Mitigando ataques de atraso de pulso no protocolo BSynC

Marcos Z. de Mello, Davi D. Gemmer, Claudiomiro F. D. Junior, Rafael R. Freitas, Ricardo T. Macedo

[1]Departamento de Tecnologia da Informação
Universidade Federal de Santa Maria
Campus Frederico Westphalen

{zanonmarcos,daviddanielg,juniordias,rafaelrfreitas}@mail.ufsm.br, rmacedo@inf.ufsm.br

Abstract. *Synchronization protocols in ad hoc networks, can act in regions that does not have an infrastructure. The BSynC protocol considers features of CRAHNs and promotes synchronization among nodes efficiently and reliably. However, this protocol is prone to delayed pulse attacks that cause a slow the synchronization process. This work proposes a scheme to mitigate pulse delay attacks in the BSynC synchronization protocol. The schema consists of four steps: the first collect messages, the second checks for a communication integrity, a third establishes a reliability of the network, and the fourth performs a discarding of messages without relevance. In future works we will perform simulations to evaluate the mitigation capacity of the proposed scheme.*

1. Introdução

As redes *ad hoc* de rádio cognitivo, do inglês *cognitive radio ad hoc networks (CRAHNs),* crescem cada vez mais devido a demanda de comunicação sem fio. As *CRAHNs* têm uma arquitetura distribuída de multi-salto devido as frequentes trocas dos canais usados pelos nós. Para que o gerenciamento do espectro destas trocas de canais ocorra, é necessário que haja uma sincronização de tempo entre os nós. Neste contexto o protocolo BSynC, *(Bio-inspired time Synchronization protocol for CRAHNs)*, desempenha um papel fundamental ao proporcionar sincronização de forma descentralizada, ao alcançar uma concomitância simétrica entre os pares de nós [Pari et al. 2013]. No entanto o BSynC é propenso ao ataque de atraso de pulso, onde nós atacantes introduzem dados falsos dentro das mensagens utilizadas, gerando um aumento no tempo de convergência e sobrecarga de mensagens.

Na literatura existem diversos esforços para aprimorar a segurança dos protocolos de sincronização em CRAHNs. Em [Pari et al. 2013], foi identificado que o protocolo BSynC é vulnerável a ataques de atraso de pulso entre os nós, apesar dos seus benefícios para as CRAHNs. Em [Rasmussen et al. 2007] foi utilizada a colaboração dos nós através de mecanismos de confiança, para avaliar o grau de confiabilidade de seus vizinhos, de modo que os nós interajam com os vizinhos mais confiáveis e ignorem os menos confiáveis. Em [Peres et al. 2015] foi apresentado um método para rejeitar nós receptores de qualquer mensagem forjada pelos atacantes caso as mensagens forem diferentes do esperado. Assim, o objetivo do trabalho é estabelecer uma confiabilidade dos nós da rede através de trocas de informações, por meio de chaves assimétricas, que possibilitaria diferenciar os nós maliciosos em uma rede de topologia em malha.

2. Solução Proposta

Este trabalho apresenta um esquema para mitigar os ataques de pulsos por nós em sincronização do protocolo BSynC. Através deste esquema, as mensagens entre os nós

são coletadas para verificar a autenticidade das mensagens pela análise de chaves simétricas ou assimétricas para ignorar automaticamente as mensagens diferentes do esperado. O esquema proposto compreende quatro etapas: *Coleta, Análise, Grau de Confiabilidade e Descarte*, como demonstra a Figura 1.

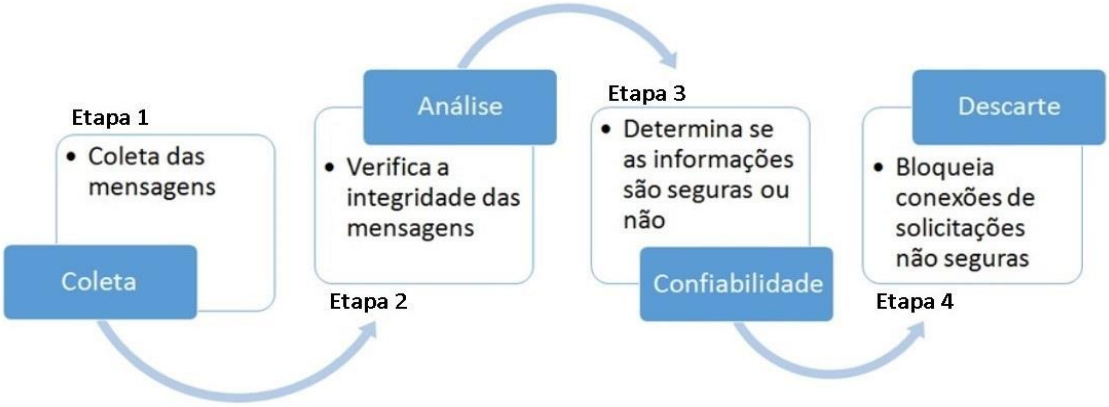

Figura 1: Esquema para mitigar ataques de atraso de pulso no protocolo BSynC.

De acordo com a Figura 1, na primeira etapa o nó em atividade coleta as mensagens que são enviadas entre os nodos da rede. A segunda etapa verifica a integridade da comunicação e sua autenticidade, através de trocas de informações por meio de chaves assimétricas entre os nós da rede, caso seja um nó malicioso o mesmo não terá resposta em sua requisição, os resultados serão guardados em arquivos estáticos nos nós. Na terceira etapa, as informações armazenadas são usadas pelo nó em período de atividade para, gerar um relatório das requisições aceitas e negadas obtendo a confiabilidade das mensagens trocadas, assim os nós trocam informações entre eles somente com as que apresentam confiança. A última etapa descarta as mensagens quais obtiveram falhas durante a verificação.

Utilizando uma topologia em malha, na qual todos os nós da rede estarão se sincronizando, um nó será o responsável pela verificação da requisição de um novo nodo por um determinado tempo, sendo assim todos os nós estarão sendo sincronizados mesmo durante uma requisição ou ataque. Como o ataque acontecera em apenas um nó a partir de que ele passe a responsabilidade de verificação para outro nó ele irá se sincronizar sem interrupções, e o atacante passa a atacar outro nó recém sincronizado.

3. Considerações finais

Este trabalho apresentou um esquema para mitigar ataques de atraso de pulso no protocolo BSynC. Em trabalhos futuros será simulada a troca de mensagens com o esquema apresentado através da implementação de um método de comparação de chaves no protocolo BSynC para verificar o impacto, de mitigação dos ataques de pulso assim como a variação de tempo para comparar as chaves da requisição.

Referências

Pari, Nadine, Aldri Santos, and Michele Nogueira (2013). "Investigando o Impacto de Ataques na Sincronização de Tempo em Redes Ad Hoc de Rádio Cognitivo. *Workshop de Redes de Acesso em Banda Larga (WRA), SBRC.*

Peres, Bruna Soares, and Olga Goussevskaia (2015). "IPv6 Multihop Host Configuration for Low-Power Wireless Networks." *In IEEE Computer Networks and Distributed Systems (SBRC), 2015 XXXIII Brazilian Symposium*.

Rasmussen, Kasper Bonne, Srdjan Capkun, and Mario Cagalj (2007). "Secnav: secure localization and time synchronization in wireless networks." *ACM international conference on Mobile computing and networking*.