Investigando o Impacto de Ataques na Sincronização de Tempo em Redes Ad Hoc de Rádio Cognitivo

Nadine Pari, Aldri Santos, Michele Nogueira

[1]Departamento de Informática
Universidade Federal do Paraná (UFPR)
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brasil

{nelpari,aldri,michele}@inf.ufpr.br

Abstract. *Time synchronization plays a key role in managing different functionalities of a cognitive radio ad hoc network (CRAHN). These networks have strong requirements and constraints related to synchronization in order to better coordinate spectrum sensing and medium access. BSynC is a protocol proposed to efficiently provide time synchronization for CRAHNs, without requiring a predefined structure. However, due to network characteristics, such as wireless communication, dynamic topology and no infrastructure of support, malicious nodes can take advantage of vulnerabilities on time synchronization protocols and wireless communication channels to disrupt the network or to save their own resources. This paper is the first to analyze the impact of two kind of easy to launch and dangerous attacks on the BSynC protocol, named lack of cooperation and pulse delay attacks. Simulation results show BSynC weaknesses mainly in face to pulse delay attack, increasing convergence time in about 15%.*

Resumo. *A sincronização de tempo desempenha um papel fundamental para as diferentes funcionalidades do gerenciamento do espectro de radiofrequência em uma rede ad hoc de rádio cognitivo (CRAHN). Essas redes possuem requisitos fortes relacionados ao sensoriamento coordenado do espectro e à necessidade do conhecimento preciso dos intervalos de tempo para acessar ao meio sem fio em vários protocolos MAC. O BSynC é um protocolo de sincronização eficaz para CRAHNs, não requerendo o suporte de uma estrutura predefinida. Contudo, devido às características do meio de comunicação sem fio e dessas redes, nós maliciosos podem se aproveitar das fragilidades de operação dos protocolos de sincronização para comprometer a rede ou poupar seus próprios recursos. Este artigo é o primeiro a analisar o impacto de dois ataques fáceis de executar e perigosos para o protocolo de sincronização BSynC, chamados de falta de cooperação e de atraso de pulso. Resultados de simulações mostram que o protocolo BSynC é vulnerável principalmente ao ataque de atraso de pulso, aumentando seu tempo de convergência em 15%.*

1. Introdução

As frequências do espectro estão atualmente atribuídas estaticamente através de licenças fornecidas por agências reguladoras, como a ANATEL (Agência Nacional de Telecomunicações) no Brasil e a FCC (*Federal Communications Commission*) nos Estados Unidos da América, sendo que cerca de 90% delas estão subutilizadas [FCC 2002].

Isto ocorre pela alta demanda de comunicações sem fio, que gera escassez em determinadas bandas [FCC 2002] e cria a necessidade de utilização mais eficiente do espectro. A tecnologia de rádio cognitivo visa tornar eficiente o uso do espectro de radiofrequência [Akyildiz et al. 2009] através de um cuidadoso sensoriamento do espectro em que os dispositivos (nós) não licenciados, chamados de usuários secundários (USs), verificam a existência de atividades dos usuários primários (UPs), titulares de licenças. Na ausência de atividades dos UPs, os USs podem usar oportunisticamente as frequências livres, também chamadas de *white spaces*. Entretanto, os USs não podem gerar qualquer modificação ou interferência no comportamento dos UPs.

Em particular, as redes *ad hoc* de rádio cognitivo, do inglês *cognitive radio ad hoc networks (CRAHNs)*, se caracterizam pela arquitetura distribuída multi-salto, a topologia de rede dinâmica devido às frequentes trocas de canais usados pelos nós e a disponibilidade do espectro sob condições variadas no tempo e no espaço [Akyildiz et al. 2009]. Os nós se comunicam entre si de uma forma multi-salto ou diretamente com os nós que estão dentro de seu raio de cobertura. No entanto, a fim de se beneficiar de todas as vantagens das CRAHNs, a sincronização de tempo desempenha um papel fundamental durante as diferentes fases do gerenciamento do espectro, tais como o sensoriamento do uso das frequências pelos UPs, a decisão sobre qual frequência e canal utilizar, o compartilhamento do espectro com outros USs e a mobilidade de frequências no espectro caso as condições deste mudem [Cormio and Chowdhury 2009]. Além da vantagem de ter um relógio preciso, a sincronização oferece vários benefícios para os protocolos de comunicação nas CRAHNs. Por exemplo, o controle de acesso ao meio pode ser projetado de uma maneira mais eficiente e simples se todos os nós estiverem sincronizados. Além disso, os esquemas de diversidade cooperativa e de seleção de canais tipicamente exigem que os nós estejam sincronizados [Zeng et al. 2010, Zivkovic and Mathar 2011, da Silva and de Rezende 2011], sendo a sincronização de tempo um auxílio na prevenção de problemas específicos da comunicação sem fio, como o *shadow fading*, que impede a cooperação entre os nós.

O protocolo de sincronização BSynC (*Bio-inspired time Synchronization protocol for CRAHNs*) é o primeiro protocolo de sincronização que considera as características das CRAHNs em seu funcionamento. Ele foi proposto com o objetivo de prover a sincronização entre os nós de uma CRAHN de forma descentralizada, eficiente e confiável [Pari et al. 2012]. O protocolo BSynC é inspirado na sincronização entre os vaga-lumes existentes em certas partes do sudeste da Ásia [Mirollo and Strogatz 1990] e alcança a sincronização simétrica entre os pares de nós através da difusão de mensagens com informação de tempo. Ele apresenta um melhor tempo de convergência de sincronização quando comparado com trabalhos correlatos [Ganeriwal et al. 2003], porém nenhuma análise sobre o impacto de ataques maliciosos foi realizada. Ataques maliciosos, como ataques de falta de cooperação e de atraso de pulso, podem comprometer o bom funcionamento do protocolo e consequentemente a sua eficácia, pois o protocolo BSynC precisa da informação correta de tempo e da cooperação dos nós para difundir as mensagens de sincronização através de toda a rede.

Este trabalho quantifica o impacto de ataques maliciosos na sincronização de tempo do protocolo BSynC a fim de direcionar pesquisas futuras que visem criar mecanismos de segurança para estas redes. A análise das vulnerabilidades e do impacto de ataques

maliciosos no protocolo BSynC é importante especialmente porque as CRAHNs herdam as vulnerabilidades das redes *ad hoc* tradicionais, como a ausência de infraestrutura e a comunicação multi-saltos [Akyildiz et al. 2009, Clancy and Goergen 2008]. Conhecer as falhas do protocolo BSynC diante dessas ameaças permite o desenvolvimento eficiente de alternativas para minimizar o impacto de tais ataques, protegendo o funcionamento do protocolo da participação de nós maliciosos. Os ataques foram simulados no Network Simulator (NS-2), aplicando um módulo de redes de rádio cognitivo. As métricas utilizadas para a análise são o tempo de convergência e a sobrecarga da rede, as mesmas utilizadas em vários trabalhos para análise do desempenho de protocolos de sincronização. Os resultados mostram uma redução no desempenho do protocolo BSynC diante dos ataques em termos de tempo de convergência e sobrecarga gerada na rede. Contudo o impacto do ataque de atraso de pulso é mais acentuado, sendo que o tempo de convergência diante desse ataque é reduzido em cerca de 15%.

O restante do artigo está organizado como segue. Na Seção 2 os trabalhos relacionados são apresentados. Na Seção 3 e 4, os fundamentos das CRAHNs e do protocolo BSynC são descritos a fim de prover um melhor entendimento dos mesmos. Na Seção 5, os procedimentos dos ataques analisados são descritos. Na Seção 6, apresentam-se o ambiente de avaliação, as métricas utilizadas e os resultados obtidos nas simulações e suas análises. Por fim, a Seção 7 conclui o artigo e direciona os trabalhos futuros.

2. Trabalhos Relacionados

Por ser um tópico de pesquisa bastante recente, verificou-se na literatura a inexistência de pesquisas focadas especificamente na segurança de protocolos de sincronização para CRAHNs. Desta forma, aumentamos o escopo da investigação dos trabalhos relacionados à área de redes *ad hoc* sem fio e redes dinâmicas, com o foco principal em aspectos de segurança dos protocolos de sincronização [Ganeriwal et al. 2008, Wang et al. 2010, Liu et al. 2010, Mehrpouyan et al. 2011]. Observou-se, por exemplo, que o ataque mais analisado nas redes de sensores sem fio (WSN) é o *ataque de atraso de pulso*, que compromete o bom desempenho dos protocolos de sincronização e interfere na precisão e no tempo de convergência [Ganeriwal et al. 2008]. Apesar de alguns autores argumentarem que esse ataque pode ser prevenido através de técnicas de criptografia, em [Hu et al. 2008] os autores alegam que, mesmo usando criptografia, o ataque de atraso de pulso pode ser gerado apenas atrasando o repasse da mensagem de sincronização por um nó intermediário malicioso. Dentre os protocolos de sincronização vulneráveis, destaca-se o TPSN (*Timing-Sync Protocol for Sensor Networks*) [Ganeriwal et al. 2003], que é o protocolo de sincronização considerado mais preciso em WSNs, e serve de referência para os dois protocolos existentes em redes de rádio cognitivo [Nieminen et al. 2009, Pari et al. 2012].

Soluções têm sido propostas para reagir contra o ataque de atraso pulso em WSNs [Rasmussen et al. 2007, Ganeriwal et al. 2008], porém nas CRAHNs este tópico ainda é um tema de pesquisa [Cormio and Chowdhury 2010]. Em [Ranganathan and Nygard 2010], apresentou-se um *survey* das abordagens de sincronização de tempo mais conhecidas e um resumo dos principais ataques nestes protocolos. Uma vez que nenhum desses protocolos foram projetados tomando aspectos de segurança como prioridade, os ataques na sincronização são facilmente lançados sem modificar o funcionamento dos protocolos.

Em [Ganeriwal et al. 2008], os autores discutem quatro tipos diferentes de ataques. Um deles é denominado de ataque de mascaramento, em que um nó usurpa a identidade de outro e difunde dados falsos nas mensagens de sincronização. No ataque de repetição, um nó atacante pode repetir os pacotes antigos de um nó legítimo, enganando os nós vizinhos e induzindo-os a sincronizar tendo como referência um tempo errado. No ataque de manipulação de mensagens, um nó atacante pode eliminar, modificar ou mesmo forjar as mensagens de tempo trocadas entre os nós a fim de interromper o processo de sincronização. No ataque de atraso de pulso, o nó atacante atrasa deliberadamente algumas das mensagens de tempo para que o processo de sincronização falhe. Estes ataques mostram a vulnerabilidade dos esquemas de sincronização existentes.

Em [Ganeriwal et al. 2008], os autores mostram que os protocolos de sincronização independentes de GPS, como o TPSN e o LTS (*Lightweight Time Synchronization for Sensor Networks*), são sujeitos a ataques de *jamming* na camada de enlace, por conta das vulnerabilidades do canal sem fio que impedem a comunicação entre os nós. Entretanto, este ataque não é exclusivo contra os protocolos de sincronização e vem sendo tratado na literatura com foco no seu impacto na comunicação de forma geral. O comportamento de nós maliciosos em MANETs tem sido tratado em diversos trabalhos [Djenouri et al. 2005]. Esses trabalhos descrevem os ataques realizados por nós não cooperativos, isto é, por nós que agem de forma egoísta, não retransmitindo mensagens dos protocolos. Conhecendo a ameaça que os ataques são para os protocolos de sincronização e para a eficiência da rede, este trabalho é o primeiro a quantificar o impacto do ataque de atraso de pulso e de falta de cooperação em um protocolo de sincronização para CRAHNs.

3. Redes *ad hoc* de rádio cognitivo

Esta seção apresenta os fundamentos das redes *ad hoc* de rádio cognitivo a fim de oferecer uma melhor compreensão das análises posteriores. Uma rede de rádio cognitivo é formada por nós, identificados por X_i neste trabalho, que possuem um dispositivo de rádio cognitivo capaz de sensoriar o espectro de radiofrequência e adaptar dinamicamente seus parâmetros de transmissão, como frequência da portadora, forma de onda de transmissão, método de acesso ao canal e potência de transmissão. O objetivo dessas redes é tornar mais eficiente a comunicação entre os nós através do uso oportunista do espectro de radiofrequência [Cormio and Chowdhury 2010]. Assim, uma rede de rádio cognitivo permite aos USs compartilharem o meio sem fio com os UPs e com outros USs. Como um RC possui a capacidade de acesso dinâmico ao espectro, ele é capaz de identificar as porções ociosas do mesmo e transmitir por um ou mais canais, garantindo que a sua transmissão não interfira em uma possível transmissão dos UPs licenciados para as bandas de frequência ociosas [Akyildiz et al. 2009].

Além das características mencionadas no parágrafo anterior, as CRAHNs possuem comunicação multi-salto e uma arquitetura distribuída dos nós. Desta forma, cada nó coordena cooperativamente o acesso aos canais livres. Os nós realizam o processo de sensoriamento do espectro individualmente e podem usar um canal comum para a troca de mensagens de controle, o qual é geralmente denominado de *canal de controle comum* ou CCC da rede. Após esta etapa, as informações sobre o uso do espectro de radiofrequência sensoriadas individualmente por cada nó são compartilhadas entre os demais nós a fim de auxiliar na execução de serviços essenciais da rede, como por exemplo, na descoberta de

rotas. Esta rede também é considerada uma rede multi-salto e multi-canal haja visto que podem selecionar um ou vários canais ociosos para comunicação. A Figura 1 ilustra uma infraestrutura de rede *ad hoc* de rádio cognitivo composta por uma estação base primária, dois usuários primários e quatro usuários secundários. Os usuários da rede primária e os nós da CRAHN podem compartilhar as mesmas bandas de frequências.

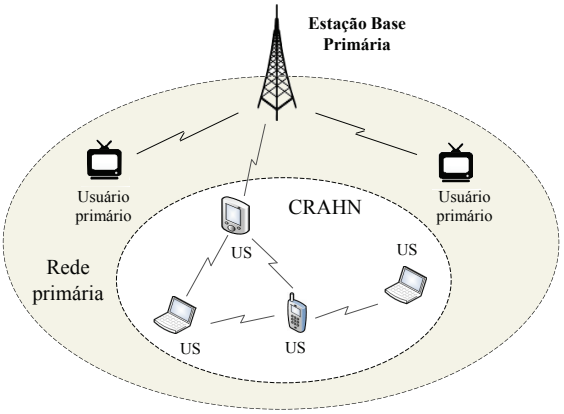

Figura 1. Rede *ad hoc* de rádio cognitivo

A sincronização de tempo nas CRAHNs tem um papel importante durante as diferentes fases da gestão do espectro dinâmico, como o sensoriamento do espectro, a decisão, o compartilhamento e a mobilidade [Cormio and Chowdhury 2009]. Além da vantagem de ter um relógio preciso, a sincronização oferece vários benefícios para os protocolos de comunicação, por exemplo, o controle de aceso ao meio pode ser projetado de maneira mais eficiente se todos os nós da rede estiverem corretamente sincronizados. Além disso, essas redes possuem requisitos fortes relacionados à necessidade do conhecimento preciso dos intervalos de tempo para acessar o meio em vários protocolos MAC.

4. Protocolo Bio-Inspirado de Sincronização de Tempo

Inspirados na perfeita sincronia dos vaga-lumes existentes em certas partes do sudeste da Ásia, o protocolo de sincronização de tempo BSynC foi projetado tendo como referência o modelo matemático descrito em [Mirollo and Strogatz 1990]. O modelo representa o comportamento da sincronização espontânea entre os vaga-lumes através de osciladores de pulso acoplado e com base nele foi provado que uma rede converge para sincronização, independente do seu número de nós e do momento de início do processo de sincronização. O modelo foi adaptado para o contexto de uma rede CRAHN. Desta forma, cada nó X_i corresponde a um vaga-lume e possui um temporizador interno t_i, além de um limiar T fixo e predefinido igualmente para todos os nós da rede. Cada nó possui ainda o seu relógio de tempo real, que pode ser ajustado positivamente ou negativamente.

O protocolo de sincronização BSynC difere de outros protocolos existentes na literatura pois não precisa estabelecer qualquer estrutura prévia, além de ser escalável. Entretanto, o protocolo ainda requer a existência de poucos nós de referência de tempo real na rede, chamados de nós mestres (NM). Estes nós estão equipados com um dispositivo que fornece o UCT *(Universal Coordinated Time)*, como o sistema de posicionamento global (GPS) ou um receptor de sinais de televisão digital. Os demais nós na rede ajustam

seus tempos em relação aos NMs. A seguir são resumidos os diferentes papéis que um nó na CRAHN pode executar no contexto do protocolo BSynC.

- **Nó mestre (NM)**: nó equipado com um dispositivo que fornece o UCT. Devido à necessidade desses nós possuírem esse equipamento auxiliar, é desejável manter baixo o número de NM na rede devido ao custo de aquisição.
- **Nó ordinário (NO)**: um nó que busca ser sincronizado. Ele não possui qualquer equipamento que forneça uma referência para o valor do tempo real universal, portanto depende da sincronização com outros nós para estimá-lo.
- **Nó ordinário de referência (NR)**: um nó ordinário selecionado por outro nó como seu nó de referência para comparar valores de relógios de tempo real e ajustar o seu relógio.

O processo de sincronização do protocolo BSynC é iniciado na rede pelos nós mestres e segue duas fases cíclicas e bem definidas: (i) a **Fase 0** - denominada de solicitação de sincronização, e (ii) a **Fase 1** - denominada de ajuste de tempo. Primeiramente, cada nó obtêm uma lista de canais livres da presença de usuário primário através das capacidades cognitivas de sensoriamento do espectro. Após obter essa lista, cada nó inicia a Fase 0, em que ele envia sua lista de canais livres para seus nós vizinhos através de um canal de controle comum (CCC) independentemente dos demais nós da rede. O nó em conjunto com cada um de seus vizinhos estabelece um canal de sincronização comum (canal livre tanto para o nó emissor como para o receptor) e estes sintonizam nesse canal para transmitir as mensagens de sincronização do protocolo. Uma vez sintonizados no mesmo canal de sincronização comum, os pares de nós iniciam a Fase 1, que determina a diferença entre os valores dos relógios de tempo real dos nós. Com base na diferença entre esses valores, os nós sincronizam seus relógios, e quando t_i atinge o valor T, a Fase 0 é reinicializada. Este processo é repetido periodicamente. Assim, após um certo número de iterações, cada nó terá o mesmo valor de tempo, convergindo na sincronização dos relógios de tempo real.

A periodicidade de cada fase do protocolo segue o modelo de sincronização dos vaga-lumes [Mirollo and Strogatz 1990]. Cada nó X_i inicia seu temporizador interno t_i em zero e este é incrementado até atingir o valor do limiar T. Quando $t_i = T$, o nó reinicializa seu temporizador t_i em 0 e emite um pulso, simulando o pisca dos vaga-lumes, e reinicia a Fase 0 do protocolo de sincronização. O pulso consiste da difusão de uma mensagem de *beacon* de requisição de sincronização aos nós vizinhos, ou seja, àqueles nós no raio de cobertura do nó X_i considerando a perspectiva do CCC da rede. Após receber uma resposta para a mensagem de *beacon* de requisição, o nó envia uma mensagem de sincronização para seu vizinho. Ao receber a mensagem de sincronização, o vizinho executa a Fase 1, em que o valor de t_i pode ser incrementado ou decrementado, acelerando ou retardando a periodicidade das ocorrências das fases do protocolo. Cada uma dessas mensagens são detalhadas a seguir.

Os nós no protocolo BSynC enviam três tipos de mensagens para seus nós vizinhos: *beacon de requisição*, *beacon de resposta* e *mensagem de sincronização*. O *beacon* de requisição contém a lista de canais livres L_i de um nó X_i, sendo representado por $b_{req}(L_i)$. O *beacon* de resposta possui o valor do canal de sincronização comum escolhido para troca de mensagens de sincronização entre quaisquer pares de nós X_i e X_j. O *beacon* de resposta é representado por $b_{res}(c_{ij})$, sendo c_{ij} o canal de sincronização co-

mum. As mensagens de sincronização são representadas por $m(X_i, t_i, Ts_i)$ e contém o identificador X_i do nó, o valor de seu temporizador interno t_i e seu *timestamp* Ts_i. Os dois primeiros tipos de mensagens são usados na Fase 0 do protocolo, enquanto o último tipo de mensagem é usado na Fase 1. As trocas de mensagens do tipo *beacon* são realizadas através do CCC e as trocas de mensagens de sincronização são realizadas pelo canal de sincronização comum escolhido pelos pares de nós. A seguir as duas fases do protocolo são descritas, tendo como base a notação apresentada na Tabela 1.

Notação	Definição
X_i e X_j	Identificadores de dois nós arbitrários na rede, sendo X_j vizinho de X_i
X_i^*	Nó mestre
A_i	Conjunto de vizinhos de X_i
L_i	Lista de canais livres de cada X_i
c_{ij}	Canal do espectro escolhido para a comunicação entre dois nós X_i e X_j
$b_{req}(L_i)$	*Beacon* contendo a lista de canais livres L_i do nó X_i
$b_{res}(c_{ij})$	*Beacon* contendo o canal para sincronização c_{ij} entre X_i e X_j
t_i	Temporizador interno de X_i
T	Limite definido igualmente em todos os nós para um ciclo de sincronização
Ts_i	*Timestamp* de X_i
$m(X_i, t_i, Ts_i)$	Mensagem de sincronização contendo o identificador X_i do nó e t_i
M	Conjunto de nós atacantes

Tabela 1. Notação

Fase 0 - Solicitação de Sincronização

O processo de solicitação de sincronização é descrito através do **Procedimento 1** e é realizado por cada nó na rede. Cada NM, X_i^*, inicializa t_i em 0 e é incrementado com a mesma periodicidade do seu relógio de tempo real. Uma vez que t_i atinge o valor T, os X_i^* difundem uma mensagem $b_{req}(L_i)$ para os nós em A_i $(l.\ 2)$ e reinicializam o valor de t_i em 0. Cada vizinho X_j que recebe o $b_{req}(L_i)$ responde com um $b_{res}(c_{ij})$ contendo o canal de sincronização escolhido $(l.\ 3)$. Depois de definir um canal de sincronização, X_i^* e X_j sintonizam neste canal $(l.\ 4)$, e X_i^* envia uma mensagem $m(X_i, t_i, Ts_i)$ $(l.\ 5)$. Todos os nós de A_i que recebem essa mensagem estabelecem X_i^* como seu nó de referência $(l.\ 8)$. Em seguida, X_j executa o procedimento de ajuste de tempo explicado adiante $(l.\ 9)$. Após estes passos, o nó X_j transmite um *beacon* $b_{req}(L_j)$ aos nós em A_j $(l.\ 10)$, os quais o definem como NR seguindo esses mesmos passos.

Fase 1 - Ajuste de Tempo

A Fase 1, detalhada no **Procedimento 2**, inicia quando um nó X_j recebe uma mensagem $m(X_i, t_i, Ts_i)$ de um nó X_i. Nessa mensagem, o X_j obtém o *timestamp* de X_i *(l.2)* e compara com o valor de seu relógio *(l.3)*. Se Ts_j é maior que Ts_i, então X_j decrementa o valor de seu relógio *(l.5)* e se Ts_j é menor que Ts_i, X_j incrementa o valor de seu relógio. X_j recebe também o valor do temporizador interno de X_i, t_i. Para esse valor, X_j também compara o valor de t_i com o valor do seu próprio temporizador interno t_j. Caso o valor de t_i e t_j sejam diferentes, a Equação 1 é aplicada para definir t'_j, que é o novo valor de t_j.

$$t'_j = f^{-1}(f(t_j) + \epsilon) \tag{1}$$

A Figura 2 ilustra o funcionamento do protocolo BSynC. No início, os nós mestres (1 e

Procedimento 1 SOLICITAÇÃO DE SINCRONIZAÇÃO

Repetir a cada T

para cada X_i^* na rede **faça**
  Difunde o $b_{req}(L_i)$ a nós em A_i
  Negocia um canal com nós em A_i com o $b_{res}(c_{ij})$
  Sintoniza seu rádio no canal de sincronização cij
  Envia uma mensagem $m(X_i, t_i, Ts_i)$ aos nós em A_i
fim para
para cada vizinho de X_i^*, i.e., cada X_j em A_i **faça**
  Estabelece X_i^* como seu NR
  Realiza o procedimento de ajuste de tempo entre X_i e X_j
  Difunde uma mensagem $b_{req}(L_j)$ aos nós em A_j
fim para

Procedimento 2 AJUSTE DE TEMPO

X_j ***ao receber uma*** $m(X_i, t_i, Ts_i)$ ***de*** X_i

para cada $X_j \in A_i$ **faça**
  Recebe o valor de Ts_i
  Calcula a diferença dos valores dos relógios Ts_i e Ts_j
  se $Ts_j > Ts_i$ **então**
    Decrementar o tempo Ts_j pela diferença dos valores dos relógios
  senão
    Incrementar o tempo Ts_j pela diferença dos valores dos relógios
  fim se
  Recebe o valor de t_i
  se $t_j \neq t_i$ **então**
    Ajuste o valor de t_j usando a Equação 1
  fim se
fim para

7) iniciam a Fase 0 enviando para seus vizinhos um *beacon* $b_{req}(L_i)$ contendo sua lista de canais livres. Um exemplo de envio dessa mensagem é ilustrado na Figura 3, em que o nó emissor envia um *beacon* contendo seus canais livres 2, 4, e 5 ($b_{req}(2, 4, 5)$), para um nó receptor vizinho. O nó receptor responde enviando o canal 5 ($b_{res}(5)$) que é o canal livre e comum a ambos os nós. Na Figura 2, após definir o canal de sincronização, os nós 2, 3 e 5 estabelecem como nós de referência os nós origem da mensagem que receberam $b_{req}(L_i)$ (nó 1 e 7). Os nós 1, 3, 7 e 5 mudam para o canal de sincronização escolhido e começam a Fase 1. O nó 2, após realizar a Fase 1 com o nó 1, receberá outra mensagem de *beacon*

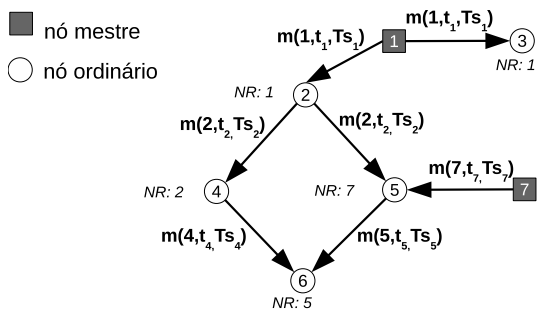

Figura 2. Funcionamento do protocolo BSynC

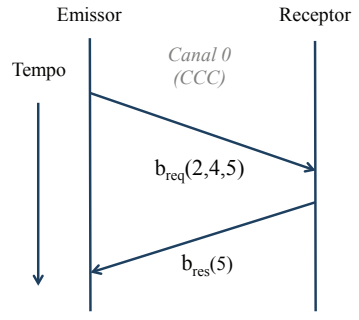

Figura 3. Negociação do canal de sincronização

do nó 5. Nesse caso, para evitar adiantar ou retroceder seu relógio incorretamente, o nó 2 faz uma consulta para seu nó de referência (nó 1), que responde enviando seu tempo, e realiza a comparação com o tempo do nó 5. Segundo esta comparação, o nó 2 incrementa ou diminui seu relógio. Este mesmo processo é realizado por todos os demais nós.

5. Ataques

Nas CRAHNs, o espectro licenciado utilizado pelos USs pode ser facilmente comprometido por um ou vários atacantes. Os ataques consistem na injeção de dados falsos no momento da troca de informação de sincronização, aproveitando o espectro de forma egoísta. Estas ações tendem a aumentar o tempo de convergência e a sobrecarga da rede. Sem uma segurança apropriada, o desempenho da rede pode ser fortemente comprometido, pois ocorrerão atrasos ou interferências na transmissão de dados e a modificação da informação transmitida entre os nós, podendo resultar em interferências com o UP, o que se deseja evitar devido às limitações da tecnologia de rádio cognitivo. Além disso, os protocolos de sincronização de tempo podem ser afetados por ataques de falta de cooperação [Kong et al. 2005]. A nossa intenção nesse artigo é analisar o impacto desses dois ataques sobre o desempenho do protocolo BSynC. As subseções seguintes detalham o comportamento desses ataques.

5.1. Ataque de falta de cooperação

No ataque de falta de cooperação, os nós podem agir de forma egoísta, se recusando a retransmitir as mensagens do protocolo de sincronização. Na Figura 4, os nós 6 e 8 são os nós não cooperativos e não retransmitem as mensagens de sincronização. Isso pode gerar um aumento no tempo necessário para todos os nós da rede sincronizarem (tempo de convergência). Esse tipo de ataque é facilmente realizado em uma CRAHN, haja visto que o *hardware* utilizado pelos dispositivos da rede geralmente são reprogramáveis e abertos a alterações pelo usuário. Quando os nós não cooperativos recebem uma mensagem de sincronização de qualquer nó vizinho, eles não a retransmitem e a descartam.

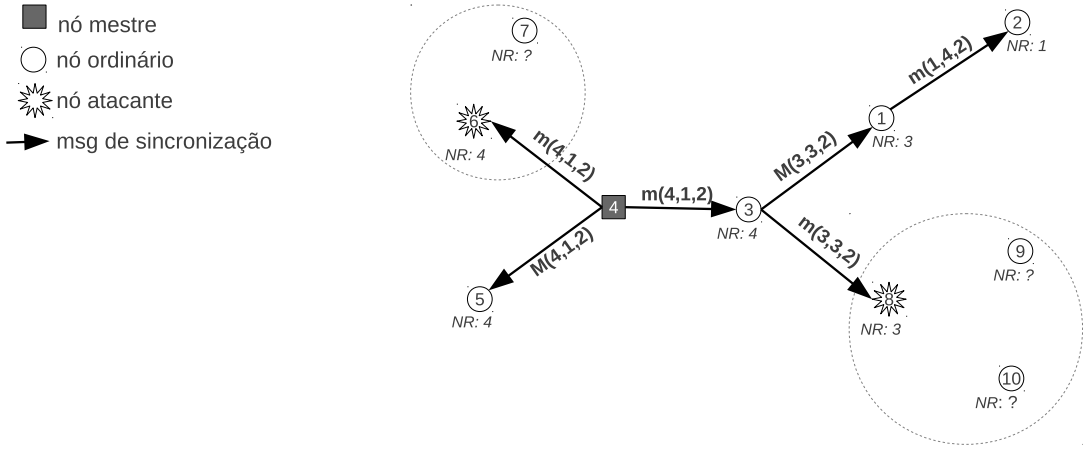

Figura 4. Ataque de falta de cooperação

5.2. Ataques de atraso de pulso

O ataque de atraso de pulso (*pulse delay attack*) injeta dados falsos dentro das mensagens utilizadas no protocolo de sincronização, com o objetivo de variar a informação de tempo

e assim aumentar o tempo de convergência. A Figura 5 apresenta o ataque de atraso de pulso, em que o nó X_i envia uma mensagem com informação de seu tempo (t_i) para o nó X_j. O nó X_m, que é um nó atacante, intercepta a mensagem e altera a informação, adicionando um tempo δ ao temporizador interno t_i e ao *timestamp* Ts_i, e envia para o nó X_j. Desta forma, o nó X_j recebe uma informação falsa. Isto pode gerar aumento no tempo de convergência e sobrecarga de mensagens, visto que será necessário mais tempo para sincronizar e portanto mais mensagens de sincronização serão trocadas.

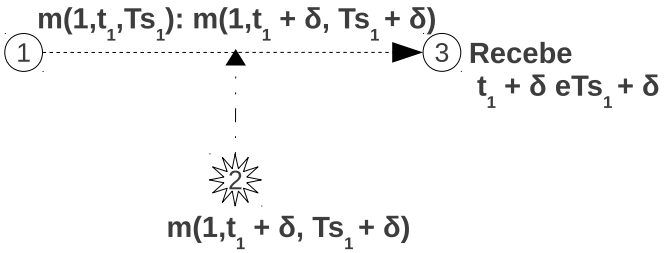

Figura 5. Ataque de atraso de pulso

Neste ataque, o nó malicioso altera a informação enviada entre dois nós legítimos e calcula um atraso aleatório, segundo uma distribuição gaussiana. Posteriormente, ele modifica a mensagem original e substitui o atraso calculado pelo tempo enviado pelo emissor e retransmite a mensagem alterada para o verdadeiro receptor.

6. Avaliação

O impacto dos ataques de falta de cooperação e de atraso de pulso é avaliado no protocolo de sincronização BSynC através de simulações. As subseções seguintes detalham o ambiente de teste, as métricas de avaliação e os resultados alcançados.

6.1. Ambiente de simulação

O protocolo BSynC foi implementado na ferramenta de simulação de rede NS-2.31. A simulação da CRAHN tem como base as mesmas características e parâmetros estabelecidos em [Akyildiz et al. 2009]. Cada nó da rede está equipado com três interfaces seguindo o padrão IEEE 802.11a, que são (i) uma interface de controle, usada para transmitir pacotes de controle e mensagens de *broadcast* aos vizinhos; (ii) uma interface de recepção, utilizada para sensoriar os canais do espectro; e (iii) uma interface comutável que permite fazer a troca de canal (*handoff*). Essa abordagem aplicada para a definição do papel de cada interface segue o modelo apresentado em [Censor-Hillel et al. 2011]. Na simulação, o número de canais possíveis de serem utilizados é de 10, o qual é um valor fixo para todas as simulações feitas. Os UPs utilizam canais predefinidos, seguindo uma distribuição de Bernoulli para definir os tempos de uso dos canais. A presença de um usuário primário na rede força a troca de canais pelos usuários secundários, caso os mesmos estejam utilizando canais prioritários para aquele usuário primário.

Foram simulados cenários com 20, 80 e 120 nós (incluindo nós atacantes) dispostos em uma região retangular de $1000m$ x $1000m$ seguindo uma distribuição gaussiana. Cada cenário foi simulado 30 vezes. O modelo de mobilidade utilizado é o *random waypoint*, em que cada nó é posicionado aleatoriamente na grade e se move com uma velocidade aleatória, sendo a velocidade máxima de 10 m/s. Esse cenário pode representar o

uso de microfones sem fio, habilitados com equipamentos de rádio cognitivo, utilizados por narradores em eventos esportivos, palestrantes em universidades, ou shows artísticos. Nesses cenários, é necessária a mobilidade dos usuários, assim como garantir que atacantes não atrapalhem a transmissão sem fio. Para alterar os níveis de mobilidade dos nós, o tempo de pausa entre os lugares de destino é variado de 0 a 10 segundos. Um menor tempo de pausa significa maior mobilidade. Os valores dos demais parâmetros de simulação são detalhados na Tabela 2. Estes parâmetros são definidos seguindo as simulações realizadas em [Pari et al. 2012]. O tempo de cada simulação é de 2000 segundos. A quantidade de nós atacantes representam 10%, 30% e 50% dos nós para cada cenário, tanto para os ataques de falta de cooperação quanto para os ataques de atraso de pulso.

Parâmetro	**Valores**
Tipo de canal	WirelessChannel
Modelo de rádio de propagação	TwoRayGround
Tipo de camada MAC	IEEE 802.11
Interface de rede	WirelessPhy
Comprimento da fila de recepção	500
Modelo de antena	OmniAntenna
Protocolo de roteamento	AODV
Número de usuários secundários	20, 50, 120
Número de usuários primários	2
Número de canais	10
Número de nós atacantes	10%, 30% e 50%
Constante ϵ na Equação 1	0.5

Tabela 2. Valores dos parâmetros de simulação

6.2. Métricas

Duas métricas foram utilizadas para avaliar o desempenho do protocolo BSynC diante de ataques: o *tempo de convergência* e a *sobrecarga na rede*. Estas métricas foram escolhidas uma vez que ajudam a determinar quanto tempo se incrementou para sincronizar a rede e quanto tráfego ocasionou devido aos nós atacantes. As métricas são detalhadas a seguir:

- **Tempo de convergência (T_c):** é a quantidade de tempo que leva para todos os nós estarem sincronizados, alcançando o chamado *estado de convergência*. Este é um dos principais indicadores de desempenho para protocolos de sincronização. O objetivo é quantificar o incremento de tempo diante dos ataques.
- **Sobrecarga na rede (S_r):** representa o tráfego (em unidade de mensagens de controle) produzido devido ao mecanismo de sincronização em proporção ao tráfego de dados total.

6.3. Resultados

Essa seção apresenta os resultados obtidos pela simulação do BSynC diante de ataques de falta de cooperação e de atraso de pulso. Os resultados são apresentados em pontos percentuais.

Ataques de falta de cooperação

A Figura 6 apresenta o resultado das simulações do protocolo BSynC com a presença de nós que não cooperam na retransmissão de mensagens de sincronização. Na presença

desses nós o tempo de convergência não variou de forma extrema e se mantém quase constante, quando comparado ao funcionamento do protocolo sem a presença de nós atacantes. Isto ocorre por conta da dinamicidade da estrutura considerada pelo BSynC, ao contrário do que ocorre com trabalhos correlatos em que a não cooperação de um nó na hierarquia desestabiliza todos os outros abaixo dele [Ganeriwal et al. 2003]. No BSynC os nós não colaborativos, e se um nó falha ou não retransmite mensagens, podem existir outros nós no mesmo raio de cobertura que enviam para ele a mesma mensagem.

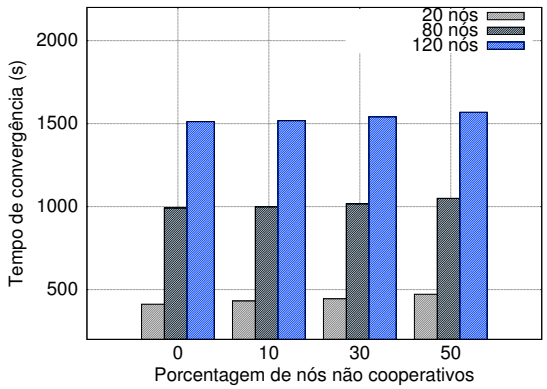

Figura 6. T_c com nós egoístas

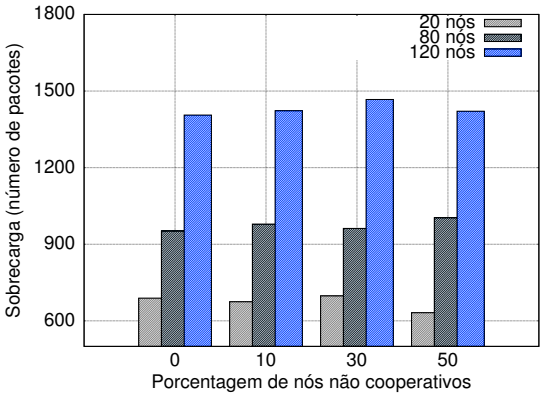

Figura 7. S_r com nós egoístas

A sobrecarga de mensagens está relacionada com o tempo de convergência. Uma vez que o tempo de convergência aumenta, a sobrecarga de mensagens do protocolo também cresce. A Figura 7 mostra o impacto do ataque de nós não cooperativos na sobrecarga de mensagens do protocolo BSynC. Comparado à sobrecarga apresentada quando não há a presença de atacantes na rede, a sobrecarga de mensagens aumenta, embora não consideravelmente. Esse pequeno aumento é consequência do aumento do tempo necessário para sincronizar todos os nós.

Ataques de atraso de pulso

O ataque de atraso de pulso é o que mais impacta no desempenho do BSynC, quando compara-se aos resultados do impacto dos ataques de falta de cooperação. Isto ocorre porque para sincronizar a rede, o BSynC precisa da informação correta da leitura dos relógios dos nós, para saber o quanto incrementar ou diminuir. No caso de um nó atacante que altera esta informação através do atraso de pulso, o desempenho do protocolo se vê drasticamente comprometido, com um incremento de 15% no total de tempo necessário para convergência na rede. A Figura 8 apresenta os resultados para esse ataque. Como pode-se prever, conforme aumenta o número de atacantes na rede, o impacto é ainda maior.

A Figura 9 ilustra os resultados do impacto dos ataques de atraso de pulso. Observa-se que a sobrecarga da rede aumenta de forma diretamente proporcional com o tempo de convergência. Isto é ocasionado porque os ataques forçam um maior tempo de convergência na rede, e consequentemente é preciso mais mensagens para obter a sincronização. Além disso, os procedimentos de sincronização deverão ocorrer com maior frequência.

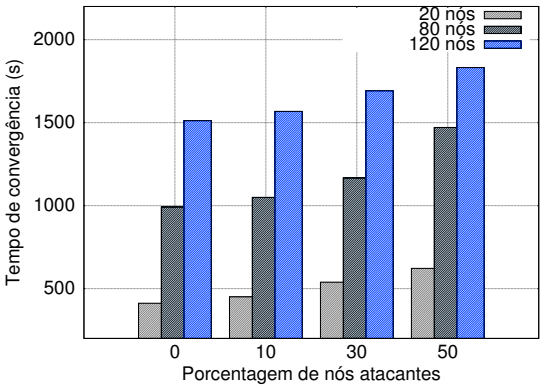

Figura 8. T_c com atraso de pulso

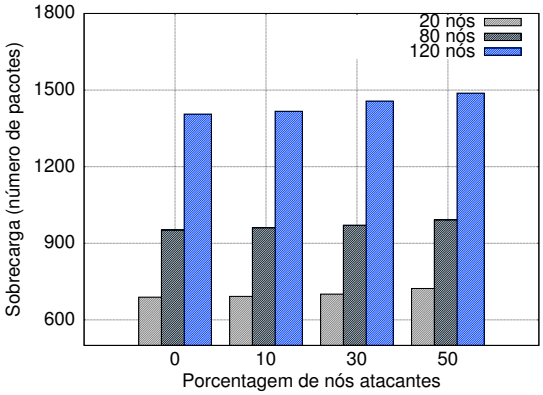

Figura 9. S_r com atraso de pulso

7. Conclusões e trabalhos futuros

Este trabalho analisou o impacto de ataques maliciosos no desempenho do protocolo BSynC, um protocolo de sincronização bio-inspirado para CRAHNs. Os ataques analisados foram o ataque de atraso de pulso e o ataque de nós não cooperativos, que são os ataques que mais afetam o desempenho de protocolos de sincronização em redes *ad hoc* sem fio. Os resultados das simulações mostram que o protocolo BSynC é suscetível a estes ataques, principalmente ao ataque de atraso de pulso. Os cenários diante do ataque de atraso de pulso mostraram que quanto maior é o número de nós atacantes, maior é o tempo de convergência. Isto deve-se à dependência do protocolo BSynC na troca de informação correta do tempo entre os nós para ter um bom desempenho.

O ataque de nós não cooperativos teve um leve impacto no BSynC, sendo que o tempo de convergência se mantém quase constante. Isto ocorre por conta da dinamicidade da estrutura considerada pelo BSynC, uma vez que se um nó falha ou não retransmite mensagens, podem existir outros nós no mesmo raio de cobertura que enviem para ele a mesma mensagem. Contudo, este cenário depende da distribuição dos nós dentro da rede. Em relação à sobrecarga da rede se observa que não tem um grande impacto pois os nós atacantes não cooperam retransmitindo as mensagens de sincronização. Como trabalho futuro pretende-se propor um módulo de segurança em que o BSynC, além de conseguir um bom tempo de convergência, não seja afetado com a presença desses ataques na rede.

8. Agradecimentos

Este trabalho foi desenvolvido com suporte financeiro do programa REUNI. Gostaríamos de agradecer ainda o esforço e auxílio de Elisa Mannes.

Referências

Akyildiz, I. F., Lee, W.-Y., and Chowdhury, K. R. (2009). CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Networks*, 7(5):810 – 836.

Censor-Hillel, K., Gilbert, S., Kuhn, F., Lynch, N. A., and Newport, C. C. (2011). Structuring unreliable radio networks. In *ACM SIGACT-SIGOPS*, PODC '11, pages 79–88.

Clancy, T. and Goergen, N. (2008). Security in cognitive radio networks: Threats and mitigation. In *Intern. Conf. on Cognitive Radio Oriented Wireless Networks and Communications*, pages 1 –8.

Cormio, C. and Chowdhury, K. R. (2009). A survey on MAC protocols for cognitive radio networks. *Ad Hoc Networks*, 7:1315–1329.

Cormio, C. and Chowdhury, K. R. (2010). Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping. *Ad Hoc Networks*, 8(4):430–438.

da Silva, M. W. R. and de Rezende, J. F. (2011). Seleção dinâmica de canais de controle em rádios cognitivos utilizando reinforcement learning. In *XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, volume 4, pages 61–74.

Djenouri, D., Khelladi, L., and Badache, N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys and Tutorials*, 7(1-4):2–28.

FCC, F. C. C. R. (2002). Report of the spectrum efficiency working group. http://transition.fcc.gov/sptf/files/SEWGFinalReport_1.pdf. Último acesso: 05 de Abril 2013.

Ganeriwal, S., Kumar, R., and Srivastava, M. B. (2003). Timing-sync protocol for sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems (SenSys)*, pages 138–149, New York, NY, USA. ACM.

Ganeriwal, S., Pöpper, C., Čapkun, S., and Srivastava, M. B. (2008). Secure time synchronization in sensor networks. *ACM Transactions on Information and System Security*, 11(4):23:1–23:35.

Hu, X., Park, T., and Shin, K. (2008). Attack-tolerant time-synchronization in wireless sensor networks. In *IEEE INFOCOM*, pages 41 –45.

Kong, J., Ji, Z., Wang, W., Gerla, M., Bagrodia, R., and Bhargava, B. (2005). Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks. In *ACM WiSe*, pages 87–96, New York. ACM.

Liu, J., Zhou, R. Z., Zheng, J. P., and Cui, J.-H. (2010). Mobi-sync: Efficient time synchronization for mobile underwater sensor networks. In *IEEE GLOBECOM*, pages 1–5. IEEE.

Mehrpouyan, H., Blostein, S. D., and Svensson, T. (2011). A new distributed approach for achieving clock synchronization in heterogeneous networks. In *IEEE GLOBECOM*, pages 1–5. IEEE.

Mirollo, R. E. and Strogatz, S. H. (1990). Synchronization of pulse-coupled biological oscillators. *SIAM Journal on Applied Mathematics*, 50:1645–1662.

Nieminen, J., Jäntti, R., and Qian, L. (2009). Time synchronization of cognitive radio networks. In *IEEE GLOBECOM*, pages 1223–1228, Piscataway, NJ, USA. IEEE Press.

Pari, N., Nogueira, M., and Aravind, K. (2012). A simple, bio-inspired time synchronization protocol for cognitive radio ad hoc networks. *Intern. Symp. on Wireless Personal Multimedia Comm. (WPMC)*.

Ranganathan, P. and Nygard, K. (2010). Time synchronization in wireless sensor networks: a survey. *International Journal of UbiComp (IJU)*, 1(2):92–102.

Rasmussen, K. B., Capkun, S., and Cagalj, M. (2007). SecNav: secure broadcast localization and time synchronization in wireless networks. In *ACM MobiCom*, pages 310–313. ACM.

Wang, Y.-W., Wang, H. O., Xiao, J.-W., and Guan, Z.-H. (2010). Synchronization of complex dynamical networks under recoverable attacks. *Automatica*, 46(1):197–203.

Zeng, Y., Liang, Y.-C., Hoang, A., and Zhang, R. (2010). A review on spectrum sensing for cognitive radio: Challenges and solutions. *EURASIP Journal on Advances in Signal Processing*, 2010(1):381465.

Zivkovic, M. and Mathar, R. (2011). Performance evaluation of timing synchronization in OFDM-based cognitive radio systems. In *IEEE Vehicular Technology Conference Fall (VTC-Fall) 2011*, pages 1–5, San Francisco, USA.