들(201)을 포함하는 것을 특징으로 하는 압축 장치.

청구항 10.

제 9항에 있어서, 상기 헤더 압축 수단들(201)은 ROHC 방식을 토대로 하고, 상기 헤더 압축 수단들(201)은 발생 식별자 또는 상기 비참조 패킷으로서 신뢰가능한 모드 패킷 없이 U 모드 또는 O 모드 패킷을 발생시키도록 구성된 것을 특징으로 하는 압축 장치.

청구항 11.

패킷 데이터 네트워크의 링크에 대하여 헤더 복원을 제어하기 위한 복원 장치로서,

- a) 상기 링크에 대하여 소정 헤더 확장 사이즈를 설정하기 위한 제어 수단들(302)과; 그리고
- b) 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신되는 경우 확인의 전송을 억제하기 위한 헤더 복원 수단들(301)을 포함하는 것을 특징으로 하는 복원 장치.

청구항 12.

제 11항에 있어서, 상기 헤더 복원 수단들(301)은 ROHC 방식을 토대로 상기 헤더 복원을 수행하기 위하여, 그리고 상기 큰 확장 헤더 리스트의 수신에 응답하는 신뢰 모드로의 변환을 수행하도록 구성된 것을 특징으로 하는 복원 장치.

청구항 13.

제 9항 또는 제 10항에 따르는 압축 장치와 제 11항 또는 제 12항에 따르는 복원 장치를 포함하는 헤더 압축을 제어하기 위한 시스템.

명세서

기술분야

본 발명은 예컨대, IP(Internet Protocol) 기반 네트워크와 같은 패킷 데이터 네트워크에서의 헤더 압축 및 복원 제어에 대한 방법, 장치들 및 시스템에 관한 것이다.

배경기술

패킷 데이터 전송을 사용하는 커뮤니케이션 네트워크에서, 각각의 데이터 패킷들은 발신 애플리케이션에서 수신 애플리케이션으로 상기 데이터 패킷을 전송하기 위하여 필요한 정보를 헤더 섹션에 전달한다. 전송되어야 하는 실제 데이터는 페이로드(payload) 섹션에 포함된다.

발신 애플리케이션에서 수신 애플리케이션으로 데이터 패킷의 전송 경로는 일반적으로 커뮤니케이션 링크들을 통해 내부 연결되는 네트워크 노드들에 의해 표현되는 다중 중재 단계들을 포함한다. 패킷 스위치들 또는 라우터들로 불리는 이러한 네트워크 노드들은, 데이터 패킷을 수신하고, 데이터 패킷의 페이로드를 수신 애플리케이션에 전달할 수신 네트워크 노드에 도달될 때까지 데이터 패킷을 다음 중재 라우터로 전송한다. 상기 데이터 패킷의 전송에 대한 서로 다른 프로토콜 레이어들의 기여도 때문에, 데이터 패킷의 헤더 섹션 길이는 페이로드 섹션의 길이를 초과할 수 있다.

따라서, 수신 애플리케이션으로 페이로드를 전달하는 것에 대한 링크 레이어의 더 나은 사용효율을 획득하기 위하여, 상기 헤더 섹션의 데이터 압축이 사용될 수도 있다. 헤더 압축은 헤더 필드들을 제거하거나 헤더 필드들의 사이즈를 감소시킴으로써 헤더의 사이즈를 감소시킨다. 이는, 만약 헤더의 문맥(context) 상태가 헤더를 압축할 때 사용된 문맥 상태와 동일하다면 복원기가 상기 헤더를 복원하는 것과 같은 방법으로 수행된다. 헤더 압축기는 네트워크 레이어 레벨(예컨대, IP 헤더들에 대하여), 전송 레이어 레벨(예컨대, 사용자 다이어그램 프로토콜(UDP) 헤더 또는 전송 제어 프로토콜(TCP) 헤더들에 대하여) 및 애플리케이션 레이어 레벨(예컨대, 하이퍼 텍스트 전송 프로토콜(http) 헤더들에 대하여)에서 수행될 수 있다.

상기 IETF(Internet Engineering Task Force) 설명 RFC 3095에서, 로버스트 헤더 압축(ROHC) 방식은 RTP/UDP/IP (Real Time Transport Protocol, User Datagram Protocol, Internet Protocol), UDP/IP 및 ESP/IP(Encapsulating Security Payload) 헤더들에 대하여 매우 강건하고 효율적인 헤더 압축 방식으로 설명된다. 기존의 헤더 압축 방식들은, 심각한 오류율과 긴 왕복 시간을 가지는 링크들에 사용될 때는 잘 동작하지 않는다. 다수의 밴드폭이 헤더 압축이 필수적인 링크들에 제한되기 때문에, 그러한 특성들이 공통된다. 지난해 동안, 특히 두 커뮤니케이션 기술들 즉, 셀룰라 텔레포니 및 인터넷이 일반 대중에게 의해 공통적으로 사용되었다. 셀룰라 텔레포니는 그 사용자들에게 그들이 어디에 있는지 상관없이 항상 합리적인 서비스 품질로 도달할 수 있는 혁신적인 확률을 제공해왔다. 반면, 상기 인터넷은 애초부터 다중 서비스용으로 설계되어 왔으며, 이것의 강점 중 하나는 모든 종류의 사용에 적용될 수 있는 유연성(flexibility)이다. IP 텔레포니는 향상된 기술적인 솔루션들 때문에 추진력을 얻고 있다. 셀룰라 폰들은 좀더 일반화되고 있고, 오디오 및 비디오뿐만 아니라 웹-브라우징, 이메일, 게임 등을 지원하는 IP 스택들을 가진다. 따라서, 서로 간에 커뮤니케이션 하는 두 이동 단말기들은 셀룰라 링크들을 통해 기지국과 연결될 수 있고, 상기 기지국들은 IP 기반 유선 네트워크에 연결될 수 있다. 만약 기술적 및 경제적으로 가능한 경우, 단말기들간에 항상 순수 IP를 갖는 솔루션은 특별한 이점을 가질 수 있다. 그러나, 이를 실행 가능 있는 대안으로 만들기 위해서는, 다수의 문제점들, 특히 밴드폭 효율에 관한 문제점들에 대한 대처방안이 강구되어야 한다.

셀룰라 폰 시스템들에 있어서, 부족한 무선 리소스들을 효율적인 방법으로 사용하는 것이 매우 중요하다. 각 셀당 충분한 수의 사용자들을 확보하는 것이 중요하며, 그렇지 않으면 그 전개 비용(development cost)은 엄청나게 비싸게 될 것이다. 음성 서비스의 품질 역시 오늘날의 셀룰라 시스템들에서와 같이 양호해야 한다. 새로운 서비스들에 대한 지원, 음성 서비스의 저 품질은 비용들이 상당히 감소되는 경우에 한하여 수용되기 쉽다.

인터랙티브 음성 대화에 사용될 때 셀룰라 링크들을 통한 IP의 문제점은 큰 헤더 오버헤드이다. 따라서, 효율성 이유로 헤더 사이즈를 감소시키는 것에 대한 필요성은 명백하다. 그러나, 셀룰라 링크들은 헤더 압축이 잘 수행되지 않게 만드는 특성을 가진다. 셀룰라 링크들에 대한 실행 가능한 헤더 압축 방식은 압축 포인트 이전의 손실뿐만 아니라 압축 포인트와 손실 포인트 사이의 링크들에서의 손실을 처리할 수 있어야 한다.

상기 압축기의 문맥은 압축기가 헤더를 압축하기 위해 사용하는 상태이다. 상기 복원기의 문맥은 복원기가 헤더를 복원하기 위해 사용하는 상태이다. 이러한 것들 중 하나 또는 결합된 두개는 의도된 것이 명백할 때 일반적으로 "문맥"이라고 언급된다. 상기 문맥은 정적 필드와 같은 그러한 패킷 스트림에서의 이전 헤더로부터의 관련 정보와, 압축기 및 복원기를 위

한 가능한 기준값들을 포함한다. 더욱이, 패킷 스트림을 설명하는 부가적인 정보는 또한 문맥의 일부분이며, 예를 들어 IP 식별자 필드가 어떻게 변화하고, 전형적인 내부-패킷이 시퀀스 넘버들 또는 타임 스탬프들에서 어떻게 증가하는지에 관한 정보가 있다.

일반적으로, 패킷은 예컨대, 프로토콜 데이터 유닛과 같은 전송 및 수신 유닛에 대응한다. 상기 패킷은 압축되고, 그 다음 예컨대, ROHC에 의해 복원된다. 상기 패킷 스트림은, 필드 수치들 및 필드 수치들의 변화 패턴들이 동일 문맥을 사용하여 압축될 수 있는 헤더들과 같은 패킷들의 시퀀스에 대응한다. 복원기의 문맥이 압축기의 문맥과 일치하지 않을 때, 복원은 원래의 헤더를 재생할 수 있게 한다. 이 상황은 복원기의 문맥이 적절히 초기화되지 않을 때, 또는 패킷들이 압축기와 복원기 사이에서 손실되거나 손상될 때 발생할 수 있다. 문맥 복구 매카니즘들은 문맥들이 존재하지 않을 때 동기화하여 상기 문맥들을 불러오는 매카니즘들이다. 이는 문맥 손상으로 인한 과도한 손실을 방지하기 위하여 필요하다.

헤더 압축이 행해져야만 하는 주요 이유는 양자 모두 동일 패킷 헤더 내에 있는, 그러나 특히 동일 패킷 스트림에 속하는 연속적인 패킷들 사이에 있는 헤더 필드들 간에 상당한 리던던시(redundancy)이 존재한다는 사실이다. 정적 필드 정보들 단지 초기적으로 전송하거나 다른 필드들에 대한 의존성들 및 예측확률들을 이용함으로써, 헤더 사이즈가 대부분의 패킷들에 대하여 상당히 감소될 수 있다. 과거 패킷들로부터의 연관된 정보는 상기 문맥에서 유지된다. 상기 문맥 정보는 차후의 패킷들을 압축하거나 복원하기 위하여 사용된다. 상기 압축기 및 복원기는 특정 사건들로 그들의 문맥들을 업데이트 한다. 문맥들은 압축된 헤더들 및 피드백 정보와 함께 전송되는 문맥 식별자(CID)에 의해 식별된다. 상기 피드백 정보는 상기 복원기에서 압축기로 정보를 전달한다. 확인 정보(ACK)는 패킷의 성공적인 복원을 확인하는데 사용되며, 상기 문맥이 높은 확률로 업데이트 된 것을 의미한다. 더 나아가, 비확인 정보(NACK)는 상기 복원기의 동적 문맥이 동기화되지 않음을 나타내는데 사용된다. 이 피드백 정보는 몇몇 성공적인 패킷들이 정확하게 복원되지 못했을 때에 발생된다.

상기 ROHC 헤더 압축 방식은 단방향성 모드(U-mode), 양방향성 낙관 모드(O-mode) 및 양방향성 신뢰 모드(R-mode)로 불리는 3가지 동작 모드를 가진다. 동작하기 위한 최상의 모드는, 피드백 확률, 오류 확률 및 분포, 헤더 사이즈 변화의 효과 등과 같은 압축 프로토콜 환경 특성에 의존한다.

상기 U-모드에 있을 때, 패킷들이 압축기에서 복원기로의 단지 한 방향으로만 전송된다. 따라서 이 모드는 복원기에서 압축기로의 귀환 경로가 이용불가능하거나 바람직하지 않은 링크들에서 사용가능하다. 상기 U-모드에서, 압축기 상태들 간의 변환은 주기적인 타임아웃 및 압축된 패킷 스트림에서 패턴들을 변화시키는 헤더 필드에서의 불규칙성을 고려하여 수행된다. 주기적인 재생들 및 오류 회복의 초기화에 대한 피드백 부족으로 인하여, U-모드에서의 압축은 효율성이 떨어질 수 있고, 임의의 양방향성 모드들과 비교하여 약간 더 높은 손실 전달 확률을 가진다. 임의의 양방향성 모드로의 변환은 패킷이 복원기에 도달하자마자 수행될 수 있고, 모드 변환이 바람직하다는 것을 나타내는 피드백 패킷으로 응답한다.

상기 O-모드는 상기 U-모드와 유사하다. 차이점은 피드백 채널이 오류 회복 요청들을 전송하기 위해 사용되고, 복원기에서 압축기로 중요한 문맥의 확인이 선택적으로 업데이트 된다는 것이다. 주기성 재생들은 O-모드에서 사용되지 않는다. 상기 O-모드는 압축 효율성과 피드백 채널의 회소 사용을 극대화 하는 것이 목적이다. 이는 잔류 오류 또는 문맥 실효로 인하여 상위 레이어로 전달되는 손상된 헤더들의 개수를 감소시킨다.

마지막으로, 상기 R-모드는 이전 두 모드들과 많은 점에서 상이하다. 가장 중요한 차이점들은 피드백 채널의 더 집중적인 사용과, 매우 높은 잔류 비트 오류율을 제외하고 압축기와 복원기 사이에서 문맥 동기화의 손실을 방지하는 압축기 및 복원기에 더 엄격한 로직이다. 피드백은 모든 문맥 업데이트들을 확인시키기 위하여 전송된다. 상기 R-모드는 손실 전달 및 손상 전달에 대하여 견고성을 극대화하는 것, 즉 헤더 손실/손상 버스트 조건하에서 문맥 실효의 확률을 최소화 하는 것을 목표로 한다.

ROHC는 패킷들이 압축기와 복원기 사이에서 손상될 수 있다는 가정하에 지정되고, 그러한 손상된 패킷들은 상기 복원기에 전달될 수 있다. ROHC는 원 헤더들과 대비하여 주기적 덧붙임 검사(CRC)를 사용하여 손상된 헤더들을 탐지한다. R-모드에서 가장 작은 헤더들이 CRC를 포함하지 않는 반면, 상기 U-모드 및 O-모드에 있어서 가장 작은 헤더들은 3-비트 CRC를 포함한다. 따라서, 가장 작은 헤더들에 대한 손상은 R-모드에서 탐지되지 않는다. U-모드에서 동작할 때, 모든 압축된 헤더들은 복원을 증명하기 위해 사용되어야 하는 CRC를 전달한다.

상기 R-모드에서, 후술할 피드백 로직은 상기 복원기에 의해 사용된다. 패킷, 즉 7-8 비트 CRC를 전달하는 패킷을 업데이트 하는 것이 정확하게 복원될 때, 바람직한 압축 모드로서 R-모드를 나타내는 모드 파라미터를 가지는 확인(ACK(R))이 상기 압축기에 전송된다. 반면, 피드백이 문맥을 업데이트 하지 않는 패킷, 즉 CRC를 전달하지 않는 패킷들에 대하여 전송되지 않는다.

어느 하나의 압축 모드에서 다른 압축 모드로 이동하기 위한 결정은 상기 복원기에 의해 내려진다. 각 문맥에 대하여, 상기 압축기 및 복원기는 그 수치가 각각 그 문맥에 대한 현재 압축기 모드 및 복원기 모드인 변수를 포함한다. 이 변수 수치는 질문의 문맥에 대하여 어떤 패킷 타입들을 사용해야 하는지, 어떤 행동들이 취해져야 하는지 등을 제어한다. 압축기 측면에서, 파라미터 C_MODE 및 C_TRANS가 제공된다. C_MODE에 대하여 가능한 수치들은 단방향(Unidirectional)에 대한 "U", 낙관(Optimistic)에 대한 "O", 신뢰(Reliable)에 대한 "R"이다. 파라미터 C_TRANS는 "U"로 초기화되어야 한다. 더 나아가, 파라미터 C_TRANS에 대하여 가능한 수치들은 진행중(Pending)에 대한 "P"와 진행완료(Done)에 대한 "D"이다. 파라미터 C_TRANS는 "D"로 초기화되어야 한다. 파라미터 C_TRANS가 "P"로 설정될 때, 압축기는 모든 모드들에 공통되는 패킷 포맷들만 사용할 것을 요구하고, 모드 정보는 적어도 주기적으로 전송되는 패킷들에 포함되고, 새로운 모드 변환은 무시되도록 요청한다.

상기 복원기 측면에서, 파라미터 D_MODE 및 D_TRANS가 제공된다. 파라미터 D_MODE에 대하여 가능한 수치들은 단방향에 대한 "U", 낙관에 대한 "O", 신뢰에 대한 "R"이다. 상기 파라미터 D_MODE는 "U"로 초기화 되어야 한다. 더 나아가, 파라미터 D_TRANS에 대하여 가능한 수치들은 초기화에 대한 "I", 진행중에 대한 "P" 및 진행완료에 대한 "D"이다. 파라미터 D_TRANS는 "D"로 초기화되어야 한다. 파라미터 D_TRANS가 "I"로 설정될 때, 상기 복원기는 각 수신된 패킷에 대하여 CRC 옵션을 전달하는 비확인(NACK)와 확인(ACK)를 전송한다.

IP 주소 필드들의 증가된 사이즈들로 인하여, IP 헤더 확장은 IP 주소 확장을 지원에 대하여 필요한 변화들을 최소화하기 위하여 IP 헤더에 도입된다. 그러나, 입력된 패킷이 큰 IP 확장 헤더를 가질 때, 상기 압축기 및 복원기는 예컨대, 압축 및/또는 복원 실패를 야기할 수 있는 문맥 손상으로 인하여 서로 간에 일관성을 상실할 수 있다. 예를 들어, 만약 압축기가 저장할 준비가 된 복원기 보다 큰 IP 확장 헤더 리스트를 압축한다면, 상기 복원기가 최대 사이즈의 IP 확장 헤더 리스트에 대하여 충분한 메모리를 할당하지 않았다는 사실에 기인하여 문맥 손상이 초래될 것이다. 상기 문맥 손상이 발생할 때, 이 주기 동안 패킷 많은 패킷들이 부정확한 복원으로 버려지는 반면, 상기 문맥을 수리하기 위한 긴 시간이 소요된다. 저 압축 효율성을 야기하는 압축되지 않은 패킷 타입이 동기화에 있어서 문맥을 가져오기 위해 사용된다. 또 다른 솔루션에 따라, 최대화 사이즈 IP 확장 헤더 리스트에 대하여 충분한 메모리가 상기 복원기에 할당될 수 있다. 그러나 이는, IP 확장 헤더 리스트의 최대 사이즈가 최대 입력 패킷 사이즈와 동일하기 때문에 방대한 메모리 사용을 초래할 것이다.

발명의 상세한 설명

따라서, 본 발명의 목적은 큰 IP 확장 헤더들로 인한 압축기와 복원기 사이에서 문맥 비일관성이 방지될 수 있는 향상된 헤더 압축 방식을 제공하는 것이다.

이 목적은 패킷 데이터 네트워크의 링크에 대하여 헤더 압축을 제어하는 방법에 의하여 수행되며, 상기 방법은, 상기 링크에 대한 소정의 헤더 확장 사이즈를 설정하는 단계; 그리고 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더가 수신되면, 차후의 복원에 대한 참조로 사용되지 않을 비참조 패킷을 전송하는 단계를 포함한다.

더 나아가, 상기 목적은 패킷 데이터 네트워크의 링크에 대하여 헤더 압축을 제어하는 방법에 의하여 수행되며, 상기 방법은, 상기 링크에 대한 소정의 헤더 확장 사이즈를 설정하는 단계; 그리고 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더가 수신되면, 확인의 전송을 억제하는 단계를 포함한다.

더 나아가, 상기 목적은 패킷 데이터 네트워크의 링크에서 헤더 압축을 제어하는 압축 장치에 의하여 수행되며, 상기 장치는, 상기 링크에 대하여 소정 헤더 확장 사이즈를 설정하는 것에 대한 제어 수단과; 그리고 상기 소정 헤더 확장 사이즈보다 더 큰 확장 헤더 리스트가 수신되면, 차후의 복원에 대한 참조로서 사용되지 않을 비참조 패킷을 발생시키기 위한 헤더 압축 수단들을 포함한다.

마지막으로, 상기 목적은 패킷 데이터 네트워크에 대하여 헤더 복원을 제어하기 위한 복원 장치에 의해 수행되며, 상기 장치는, 상기 링크에 대해 소정 헤더 확장 사이즈를 설정하는 것에 대한 제어 수단과; 그리고 상기 소정 헤더 확장 사이즈보다 더 큰 사이즈의 확장 헤더 리스트가 수신되면, 확인의 전송을 억제하기 위한 헤더 압축 수단들을 포함한다.

따라서, 큰 IP 확장 헤더를 가지는 패킷이 수신될 때 정규 방법으로 복원기 및 압축기 작업을 유지하는 헤더 압축 및 복원 방식이 제공된다. 상기 솔루션은 기존 ROHC 표준과 양립가능하고, 압축기와 복원기 사이의 문맥 비일관성을 방지한다. 문맥들이 복구될 필요가 없고, 복원된 패킷들이 임의의 패킷의 버려짐 없이 정확히 상위 프로토콜 레이어들로 전달되기 때문에 더 높은 압축 효율이 달성된다. 더욱이, 상기 구현의 메모리 사용은 상당히 감소될 수 있다.

상기 헤더 압축은 ROHC 방식을 토대로 할 수 있다. 이 경우에 있어서, 상기 링크의 압축기 측면으로부터 전송된 비참조 패킷은, 동작 모드가 U 모드 또는 O 모드인 경우 발생 식별자 없는 패킷이 될 수 있으며, 여기서, 발생 식별자는 헤더 확장 리스트들의 동일 발생을 나타내기 위하여 사용된다. 반면, 비참조 패킷은 동작 모드가 R 모드인 경우 복원 문맥을 업데이트하지 않는 ROHC-신뢰 모드 패킷이 될 수 있다. 특히, 이 신뢰 모드 패킷은 R-1 모드 패킷이 될 수 있다.

ROHC 방식의 경우에 있어서, 상기 헤더 복원은 큰 확장 헤더의 수신에 응답하는 신뢰 모드로의 변환을 수행하기 위하여 적용될 수 있다.

더 나아가, 상기 역제는 소정 헤더 확장 사이즈와 동일하거나 더 작은 사이즈의 확장 헤더가 수신될 때까지 유지될 수 있다.

실시예

바람직한 실시예가 도 2에 나타낸 바와 같이, ROHC 방식을 사용하여 전송 엔티티(200)와 수신 엔티티(300) 간의 패킷 데이터 전송 링크에 기반을 두고 설명될 것이다. 상기 전송 엔티티(200) 및 수신 엔티티(300)는 예컨대, IP-기반 셀룰라 네트워크와 같은 IP-기반 네트워크의 라우터가 될 수 있다.

바람직한 실시예에 따른 본 압축 및 복원 방식은, IPv4 또는 IPv6 헤더들에 첨부될 수 있는 큰 IP 확장 헤더들 또는 헤더 리스트들에 대처하도록 설계된다. 도 1은 ROHC 압축 패킷에 대한 IETF 사양 RFC 3095에서 특정된 확장 헤더 필드의 형식을 개략적으로 보인 것이다. 도 1에 따르면, 확장 헤더 필드는, 후술할 옥텟들(130)에 제공되는 특정 압축된 시퀀스 넘버들의 존재를 나타내기 위하여 플래그 옥텟(120)을 포함한다. 1비트 플래그들은, 대응하는 상기 옥텟들(120)의 헤더 아이템이 압축될 때 설정된다. 각 플래그가 설정되지 않을 때, 상기 대응하는 헤더 아이템이 압축되지 않거나 또는 존재하지 않는다. 특정의 제1 플래그 CL은 가변 길이의 압축된 헤더 리스트의 존재를 나타낸다. 따라서, 상기 제1 플래그 CL에 근거해, 상기 압축된 헤더 리스트(140)가 상기 확장 헤더 필드(100)에 첨부될 것인지 여부가 결정될 수 있다.

도 3은, 도 2에 도시된 전송 엔티티(200)의 압축기(201)의 압축을 제어하기 위한 압축 제어 유닛(202)에서 수행되는 압축 제어 절차의 개략적인 흐름도를 도시한다. 유사하게, 수신 유닛(300)에서 복원기(301)의 복원을 제어하기 위한 복원 제어 유닛(302)이 제공된다. 전송 엔티티(200)측의 압축기(201) 및 상기 압축 제어 유닛(202)는 압축기(201)는 단일 유닛 또는 전송 엔티티(200)에 저장된 프로그램의 소프트웨어 루틴으로서 구성될 수 있다. 이는 수신 엔티티(300)측의 압축기(301) 및 복원 제어 유닛(302)에도 동일하게 적용될 수 있다.

도 2에 도시되어 있으며, 대역을 벗어난 채널일 수도 있는 제어 채널 cch과 그리고 상기 압축기(201)와 복원기(301)를 연결하기 위한 데이터 채널 dch를 구비하는 2-라인 연결은, 상기 데이터 채널 dch 및 제어 채널 cch가 또한 서로 다른 신호 스트림 또는 서로 다른 프로토콜 레이어의 패킷 유닛과 연관될 수 있기 때문에 포괄적인 혹은 개략적인 도시로서 여겨져야 함이 주목된다. 예컨대, ROHC에 대한 개별 리소스 제한 때문에, IP 확장 헤더 또는 확장 헤더 리스트의 각 소정 숫자들 또는 사이즈들은 예컨대, 전송 엔티티 및 수신 엔티티 오퍼레이터 또는 대응하는 초기화 루틴에 의하여 연관된 링크에 대하여 독립적으로 설정된다. 따라서, 상기 확장 헤더 또는 확장 헤더 리스트의 최대 사이즈는 압축기(201) 및 복원기(301)에 국부적으로 형성되고, 이 중 하나는 다른 하나가 사용하는 값을 알지 못한다.

도 3에 도시된 흐름도에 따르면, 압축 모드는 초기에 단계 S100에서 형성된다. 이 모드 형성의 과정에서, 상기 확장 헤더 리스트에 대해 최대 허용 가능하거나 지원될 수 있는 사이즈가 설정되거나 형성된다. 도 3의 단계 S101에서, IP 확장 헤더(140)를 가지는 패킷이 수신되면, 이 패킷은 예컨대, 입력되는 패킷을 분석하는 동안, 압축기(201)에 의해 탐지된다. 상기 압축 제어 유닛(202)은 수신된 IP 확장 헤더(140)의 사이즈가 전송 엔티티(200)에서 압축을 위해 설정되는 형성된 최대 확장 헤더 리스트 사이즈보다 큰지 여부를 검사한다. 만약 크지 않다면, 단계 S102에서 U모드 또는 O모드가 설정되는지 여부를 검사한다. 만약 그렇다면, 단계 S103에서 발생 식별자가 수신된 패킷에 할당된다. 만약 U-모드도 O-모드도 설정되지 않는다면, R-모드 패킷이 단계 S107에서 발생된다. 본 경우에 있어서, 패킷이 수신될 때 상기 압축기는 U-모드 또는 O-모드에 있다고 가정된다. 이 모드들에 있어서, 연속된 동일한 리스트들은 동일 발생에 속하는 것으로 고려되고, 모두에게 동일 발생 식별자가 할당된다. 상기 발생 식별자는 리스트가 변하고, 참조 리스트로 사용되기 위한 후보인 압축된 리스트와 복원된 리스트에 운반될 때마다 "1"씩 증가된다. 참조 기반 압축 방식, 즉 추가 또는 삭제 기반 방식에 있어서, 리스트의 압축 또는 복원은 압축기(201) 및 복원기(301)의 문맥에 존재하는 것으로 가정되는 참조 리스트를 토대로 한다. 상기 압축된 리스트는 현재 리스트와 참조 리스트 간의 차이들을 코드화한 것이다. 압축된 리스트의 수신하에서, 상기 복원기(301)는 원래 리스트를 획득하기 위하여 그 차이들을 그것의 참조 리스트에 적용한다. 보통, 발생 식별자는 상기 리스트가

참조 리스트로 사용되기 전에 적어도 소정 수의 헤더들에 반복되어야 한다. 그러나, 몇몇 확인들은 O-모드 또는 U-모드에서 전송될 수 있고, 헤더에 대한 확인이 수신될 때면 언제든지 그 헤더의 리스트가 알려진 것으로 판단되어, 추가로 반복될 필요가 없다. 이 참조 기반 압축 방식에 관한 보다 구체적인 사양들은 상기 IETF 설명 RFC 3095로부터 얻을 수 있다.

단계 S108에서, 상기 처리된 패킷은 복원기(301)로 전송되고, 본 절차는 단계 S101로 되돌아간다.

만약 도3의 단계 S101에서의 검사 동작이, 수신된 IP 확장 헤더 리스트의 사이즈가 형성된 최대 헤더 확장 리스트 사이즈보다 더 큰 결과를 초래할 때, 단계 S104에서 상기 압축기(201)가 U-모드 또는 O-모드에 있는지 여부가 검사된다. 만약 단계 S104에서 상기 압축기(201)가 U-모드 또는 O-모드에 있다고 결정되면, 상기 압축기(201)는 발생 식별자 없이 확장 헤더 리스트(140)를 가지는 패킷을 발생시킨다(단계 S105). 발생 식별자 없는 그러한 리스트들은 새로운 발생 식별자를 할당받지 않으며, 미래의 참조 리스트로서 사용되지 않는다. 따라서, 이들은 복원기(301)에서 상기 문맥을 업데이트 하는데 사용되지 않는다.

반면, 단계 S104에서 만약 상기 압축기(201)가 U-모드 또는 O-모드에 있지 않다고, 즉 R-모드에 있다고 결정된다면, 상기 압축기(201)는 RFC 3095에서 정의된 임의의 R1 패킷 종류에 대응될 수 있는 R1-*패킷을 전송한다(단계 S106). 그러한 패킷들은 CRC 필드를 구비하지 않고, 그에 따라 복원기(301)에서 상기 문맥을 업데이트 하기 위한 참조로서 사용되지 않을 것이다. 마지막으로, 단계 S108에서, 상기 발생된 패킷은 복원기(301)로 전송된다.

도 4는 상기 복원 제어 유닛(302)이 수신 엔티티(300)에서 복원기(301)를 제어하는데 있어 기초로 하는 복원 제어 절차의 개념적인 흐름도이다. 도 3의 단계 S100과 유사한 단계 S200에서 복원에 대하여 최대 허용가능하거나 지원될 수 있는 확장 헤더를 형성한 후, 단계 S201에서 수신된 IP 확장 헤더 리스트의 사이즈가 상기 형성된 최대 사이즈보다 더 큰지 여부가 검사된다. 만약 상기 수신된 사이즈가 상기 형성된 최대 사이즈보다 더 크다면, 단계 S202에서 정규 확인이 상기 압축기(201)로 전송되는 것이 허용된다. 주목되는 사항으로써, U-모드 또는 O/R-모드에서 모든 패킷들이 확인되지 않기 때문에, 이 단계에서 복원기(301)가 반드시 확인을 전송할 필요가 없게 된다.

반면, 만약 상기 수신된 사이즈가 상기 형성된 최대 사이즈보다 크다면, 단계 S203에서 상기 복원기(301)가 U-모드 또는 O-모드인지 여부를 검사한다. 만약 그렇다면, 상기 복원 제어 유닛(302)은 R-모드로의 변환을 초기화할 것이고, 상기 복원기(301)는 R-모드 이후에 임의의 확인을 전송하지 않을 것이다(단계 S204). 이 확인들의 역제는, 상기 형성된 최대 사이즈보다 작은 IP 확장 헤더 리스트를 가지는 패킷이 수신될 때까지 지속된다. 만약 상기 복원기(301)가 U-모드 또는 O-모드에 있지 않다고 즉, R-모드에 있다고 단계 S203에서 결정되면, 확인의 전송인 단계 S205에서 억제된다. 마지막으로, 단계 S202, S204 및 S205 이후에, 각각 상기 절차는 단계 S201로 되돌아 간다. 따라서, 초과된 사이즈를 가지는 IP 확장 헤더가 수신되는 한 상기 복원기(301)에서 상기 압축기(201)로 확인들이 전송되지 않는다.

도 5는 큰 확장 헤더를 가지는 패킷 k가 수신될 때, 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTD를 가지는 복원기(301)와 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTC를 가지는 압축기(201) 간의 패킷 전송 방식에 대한 특정 예시를 도시한다.

이 예시에 있어서, 상기 압축기(201)에서의 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTC는 상기 복원기(301)에서의 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTD보다 크거나 최소한 동일하다. 상기 패킷 k에 있는 확장 헤더 리스트는 상기 복원기(301)에서의 형성된 최대 확장 헤더 리스트 사이즈 IP_EXD보다 크지만, 상기 형성된 최대 확장 헤더 리스트 사이즈 IP_EXC보다 작다. 상기 압축기(201)가 U-모드 또는 O-모드에 있다고 가정될 때, 상기 압축기는 발생 식별자를 가지는 패킷을 전송한다. 더 나아가, 도 4의 절차에 따르면, 상기 복원기(301)는 상기 패킷 k를 확인하지 않고, R-모드로의 모드 변환을 나타내는 파라미터를 가지는 비확인 NACK(R)을 전송한다. 이 NACK(R) 메시지를 수신할 때, 상기 압축기(201)는 또한 파라미터 C_MODE에 의해 나타낸 바와 같이 R-모드로의 변환을 수행한다. 더욱이, 확인이 수신되지 않을 때, 상기 패킷 k가 참조로서 사용될 수 없기 때문에 파라미터 C_TRANS는 상태 "P"로 설정된다. 그 다음, 상기 압축기(201)는 상기 복원기(301)에서 차후의 복원에 대한 참조로서 사용될 수 있는 예컨대, UOR-2와 같은 패킷 타입 2를 전송한다. 대안으로서, 상기 압축기(201)는 상기 문맥의 동적인 일부분과 커뮤니케이션하는 IR-DYN 패킷 즉, RFC 3095로 정의되는 비상수 함수들의 파라미터들을 전송할 수 있다. 그러나, 이 패킷들 내의 리스트는 여전히 상기 복원기(301)의 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTD보다 크다.

R-모드 및 D_TRANS 파라미터 상태 "P"에 있는 상기 복원기(301)가 UOR-2 또는 IR-DYN 패킷을 수신할 때, 도 4의 단계 S205에서 나타낸 바와 같이 상기 복원기는 임의의 확인을 전송하지 않는다. 이 절차는, 형성된 최대 확장 헤더 리스트 사이즈 IP_EXTD와 같거나 작은 사이즈의 확장 헤더 리스트를 가지는 패킷 N이 상기 압축기(201)에 수신되고 상기 복원

기(301)에 전송될 때까지 계속된다. 허용가능한 확장 헤더 리스트 사이즈를 가지는 이 패킷의 수신 응답으로서, 상기 복원기(301)는 확인 ACK를 발생시키고, 상기 압축기(201)는 C_TRANS 파라미터를 상태 "D"로 설정하며, 미래 압축을 위한 참조 리스트로서 상기 패킷 N에 있는 리스트를 사용한다.

만약 상기 복원기(301)가 상기 복원기에 대하여 형성된 최대 사이즈 IP_EXTD보다 큰 확장 헤더 리스트를 가지나 확장 헤더 리스트에 발생 식별자를 가지지 않는 패킷을 수신한다면, R-모드로의 변환은 초기화되지 않는다. 만약 상기 수신된 사이즈가 복원기(301)에서의 형성된 최대 사이즈 IP_EXTD보다 크고, 형성된 최대 사이즈 IP_EXTC보다도 크다면, 상기 변환이 발생할 것이다.

상기 압축기(201)에 정의된 슬라이딩 윈도우의 오버플로우가 발생할 때, 슬라이딩 윈도우 내의 모든 요소들을 유지할 수 있고, 현재 참조 리스트를 사용하여 R1-* 패킷을 전송할 수 있다. 대안으로, 가장 오래된 요소가 슬라이딩 윈도우로부터 제거될 수 있고, CRC를 가지는 패킷이 삽입될 수 있다. 만약 슬라이딩 윈도우 내의 패킷들이 참조 리스트로 사용될 수 없는 것을 의미하는 피드백이 전혀 수신되지 않는다면, 현재 참조 리스트는 여전히 압축을 위해 사용될 것이다.

본 발명은 상기 언급된 실시예에 한정되지 않으나, 가변 사이즈의 확장 헤더들이 사용되는 임의의 확인된 패킷 데이터 전송 링크에서 구현될 수 없음에 주의한다. 따라서, 상기 언급된 실시예는 첨부된 청구항들의 범위 내에서 변화시킬 수 있다.

도면의 간단한 설명

이하에서, 본 발명은 수반된 도면들을 참조하여 언급된 실시예에 근거해 좀더 구체적으로 설명될 것이다.

도 1은 IP 확장 헤더 필드 포맷의 개념적인 표현을 도시한다.

도 2는 상기 언급된 실시예에 따라 압축기 및 복원기를 포함하는 전송 링크의 개념적인 블록도를 도시한다.

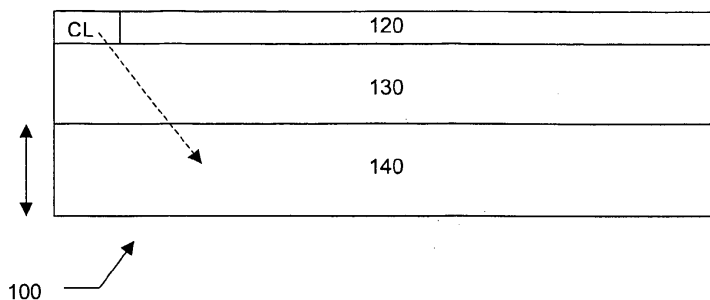
도 3은 상기 언급된 실시예에 따라 압축 제어 절차의 개념적인 흐름도를 도시한다.

도 4는 상기 언급된 실시예에 따라 복원 제어 절차의 개념적인 흐름도를 도시한다.

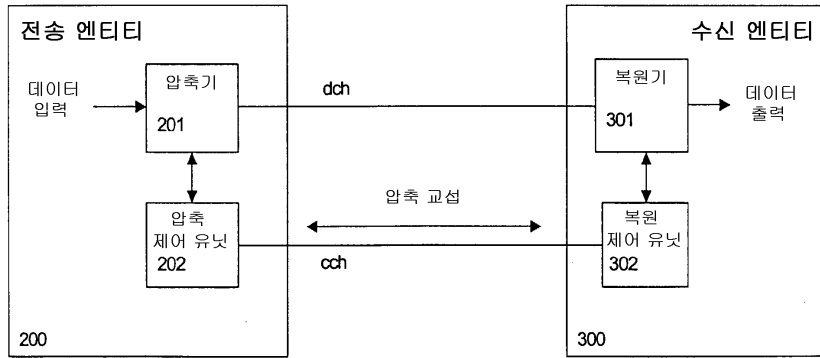
도 5는 상기 언급된 실시예에 따라 패킷 흐름도의 예시를 도시한다.

도면

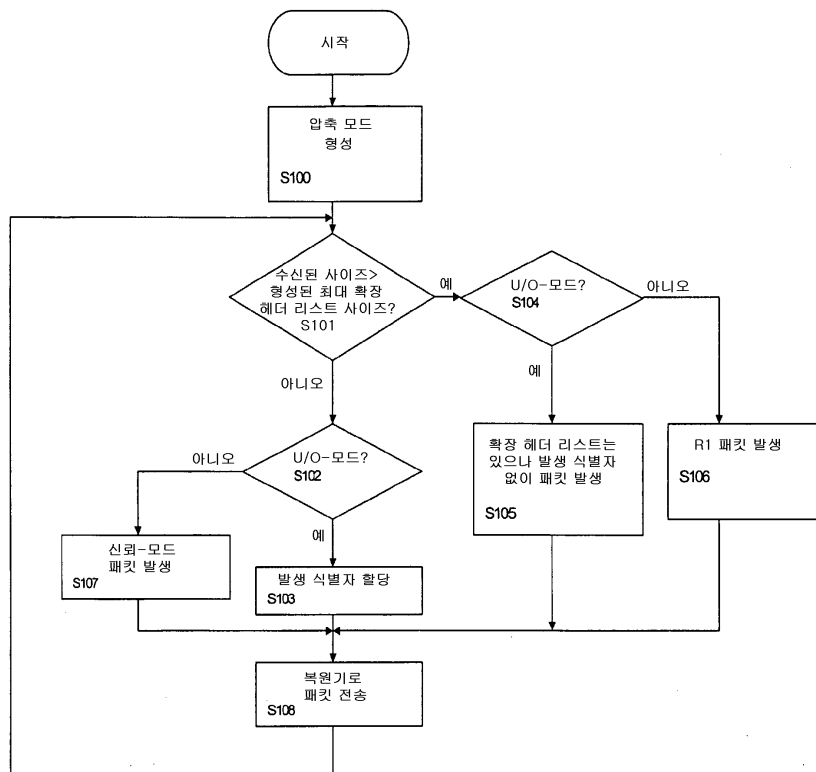
도면1



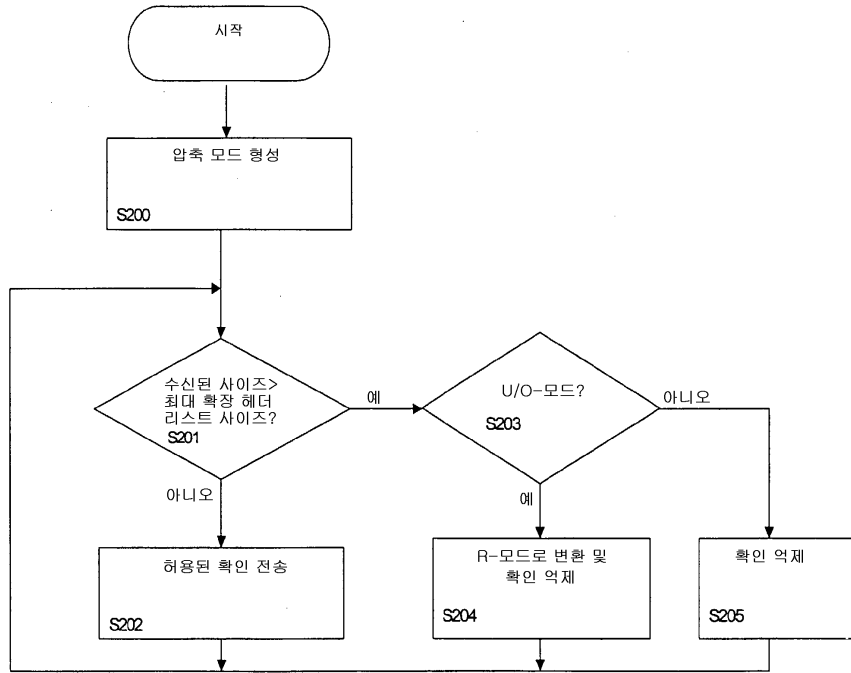
도면2



도면3



도면4



도면5

