Comparação entre as Extensões *Bundle Security Protocol*, *Streamlined Bundle Security Protocol* e *Bundle Protocol Security Specification* para o *Bundle Protocol*

Lucas W. P. Pinto[1], **Jéferson C. Nobre**[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
Caixa Postal 275 – 93.022-000 – São Leopoldo – RS – Brasil

were.sl@gmail.com, jcnobre@unisinos.br

Abstract. *This document has as an objective to present a comparative study between the developed extensions to the Bundle Protocol known as Bundle Bundle Security Protocol, Streamlined Bundle Security Protocol and Security Bundle Protocol Specification. Then it presents the reasons that led to the development of such extensions, which were not considered relevant in the beginning of the development of the Bundle Protocol. Finally, it explains the different characteristics of each extension and compares them with each other.*

Resumo. *Este documento tem como objetivo apresentar um estudo comparativo entre as extensões desenvolvidas para o Bundle Protocol conhecidas como Bundle Security Protocol, Streamlined Bundle Security Protocol e Bundle Protocol Security Specification. Apresenta ao decorrer do trabalho os motivos que levaram ao desenvolvimento de tais extensões, que não foram consideradas relevantes no principio do desenvolvimento do Bundle Protocol. Por fim, explana as diferentes características de cada extensão e as compara entre si.*

1. Introdução

Ambientes desafiadores (*Challenged Networks*) apresentam dificuldades para o funcionamento de redes tradicionais, como a Internet. As condições encontradas nestes ambientes ocasionam alguns problemas em redes de computadores, como por exemplo longos períodos de desconexões que dificultam a comunicação fim-a-fim. São exemplos de ambientes desafiadores a Internet Interplanetária (*InterPlanetary Networking* - IPN), Redes em Campos de Batalha (*Battlefield Networking*), comunicações rurais e comunicações submarinas. Essas redes são agrupadas pelo conceito de Redes Tolerantes à Atrasos/Desconexões (*Delay/Disruption Tolerant Networking* - DTN) [Cerf et al. 2007].

O conceito de DTN tomou forma através dos estudos do Grupo de Pesquisa de DTN (*DTN Research Group* - DTNRG) da IRTF (*Internet Research Task Force*) [DTNRG 2016]. Esta equipe desenvolveu um framework para DTN com o objetivo de auxiliar na resolução dos problemas encontrados nos ambientes desafiadores, e de tornar viável a utilização efetiva de redes nestes ambientes. Considerando que seu objetivo principal fora concluído, a equipe transferiu a responsabilidade de novas implementações para o grupo de trabalho de DTN (*DTN Working Group* - DTNWG) da IETF (*Internet Engineering Task Force*) [DTNWG 2016].

O DTNRG percebendo a necessidade de um mecanismo padrão para auxiliar na comunicação entre nodos em DTNs, desenvolveu o protocolo Bundle (*Bundle Protocol* -

BP)[Scott and Burleigh 2007]. O BP viabiliza a transmissão de mensagens entre nodos, através de uma lógica de armazenamento e envio de pacotes. Isto permite que o nodo armazene localmente todos os pacotes que recebe, para enviá-los quando houver uma conexão disponível com outro nodo. Embora funcional, o BP deixa fora de seu escopo a garantia de segurança e verificação de erros nestas comunicações. Isto se deve ao fato de existirem uma série de barreiras que dificultam a implementação de segurança em DTNs [Ivancic 2010].

Inicialmente o BP não tratava os problemas específicos de segurança existentes em uma DTN, porém com o passar do tempo o grupo de trabalho percebeu que era necessário alguma forma de implementação de segurança no BP. A partir daí o grupo vem desenvolvendo uma série de extensões para o BP que focam exclusivamente em segurança, são elas *Bundle Security Protocol* (BSP), *Streamlined Bundle Security Protocol* (SBSP) e *Bundle Protocol Security Specification* (BPSec).

2. Fundamentação Teórica

O Protocolo Bundle (*Bundle Protocol* - BP) foi desenvolvido pelo DTNRG, e seu objetivo é tratar de alguns problemas encontrados em DTNs e abstrair a responsabilidade de aplicações que rodam nestas redes de resolve-los. A sua arquitetura foi desenvolvida para atender as necessidades de uma grande variedade de classes de redes divergentes, incluindo IPN, redes submarinas, redes de campos de batalha, entre outros. [Wood et al. 2009].

A especificação descrita na RFC 5050, define que o BP trabalha na camada de agregação, e se utiliza de interfaces com as camadas inferiores chamadas de Adaptadores da Camada de Convergência (*Convergence Layers Adapters* - CLAs) para realizar o transporte de informações. Não é necessário instalar o BP em todos o nodos de uma rede, apenas nos *endpoints* e em alguns nodos intermediários selecionados, geralmente localizados nas bordas das partes homogêneas de uma rede heterogênea. A Figura 1 apresenta a estrutura encontrada em uma rede DTN.

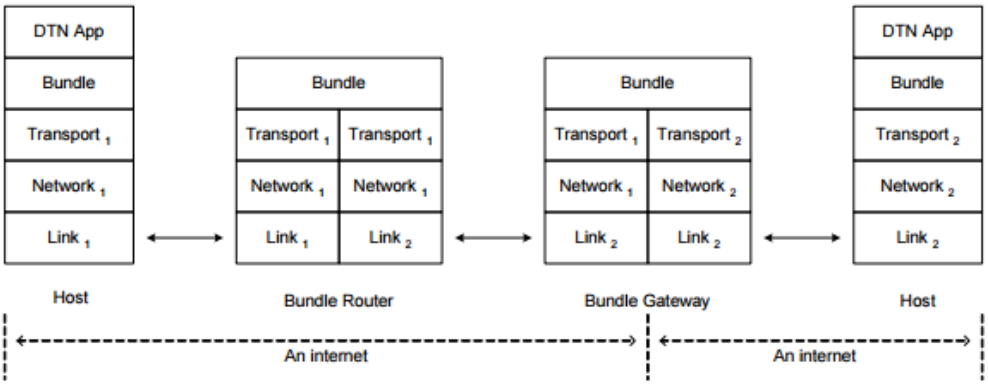

Figura 1. Arquitetura de uma DTN

A instalação do BP nos *endpoints* e em alguns nodos intermediarios faz com que o caminho original fim-a-fim seja divido em múltiplos pulos de DTN. As semânticas de transporte fim-a-fim são redefinidas, sendo agora confinadas dentro de cada pulo DTN.

Isto torna possível que seja usado em cada pulo o melhor protocolo de transporte para aquela situação. Esta possibilidade de juntar protocolos de acordo suas características é a primeira grande vantagem oferecida pela arquitetura do BP. Em particular, isto permite o uso de variantes especializados do TCP, como o Hybla [Caini and Firrincieli 2004], em links de GEO satélites, ou protocolos especializados como o Saratoga [Wood et al. 2007] e o LTP (*Licklider Transmission Protocol*) [Ramadas et al. 2008], em satélites LEO (*Low Earth Orbit*) e pulos no espaço livre [Rodrigues 2014].

A fragmentação do bundle é uma das características mais distinguiveis de DTN. Pode ser proativa para ajustar a dimensão de um bundle com a limitação de dados que podem ser transferíveis em um contato, ou reativa, para evitar retransmissão de informação já recebida em caso de desconexão de um link. Com relação a fragmentação reativa, é preciso notar que a possibilidade de reiniciar um download de um ponto intermediario é muito comum em muitas aplicações de transferências de arquivos. Essa característica agora é oferecida a camadas superiores, por exemplo para aplicações DTN, como um serviço do BP. Em contraste com aplicações TCP, as aplicações DTN não precisam incluir qualquer código para implementar esta função.

3. Problemas de Segurança do *Bundle Protocol*

Embora muito do BP já tenha sido discutido e oficializado em RFCs, ainda existem muitos problemas a serem resolvidos em sua arquitetura. Todas as especificações de segurança citadas nas sessões anteriores, ainda estão para terem uma implementação prática e não fazem parte da definição do BP.

O BP sem estas extensões não realiza verificações para detectar bundles danificados, pois não possui suporte para detecção de erros e rejeição de bundles corrompidos (tanto em blocos de metadados quanto em blocos de carga de informações). Fazendo com que o BP não consiga determinar se o pacote entregue ao destino está livre de erros ou não.

Sem uma forma confiável de detecção de erros, a técnica de transferência do BP não pode garantir que um nodo que se tornará o novo portador do bundle e terá a responsabilidade de entregar este ao próximo nodo, realmente recebeu um bundle não corrompido para conseguir repassar. Além disso, a corrupção de metadados em um bundle podem causar diversos problemas graves, como a impossibilidade de se descriptografar blocos previamente criptografados até a não entrega desde bundle para outro nodo.

Esta importante funcionalidade do bundle foi deixada propositalmente de fora de sua arquitetura com a justificativa de que nem todas as aplicações necessitam de detecção de erros ou integridade de dados, e que se desejarem devem implementá-los por conta própria. Porém esta afirmação falha em perceber que a possível corrupção de metadados do próprio bundle não é verificada pela camada de aplicação, e que o protocolo em si deveria ser capaz de determinar estes problemas no seus cabeçalhos.

Deixar recuperação de erros para as aplicações é apenas possível quando elas tem muito controle sobre a rede em que estão rodando, possuindo a capacidade de reenvio de mensagens com erros. Redes DTN não possuem controle sobre as condições dos ambientes desafiadores e por isso podem não ter estrutura para reenvio de mensagens, neste caso impossibilitando uma aplicação de fazer este tipo de controle.

4. Extensões de Segurança para o *Bundle Protocol*

Segurança é importante para o protocolo Bundle. Muitas vezes os ambientes desafiadores sobre os quais o protocolo Bundle opera, são hostis e requerem que a DTN seja protegida de acesso não autorizado. Porém estes ambientes possuem algumas barreiras que impõem desafios para a implementação de mecanismos de segurança no protocolo Bundle, como por exemplo, a impossibilidade de gerenciar chaves em uma DTN. Além disso, as DTNs podem estar funcionando sobre ambientes onde uma porção da rede seja comprometida, e acabe conflitando com os pilares de segurança de confidencialidade, integridade e disponibilidade [Birrane 2014].

As extensões de segurança seguem as seguintes diretivas de funcionamento:

4.1. Granularidade do Bloco

Blocos em um bundle representam diferentes tipos de informação. O bloco primário contém identificação e informação de roteamento. O bloco de payload carrega dados da aplicação. O Bloco de extensão carrega uma variedade de dados que podem prover informações adicionais necessárias para o processamento de um bundle ao logo do caminho. É importante aplicar diferentes tipos de segurança em um bundle, pois este possui blocos que podem representar diferentes tipos de informação com diferentes necessidades de segurança.

Por exemplo, em um bundle um bloco de payload pode ser criptografado para proteger seu conteúdo, mas um bloco de extensão contendo informações relacionadas com esse payload deve ficar descriptografado, pois precisa disponibilizar essas informações para um nodo, sem que esse possa descriptografar o payload também.

4.2. Múltiplas Origens de Segurança

O BP permite que blocos de extensão sejam adicionados em um bundle a qualquer momento durante a sua existência em uma DTN. Quando um nodo adiciona um novo bloco de extensão no bundle, este novo bloco pode ter extensões de seguranças aplicadas à ele. Similarmente, um nodo pode adicionar serviços de segurança em um bloco de extensão já existente, desde que seja consistente com sua política de segurança. Por exemplo, um nodo que se encontra na borda de uma parte confiável da rede com uma não confiável, pode aplicar criptografia ao bloco de payload em todos os bundles saindo da parte confiável em direção a não confiável.

Nos dois casos, um nodo que não o originário do bundle pode adicionar um serviço de segurança neste bundle, e com isso, se tornar a origem daquele serviço de segurança fazendo com que a origem de segurança seja diferente da origem do bundle. Serviços de segurança devem sempre saber quem é o seu nodo de origem, para conseguir aplicar propriamente políticas e seleção de chaves associadas com o processamento de segurança no nodo de destino.

Por exemplo, um nodo N1 envia um bundle como N3 sendo o destino final. No meio do caminho o nodo N2 adiciona um serviço de segurança no bundle, neste momento o nodo N1 ainda é considerado a origem do bundle, porém N2 agora é considerado a origem do serviço de segurança. Quando o bundle atingir seu destino no nodo N3, este irá saber quais métodos irá utilizar para processar o serviço de segurança, pois sabe quem o aplicou.

Um bundle pode ter múltiplos blocos de segurança e esses blocos podem ter diferentes nodos de origem. Cada bloco de segurança em um bundle deve ser associado com uma operação de segurança específica. Todos os blocos de segurança que realizam a mesma operação devem ter o mesmo nodo de origem.

Por fim, todos os nodos devem enviar os blocos na mesma ordem em que os receberam. Este requisito se aplica em toda a DTN, não apenas nos nodos que adicionam blocos de segurança ou os processam.

Diferentes nodos em uma DTN podem ter diferentes capacidades de segurança. Alguns nodos podem não ser cientes de segurança e não irão entender qualquer bloco de extensão relacionado a segurança. Outros nodos podem ter políticas de segurança que irão requerer que os serviços de segurança sejam processados em nodos que não o de destino do bundle (por exemplo, verificar assinaturas de integridade em nodos que se encontram antes do destino). Alguns nodos podem ignorar o processamento de segurança se eles não forem o destino no bundle.

4.3. Considerações de Segurança

Gestão de chaves em DTNs é reconhecido como um tópico difícil e não é resolvido nas extensões de segurança.

Algumas aplicações de DTN precisam assinar e criptografar uma mensagem, e existem alguns problemas à levar em consideração sobre isso. Se a intenção é de a prover uma segurança de que a mensagem, de fato, não foi modificada desde a sua orgiem, então deve ser primeiramente assinada e só então criptografada. Uma assinatura em uma mensagem criptografada não estabelece nenhuma relação entre o assinante e a mensagem que foi cifrada.

Por outro lado, se a intenção é reduzir o risco de ataque de negação de serviço (*Denial-Of-Service Attacks* - DOS Attacks), então a assinatura da mensagem criptografada é apropriado. Uma mensagem que falha em uma verificação de assinatura não passará pelo intenso processo computacional para ser descriptografada.

Se um nodo for gerar algum relatório em um evento de falha se segurança, então alguma informação com relação a estrutura interna ou políticas de segurança da DTN podem vazar. É recomendado que seja utilizado muito cuidado ao se utilizar este recurso.

4.4. Bundle Security Protocol - BSP

A existência de problemas de segurança não tratados em DTN, levou a criação da extensão de segurança para o BP conhecida como (*Bundle Security Protocol* - BSP)[Symington et al. 2011].

O BSP é aplicado por definição apenas aos nodos que aceitam sua implementação, estes nodos são conhecidos como Nodos Cientes de Segurança (*Security-Aware Nodes*). Podem existir nodos em uma DTN que não implementam o BSP, e estes podem se comunicar sem nenhuma restrição com os nodos que são cientes de segurança. Porém as operações de segurança apenas poderão serem executadas em nodos que implementaram o BSP.

Uma das características mais interessantes do BSP é que ele leva em consideração a segurança fim-a-fim e pulo-a-pulo, com soluções diferentes. É oferecida a possibilidade

de proteger os dados que estão sendo transportados no bundle e outros tipos de dados (e.g. metadados), com diferentes chaves. Ambas destas características são inovadores e permitem proteger eficientemente o tráfego do bundle.

O BSP pode adicionar os seguintes blocos de segurança em um Bundle:

- Bloco de Autenticação do Bundle (*Bundle Authentication Block* - BAB): É utilizado para garantir a autencidade e integridade do pacote de um único pulo entre dois nodos. Por isso, BABs operam apenas entre dois nodos adjacentes.
- Bloco de Integridade de Carga (*Payload Integrity Block* - PIB): Empregado para prover autenticação e integridade sobre múltiplos pulos (normalmente, mas não necessariamente, fim-a-fim). Mesmo que essencialmente o PIB seja considerado fim-a-fim, ele pode ser verificado em qualquer nodo que se encontre entre a o nodo que concatenou o PIB ao pacote, e o destino final do bundle. Porém será necessário que este nodo tenha acesso as chaves criptográficas de autenticação.
- Bloco de Confidencialidade de Carga (*Payload Confidentiality Block* - PCB): Utilizado para prover confidencialidade dos dados sendo carregados pelo bundle entre a origem e o destino, analogamente ao PIB.
- Bloco de Extensão de Segurança (*Extension Security Block* - ESB): Desenvolvido para prover segurança para bloco que não o de carga de dados, como por exemplo metadados. A ideia é de que as chaves do ESB, sendo diferentes de outros blocos de segurança, podem ser disponibilizadas para nodos intermediários selecionados, como roteadores DTN, sem comprometer a segurança fim-a-fim.

É importante citar que alguns aspectos definidos em [Symington et al. 2011] foram recentemente descobertos como dificilmente compatíveis com a fragmentação do BP. É muito provável que as características do BSP sejam revisadas e simplificadas em um futuro próximo para remediar este problema [Rodrigues 2014].

4.5. Streamlined Bundle Security Protocol - SBSP

O conceito de *Streamlined Bundle Security Protocol* - SBSP veio de uma necessidade de simplificação do BSP. Diferente do BSP, o SBSP define apenas três blocos adicionais que podem ser concatenados a um pacote bundle para garantirem a segurança de uma mensagem [Birrane 2014].

O SBSP pode adicionar os seguintes blocos de segurança em um Bundle:

- Bloco de Autenticação do Bundle (*Bundle Authentication Block* - BAB): Garante autenticação e integridade de pacotes pulo-a-pulo.
- Bloco de Integridade de Carga (*Payload Integrity Block* - PIB): é usado para garantir a autencidade e integridade da parte do pacote que o remetente do PIB deseja assegurar. A autenticação da informação no PIB pode ser verificada por qualquer nodo que se encontro no caminho do remetente do PIB e o destinatário do pacote.
- Bloco de Confidencialidade de Carga (*Payload Confidentiality Block* - PCB): indica que que uma parte do pacote foi criptografada, toda ou apenas uma parte dela, no nodo originário do PCB para garantir a proteção de seu conteúdo até o nodo de destino.

4.6. Bundle Protocol Security Specification - BPSec

A constante necessidade de melhoria da segurança, levou por fim ao desenvolvimento da mais recente proposta de extensão para o BP, chamada de BPSec. Esta extensão foi baseada nas estruturas do BSP e do SBSP, tendo como objetivo primário simplificar o uso de segurança no BP, assim como aumentar sua segurança.

O BPSec pode adicionar os seguintes blocos de segurança em um Bundle:

- Bloco de Integridade de Bloco (*Block Integrity Block* - BIB): é usado para garantir a autencidade e integridade da parte do pacote que o remetente do BIB deseja assegurar. Funciona como uma assinatura do bundle.
- Bloco de Confidencialidade de Bloco (*Block Confidentiality Block* - BCB): indica que que uma parte do pacote foi criptografada. Bundles que possuem este bloco foram criptografados.

5. Discussão

As três extensões para o BP citadas neste trabalho, apesar de serem consideradas diferentes, são na verdade uma evolução de um mesmo conceito. O BSP sendo a primeira extensão a ser desenvolvida, apresentou um grande problema em relação a complexidade de implementação. O SBSP partiu da ideia do BSP e foi uma tentativa de simplificação deste. Por fim a mais recente extensão chamada de BPSec, seria a versão definitiva de segurança para o BP.

A maior diferença notável entre as extensões é a simplificação de seus blocos de segurança, que com o tempo foram diminuindo de quantidade para facilitar sua implementação. Com isso o ganho de performance do BPSec também é maior, pois com menos blocos de segurança, mais rápido serão os processamentos de segurança em cada nodo.

É importante citar que não existe uma comparação de performance testada entre as extensões, mas com a diminuição de processamentos de segurança em cada nodo, se espera que exista uma diferença.

Tabela 1. Comparação das Características entre as Extensões

	BSP	SBSP	BPSec
Complexidade	Elevada: 4 blocos	Média: 3 Blocos	Simples: 2 Blocos
Performance	Lenta	Média	Teoricamente mais rápida

Com relação a diferença de segurança, se tem a noção de que as extensões BSP e SBSP possuem um nível mais elevado de segurança, pois fornecem mais blocos com funções diferentes. Porém o BPSec foi desenvolvido com uma noção de que muitos blocos proviam um nível de segurança desnecessário para DTNs.

6. Conclusão e Trabalhos Futuros

Este trabalho teve o objetivo de mostrar um comparativo entre as extensões desenvolvidas até o momento para o protocolo BP. Mesmo que exista um maior ganho de segurança

com as versões antigas, as limitações de hardware encontradas em DTNs exigem que seus nodos não possam gastar tantos recursos com processamento. A escolha de qual melhor extensão para ser implementada irá sempre depender do ambiente em que a DTN se encontra.

Para futuras pesquisas seria interessante um experimento prático com os três protocolos, para verificar a veracidade de dificuldades de implementações nas versões antigas, ou do ganho de performance em BPSec.

Referências

Birrane, E. (2014). Streamlined bundle security protocol specification. Technical report, Delay-Tolerant Networking Research Group.

Caini, C. and Firrincieli, R. (2004). Tcp hybla: a tcp enhancement for heterogeneous networks. *International journal of satellite communications and networking*, 22(5):547–566.

Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and Weiss, H. (2007). Rfc 4838. *Delay-Tolerant Networking Architecture, IRTF DTN Research Group, April*.

DTNRG (2016). Delay-tolerant networking research group. ¡https://irtf.org/concluded/dtnrg¿. Acesso em: ago. 2016.

DTNWG (2016). Delay-tolerant networking working group. ¡https://datatracker.ietf.org/wg/dtn/charter/¿. Acesso em: set. 2016.

Ivancic, W. D. (2010). Security analysis of dtn architecture and bundle protocol specification for space-based networks. In *Aerospace Conference, 2010 IEEE*, pages 1–12. IEEE.

Ramadas, M., Burleigh, S., et al. (2008). Licklider transmission protocol-specification.

Rodrigues, J. (2014). Advances in delay-tolerant networks (dtns): Architecture and enhanced performance.

Scott, K. and Burleigh, S. (2007). Bundle protocol (bp). ietf request for comments. Technical report, RFC 5050.

Symington, S., Farrell, S., Weiss, H., and Lovell, P. (2011). Bundle security protocol specification. Technical report.

Wood, L., Eddy, W. M., and Holliday, P. (2009). A bundle of problems. In *Aerospace conference, 2009 IEEE*, pages 1–17. IEEE.

Wood, L., Eddy, W. M., Ivancic, W., McKim, J., and Jackson, C. (2007). Saratoga: a delay-tolerant networking convergence layer with efficient link utilization. In *Satellite and Space Communications, 2007. IWSSC'07. International Workshop on*, pages 168–172. IEEE.