Análise do Impacto em Redes DTN na Implementação de Autenticidade do Nodo Enviador

Cristiane Bellenzier Piaia[1], **Afonso Comba de Araújo Neto**[2]

[1]Serviço Nacional de Aprendizagem Comercial
Faculdade Senac Porto Alegre

cbellenzierpiaia@gmail.com

[2]Centro de Processamento de Dado – Universidade Federal do Rio Grande do Sul (UFRGS)
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS – Brazil

afonso@cpd.ufrgs.br

Resumo. *Delay Tolerant Network (DTN) são redes especiais onde requisitos como disponibilidade são diferentes das redes TCP/IP tradicionais. Muita pesquisa e desenvolvimento relacionadas as mesmas estão em andamento, porém a segurança é um dos pontos que apresenta muitas lacunas. Este trabalho apresenta uma implementação de autenticação do nodo enviador da mensagem em DTN. A solução desenvolvida utiliza algoritmo RSA para criptografar os dados e uma função de hash para validar a identidade dos nodos que se comunicam.*

1. Introdução

Delay Tolerant Network (DTN) são redes sem fio que além de utilizarem o ar como propagação, apresentam características únicas tais como atrasos longos e frequentes desconexões [de Oliveira et al. 2007].

Com o intuito de garantir a autenticidade do nodo enviador da mensagem, este trabalho propõe e desenvolve uma opção de segurança para redes DTN.

Este documento está dividido como segue. Na seção Trabalhos Relacionados é apresentada a fundamentação teórica referente à segurança para DTN. A seção Solução trata da proposta desenvolvida. Já na seção Resultados, os mesmos são apresentados e os aspectos observados através de simulações realizadas. Já na seção final, a Conclusão estão é apresentada, assim como trabalhos futuros.

2. Trabalhos Relacionados

Em [Templin 2015] é proposto um trabalho que visa resolver o problema com gerenciamento das chaves utilizadas pelos nodos. Boletins informativos contendo informações sobre chaves publicas são realizados por uma administradora de chaves. Esses boletins devem ser recebidos por todos os nodos em qualquer posição geográfica. Cada nodo é responsável por criar suas chaves, e em seguida informar a administradora, que comunica através de seus boletins, os demais nodos. Como fica claro, o ponto base dessa solução é confiança na administradora de chaves.

Para resolver problemas como autenticidade, integridade e serviços confidenciais, o *Bundle Security Protocol* foi proposto [Farrell et al. 2011].

O trabalho apresentado por [Clarke et al. 2012] mostra uma combinação de soluções de segurança já aceitas em redes tradicionais e DTN (como a RFC 6257), além de uma série de preocupações a serem resolvidas arquiteturalmente. A proposta não foi validada até o presente momento.

Baseado em Infra-estrutura de chaves públicas, utilizando conceitos tradicionais de criptografia para prover autenticidade e integridade [Johnson et al. 2012] apresenta um proposta para DTN e a avalia.

3. Solução Proposta

Este trabalho implementa um algoritmo assimétrico de criptografia e função de *hash* para garantir a autenticidade do enviador da mensagem. O algoritmo de chaves assimétricas utilizado neste trabalho foi RSA [Rivest et al. 1978]. O algoritmo utilizado para cálculo de *hash* foi o *Secure Hash Algorithm* [FIPS 1995]. Nesse trabalho fez-se o uso da versão com tamanho de 256, SHA-256. O objetivo do experimento é avaliar qual o impacto no envio e no recebimento das mensagem quando o nodo enviador encontra-se autenticado.

Envio da Mensagem O algoritmo de *hash* foi utilizado visando validar que o enviador da mensagem, não foi alterado em seu trajeto, o resultado é anexado junto as informações relacionadas ao nodo enviador da mensagem. O valor do *hash* é encriptado utilizando o algoritmo RSA, com a chave privada do enviador da mensagem. Cada nodo é responsável pela criação de suas próprias chaves, dessa forma, o cenário de testes fica simplificado, pois cada certificado pode ser instalado em cada nodo de forma *offline*, dessa forma não interferindo na execução do algoritmo. A chave pública do enviador da mensagem também é anexado junto as suas informações.

Recebimento da Mensagem No momento em que a mensagem chegar em algum nodo intermediário ou em seu destino, utilizando a chave pública do enviador da mensagem, o conteúdo do *hash* é descriptografado e verificada a veracidade dos dados referente ao enviador da mensagem. Dessa forma é possível garantir que o enviador da mensagem realmente é quem afirma ser. Já quando o cálculo do *hash* é validado, também é possível garantir que não houve alteração no enviador da mensagem.

4. Avaliação Experimental

4.1. Simulação

Foi utilizado um simulador desenvolvido para tal tipo de rede, chamado de ONE (*Opportunistic Network Environment*) [Keränen et al. 2009].

Algumas bibliotecas foram incluídas para a implementação da solução: *Big Integer*, *Secure Random* e *Message Digest*.

Algumas classes foram acrescidas ao pacote referente aos algoritmos de RSA e *hash*. Já as seguintes classes próprias do simulador, formam modificadas: *DTNHost* e *MessageRouter*.

DTNHost foi alterada para criar as chaves do nodo enviador, realizar o seu cálculo do *hash* e encriptar esses dados.

Já em *MessageRouter* os dados então são descriptografados e validados. Em caso negativo, o pacote é descartado.

Com a solução desenvolvida, é possível garantir que os nodos que enviam a mensagem são quem afirmam ser, e não sofreram alteração durante o trajeto percorrido. Porém não garante que apenas nodos autorizados enviem mensagem, o que é prejudicial em DTN pois consome recursos da rede.

4.2. Cenário para Simulação

Foram realizadas sete rodadas de simulações. Os resultados apresentados nesta seção foram obtidos pela média de todas as rodadas, com um intervalo de confiança de 95% [Jain 1990].

Cada rodada contempla os seguintes quesitos: 12 horas de simulação, padrão do simulador, 60 elementos, onde 30 pessoas e 30 automóveis [Nunes et al. 2010], *Time To Live*) de 5 horas, *buffer* de 5 MBytes, alcance de 30 metros, usual em dispositivos móveis [Nunes et al. 2010], 250kbps de velocidade de transmissão, valor também padrão do simulador, *Shortest Path Map Based Movement* como padrão de movimentação[Keränen and Ott 2007], estratégia das filas FIFO (*First In First Out*) [Nunes et al. 2010], protocolo de roteamento utilizado foi o *Spray and Wait* e o tempo de *Warmap* foi de 1000 segundos, padrão do simulador.

5. Resultados

Como o enviador da mensagem é responsável pela criação de suas próprias chaves, e do cálculo de *hash*, não há nenhuma alteração no processo para criação das mensagens, por esse motivo o número de mensagens criadas não sofreram alterações, com e sem autenticação 999.

Quando uma mensagem é recebida por nodos intermediários (recebida por nodos e repassadas) ou pelo seu destino, a chave pública do enviador da mensagem é utilizada para descriptografar o cálculo de *hash* e o mesmo é verificado. Por esse motivo, caso a chave pública não consiga descriptografar a mensagem é garantido que o enviador da mensagem, não é quem diz ser. Porém, caso seja possível descriptografar a mensagem com sua chave pública, mas o cálculo de *hash* não conferir, então ocorreu uma alteração do destinatário da mensagem.

Como nesse cenário não foi simulado qualquer ataque que realize alguma dessas alterações nos nodos, a média da quantidade de mensagens entregues também não sofreram alteração, com e sem autenticação foram 960.

Para que ocorra divergência entre a quantidade de mensagens entregues com ou sem autenticação, é necessário que não seja possível descriptografar o nodo ou que o cálculo de *hash* esteja divergente.

6. Conclusão

DTN são redes sem fio com características únicas como frequentes desconexões e atrasos na entrega de suas mensagens.

A segurança é um de seus desafios, e é o assunto abordado nesse trabalho. Este trabalho estudou trabalhos realizados na área e apresenta uma solução para o problema de autenticidade do nodo enviador da mensagem.

Essa solução realiza o cálculo de *hash* do enviador da mensagem, o criptografa utilizando sua chave privada, dessa forma quando a mensagem é recebida, sua chave pública é utilizada para descriptografar a mensagem. Caso não seja possível realizar essa operação a mensagem é descartada pois o enviador da mensagem não é quem diz ser. Já em caso positivo, é realizada uma verificação do cálculo de *hash*, e em caso positivo a mesma é aceita ou repassada, porém se negativo, a mensagem também é descartada pois ocorreu uma alteração no enviador da mensagem.

A solução não apresentou impacto negativo no desempenho da rede, porém não foram realizados cenários com ataques na rede para avaliar o real desempenho da solução proposta, o que prentende ser realizado em um trabalho futuro, além de computar de forma temporal o envio e a recepção das mensagens.

Referências

Clarke, N. L., Katos, V., Menesidou, S.-A., Ghita, B., and Furnell, S. (2012). A novel security architecture for a space-data dtn. In *International Conference on Wired/Wireless Internet Communications*, pages 342–349. Springer.

de Oliveira, C. T., Moreira, M. D., Rubinstein, M. G., Costa, L. H. M., and Duarte, O. C. M. (2007). Redes tolerantes a atrasos e desconexoes. *SBRC Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*.

Farrell, S., Weiss, H., Symington, S., and Lovell, P. (2011). Bundle security protocol specification. RFC 6257.

FIPS, P. (1995). 180-1. secure hash standard. *National Institute of Standards and Technology*, 17.

Jain, R. (1990). *The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling*. John Wiley & Sons.

Johnson, E., Cruickshank, H., and Sun, Z. (2012). Providing authentication in delay/disruption tolerant networking (dtn) environment. In *International Conference on Personal Satellite Services*, pages 189–196. Springer.

Keränen, A. and Ott, J. (2007). Increasing reality for dtn protocol simulations. *Helsinki University of Technology, Tech. Rep*.

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, New York, NY, USA. ICST.

Nunes, C. M., Dotti, F. L., and Oliveira, J. (2010). Aprp-group: Roteamento para redes dtn com repasse baseado em agrupamento de nodos por potencial de entrega. *XXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 451–464.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Templin, F. L. (2015). Dtn security key management. Technical report.