PTP Flood: ataque cibernético de DoS em cliente PTP

Diego W. M. Piffaretti[1], Gabriela Moutinho de Souza Dias[1], Anderson F. Pereira dos Santos[12]

[1]Programa de Pós-Graduação em Sistemas e Computação do Instituto Militar de Engenharia (IME)
Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, CEP: 22290-270

[2]Venturus Centro de Inovação Tecnologica
Campinas, SP – Brasil

{martins.diego,gabriela,anderson} @ime.eb.br

Abstract. *This article investigates the vulnerability of the Precision Time Protocol (PTP) to replay attacks, even with the TLV feature enabled, resulting in a denial of service, an attack we refer to as "PTP flood". The attack overloads the target device with the continuous retransmission of packets, rendering it unable to process legitimate requests. The article also presents an analysis of the behavior of memory consumption during the attack and emphasizes the identification and prevention of these attacks to ensure the integrity and availability of network systems.*

Resumo. *Este artigo investiga a vulnerabilidade do Precision Time Protocol (PTP) a ataques de replay, mesmo com o recurso TLV habilitado, resultando em uma negação de serviço, um ataque que chamamos de "PTP flood". O ataque sobrecarrega o dispositivo alvo com a retransmissão contínua de pacotes, tornando-o incapaz de processar solicitações legítimas. O artigo também traz uma análise do comportamento do consumo de memória durante o ataque e ressalta a identificação e a prevenção desses ataques para garantir a integridade e a disponibilidade dos sistemas de rede.*

1. Introdução

O interesse em cibersegurança tem crescido devido ao aumento de ataques cibernéticos. Infraestruturas críticas, como comunicações e energia, são vitais para a segurança nacional e o desenvolvimento econômico [Tidy 2022]. No Brasil, após ataques em São Paulo em 2006 [GOV.BR 2023], o governo identificou infraestruturas essenciais para proteção. Em 2018, foi aprovada a Política Nacional de Segurança de Infraestruturas Críticas.

Com a necessidade de precisão temporal crescente, protocolos de comunicação evoluíram para tempos de resposta mais rápidos, passando de milissegundos para microssegundos [Loveless, Jacob and Stoikov, Sasha and Waeber, Rolf 2013]. Devido à evolução das infraestruturas críticas, a indústria está migrando do *Network Time Protocol* (NTP) [Jahan 2023] para o *Precision Time Protocol* (PTP).

O PTP é usado para sincronização de relógios altamente precisa em telecomunicações, automação industrial e sistemas financeiros [Howard 2023]. O IEEE criou o padrão 1588–2019 para sincronização de relógios em redes [1588-2019 2020], organizando nós PTP em uma hierarquia mestre-cliente, na qual o *grandmaster* (relógio central) coordena o tempo em toda a rede PTP. A versão mais recente do PTP inclui melhorias de segurança, como o TLV (*Type Length Value*) para proteger a integridade das mensagens PTP.

Considerando a relevância do PTP na operação de infraestruturas críticas e na cibersegurança, é importante investigar possíveis vulnerabilidades na versão mais recente do PTP. Este trabalho utiliza técnicas de inundação de pacotes (*flood*) para sobrecarregar um cliente PTP até que ele fique indisponível, mesmo com o TLV habilitado. O cliente PTP, ao atingir 100% de uso de memória RAM, entra em modo passivo, não sincronizando ativamente com um mestre. Como principal objetivo, está o de investigar vulnerabilidades na versão mais recente do PTP, demonstrando a eficácia do ataque de inundação de pacotes em um cliente PTP, tendo como desafio atingir 100% de uso de memória RAM, e fazer com que o cliente entre em modo passivo, mesmo com o recurso de TLV habilitado, uma condição ainda não documentada na literatura existente.

O restante deste artigo está estruturado da seguinte forma: os principais trabalhos relacionados na Seção 2, a descrição dos experimentos na Seção 3, e a respectiva análise dos resultados na Seção 4 e, por fim, a conclusão na Seção 5.

2. Trabalhos Relacionados

Analisando os resultados obtidos na revisão da literatura, verificou-se que há registros de diversas pesquisas que focam no protocolo PTP e sua segurança. A Tabela 1 lista os principais trabalhos (a partir de 2020) e os ataques correspondentes, além de comparar as versões do PTP exploradas.

Como destaque, o artigo [Fotouhi et al. 2023] aborda a importância da segurança em redes que utilizam o PTP, além de realizar ataques de *replay*, sendo um dos artigos que possuem os testes mais próximos a este trabalho. Apesar de utilizar ataques de replay, o autor não utilizou o recurso de TLV. Este presente trabalho utiliza ataques de replay com TLV habilitado, algo ainda não observado na literatura.

Ataques de replay ocorrem quando pacotes válidos são interceptados e retransmitidos. Ataques de Negação de Serviço (DoS) interrompem serviços sobrecarregando o alvo com o tráfego [Mizrahi 2014].

O artigo [DeCusatis et al. 2020] também inspirou este trabalho, abordando ataques de replay e DoS, mas sem TLV habilitado. O estudo investiga como ciberataques afetam a sincronização do PTP e identifica riscos de segurança.

O trabalho [Berardi et al. 2023] mostra que atacantes podem usar TLVs para manipular a sincronização de tempo, causando interrupções. O trabalho [Rezabek et al. 2023] implementou ferramentas para medir o desempenho do PTP com extensões de segurança, sem impacto significativo na precisão. O trabalho [Alghamdi and Schukat 2022] propõe um nó supervisor confiável (TSN) para melhorar a segurança do PTP. Os autores em [Moradi and Jahangir 2021] sugerem um algoritmo para detectar ataques de atraso em redes PTP usando métodos estatísticos. Em [Alghamdi and Schukat 2021] explora estratégias de ataque e locais potenciais, mostrando que as extensões de segurança do PTP são parcialmente eficazes. O trabalho [Alghamdi 2021] analisa ameaças persistentes avançadas (APT) à infraestrutura PTP e propõe um nó supervisor confiável para detectar padrões anormais e localizar invasores. O trabalho [Moussa et al. 2020] propõe uma extensão ao IEEE 1588 com uma "Mensagem de Segurança" para detectar ataques cibernéticos. O trabalho [Alghamdi and Schukat 2020a] analisou ataques como Man-in-the-Middle, atraso e mo-

Tabela 1. Trabalhos relacionados, ataques e versão do PTP

	Ataques			Versão do PTP	
Artigo	DoS	Replay	Outros	PTP v2.0 (IEEE-2018)	PTP v2.1 (IEEE-2019)
Fotouhi [Fotouhi et al. 2023]	X	X	X		X
Berardi [Berardi et al. 2023]	X		X		X
Rezabek [Rezabek et al. 2023]		X	X		X
Alghamdi [Alghamdi and Schukat 2022]	X	X	X		X
Moradi [Moradi and Jahangir 2021]			X	X	
Alghamdi [Alghamdi and Schukat 2021]		X			X
Alghamdi [Alghamdi 2021]	X	X	X		X
Moussa [Moussa et al. 2020]			X	X	
Alghamdi [Alghamdi and Schukat 2020a]			X	X	
DeCusatis [DeCusatis et al. 2020]	X			X	
Alghamdi [Alghamdi and Schukat 2020c]	X	X	X		X
Alghamdi [Alghamdi and Schukat 2020b]		X	X		X
Alghamdi [Alghamd and Schukat 2020]		X	X		X
Itkin [Itkin and Wool 2020]			X	X	

dificação de pacotes. O trabalho [Alghamdi and Schukat 2020c] também discutiu vulnerabilidades a ataques de atraso assimétrico e bizantinos, mostrando seu impacto na sincronização. O trabalho [Alghamdi and Schukat 2020b] propôs dispositivos programáveis para executar vários ataques. O trabalho [Alghamd and Schukat 2020] apresentou um modelo de detecção para identificar ataques ao PTP. Por fim, o trabalho [Itkin and Wool 2020] destacou as propriedades de segurança necessárias para qualquer extensão de segurança no PTP.

3. Experimentos

Para a realização dos experimentos, foi primeiramente realizado a preparação do ambiente e, posteriormente, a geração das amostras.

3.1. Preparação do ambiente

O ambiente de testes foi construído com máquinas virtuais, utilizando emuladores para os dispositivos PTP mestre e cliente. Um relógio mestre foi emulado na máquina virtual atacante (Kali Linux) com o software *mpsrc* versão 2.2.4 [Meinberg a]. O TLV foi habilitado para descartar mensagens fora do padrão. O cliente foi emulado com o software PTP Track Hound [Meinberg b], configurado com 1 GB de RAM para refletir melhor a realidade dos dispositivos clientes em uma rede PTP. Para os experimentos, foi desenhada uma arquitetura simplificada que reflete a realidade em uma rede verdadeira, conforme mostrado na Figura 1.

Após iniciar a captura de dados, foi gravado 1 minuto de tráfego legítimo PTP entre mestre e cliente, salvo como *alpha*.pcap, com o menor intervalo de mensagens possível (-7, 128/s). Em seguida, para haver uma amostra com uma gravação maior de tempo, foi gravado 3 minutos de tráfego legítimo, salvo como *beta*.pcap, com as mesmas configurações, mas maior duração e mais pacotes transmitidos. Com as amostras coletadas, é possível aplicar a técnica de ataque de *Replay* (repetição). Para isso, foi utilizado o software *tcprelay*. As amostras estão disponíveis no repositório do *github* [1].

[1] `https://github.com/piffaretti/ptp_repository`

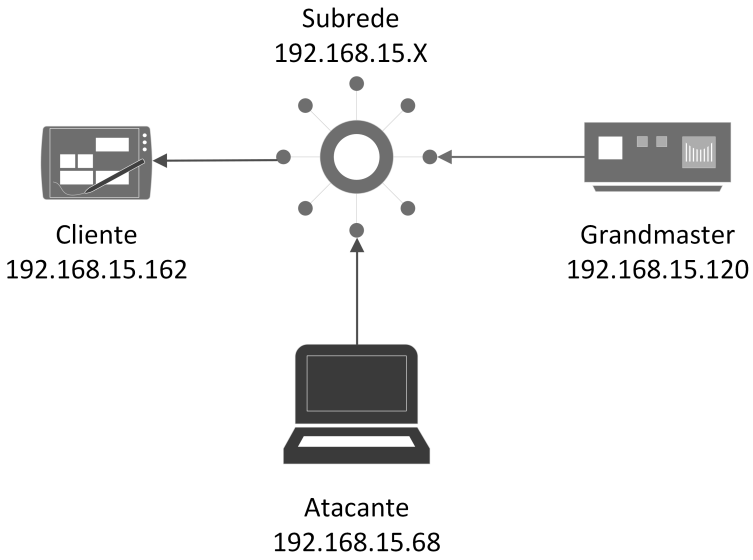

Figura 1. Arquitetura simplificada do ambiente de testes

3.2. Resultados preliminares

A Tabela 2 apresenta a quantidade de memória RAM em megabyte (MB) e a porcentagem consumida ao longo do tempo. É possível notar que no minuto 16 de execução da amostra *alpha*, foi consumido 1024 MB, ou seja, 100% da memória RAM disponível no cliente, fazendo com que o mesmo não conseguisse mais processar nenhuma requisição. A amostra *alpha* atingiu 100% aos 15 minutos e 46 segundos de execução.

A amostra *alpha* foi transmitida originalmente com uma média de 255,1 pps (pacotes por segundo). Ao utilizar a técnica de *Replay* em alta velocidade, a amostra *alpha* foi retransmitida com média de 3743,57 pps, ou seja, o ataque de replay conseguiu repassar, aproximadamente, 15 vezes mais pacotes por segundo do que no tráfego original.

É possível notar que no minuto 18 de execução da amostra *beta*, foi consumido 1024 MB, ou seja, 100% da memória RAM disponível no cliente. A amostra *beta* atingiu 100% aos 17 minutos e 36 segundos de execução.

4. Análise dos resultados preliminares

Conforme demonstrado na seção anterior, tanto na amostra *alpha* quanto na *beta*, o ataque de negação de serviço ocorreu com sucesso, ocupando 100% de memória RAM do cliente PTP. Em ambos os experimentos, foi observado que o consumo de memória ao longo do tempo apresentou um comportamento bem próximo ao linear. A partir dos dados que constam na Tabela 2, foi realizada uma regressão linear, com o objetivo de analisar o comportamento do consumo de memória RAM e fornecer uma visão quantitativa do impacto dos ataques de negação de serviço no consumo de memória RAM ao longo do tempo, a qual pode ser observada na Figura 2.

As amostras *alpha* e *beta* apresentaram as seguintes equações da regressão linear:

- Amostra *alpha*: $\hat{y} = 61.66176X + 78.125$
- Amostra *beta*: $\hat{y} = 57.41176X + 12.03268$

Tabela 2. Consumo de memória RAM das amostras *alpha* e *beta*

	Amostra *alpha*		Amostra *beta*	
Minuto	MB	porcentagem	MB	porcentagem
1	99	9,7%	70	6,8%
2	181	17,7%	134	13,1%
3	264	25,8%	184	18,0%
4	327	31,9%	230	22,5%
5	380	37,1%	295	28,8%
6	458	44,7%	353	34,5%
7	537	52,4%	418	40,8%
8	607	59,3%	466	45,5%
9	654	63,9%	514	50,2%
10	705	68,8%	591	57,7%
11	775	75,7%	659	64,4%
12	822	80,3%	707	69,0%
13	886	86,5%	772	75,4%
14	935	91,3%	822	80,3%
15	982	95,9%	871	85,1%
16	1024	100,0%	936	91,4%
17	N/A	N/A	988	96,5%
18	N/A	N/A	1024	100,0%

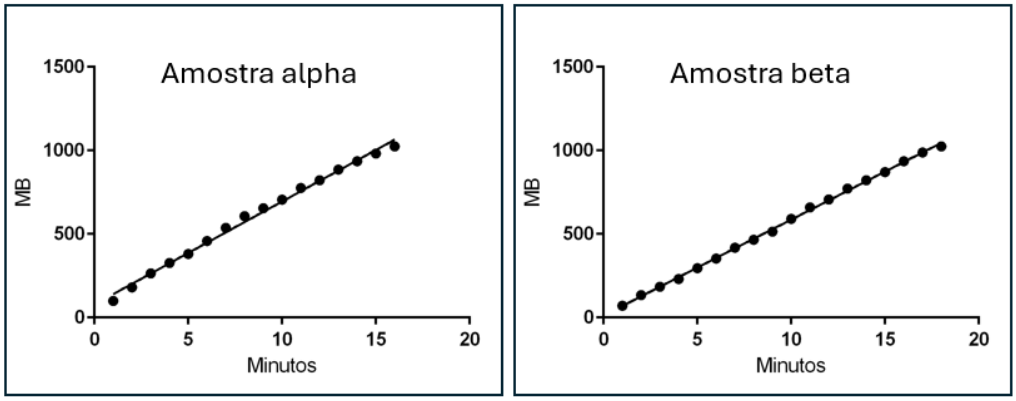

Figura 2. Regressão linear do consumo de memória RAM do cliente PTP ao longo do tempo, para as amostras *alpha* e *beta*

A partir da análise dos coeficientes e interceptos das equações de regressão linear, é possível concluir que a amostra *alpha* apresenta uma taxa de aumento no consumo de memória RAM maior do que a amostra *beta*. Isso indica que o ataque foi mais agressivo durante o experimento utilizando a amostra *alpha*. É possível notar pela Figura 2 que existe um indício de um modelo de regressão linear, o qual precisa ser melhor investigado, momento atual da pesquisa, onde mais amostras devem ser geradas e executadas para se analisar essa tendência.

É importante destacar que o PTP é vulnerável a ataques de replay. Esses ataques ocorrem quando um adversário mal-intencionado intercepta pacotes de rede válidos e os

retransmite, podendo acarretar ataques de negação de serviço. Esse tipo específico de ataque DoS está sendo referido como 'PTP flood'.

O PTP flood é particularmente prejudicial porque não apenas interrompe o serviço de sincronização de tempo, mas também pode afetar outros serviços na rede que dependem do PTP. Portanto, é crucial implementar medidas de segurança adequadas para proteger contra tais ataques.

4.1. Mitigação

Como meio de mitigação, sugerimos anexar um marcador à primeira mensagem originada do mestre e incrementar esse valor para cada mensagem subsequente. Desta maneira, cada pacote enviado do mestre teria um ID exclusivo em um determinado intervalo de IDs disponíveis, e o cliente poderia verificar se um ID de mensagem recebida corresponde a esse intervalo. Como segunda mitigação, a possibilidade de estabelecimento de uma identidade digital para os nós mestres, e na aceitação apenas de pacotes no cliente originados de mestres com uma identidade válida. Um exemplo desta abordagem é o uso do FPA (*First Packet Authentication*) com TAC (*Transport Access Control*) [DeCusatis et al. 2020].

5. Conclusão

Este artigo, através da análise dos resultados, evidenciou que os ataques de replay em um cliente PTP, mesmo com o TLV habilitado, resultam em uma negação de serviço, ataque ao qual chamamos de PTP flood. Este ataque de negação de serviço ocorre devido à sobrecarga imposta ao dispositivo alvo devido à retransmissão contínua de pacotes, o que acaba por incapacitá-lo de processar solicitações legítimas. Além disso, o consumo de memória durante o ataque demonstrou um comportamento que indica um modelo linear ao longo do tempo. É importante ressaltar que a identificação e a prevenção desses ataques são fundamentais para garantir a integridade e a disponibilidade dos sistemas de rede. Portanto, pontos de mitigações foram sugeridos a fim de detectar e conter tais ataques. Finalmente, pesquisas futuras podem se concentrar em explorar outras técnicas de ataques no PTP com os requisitos de segurança disponíveis implementados, explorar mais as mitigações e análises mais avançadas da regressão linear por meio de novas amostras.

Referências

[1588-2019 2020] 1588-2019, I. S. (2020). Ieee standard for a precision clock synchronization protocol for networked measurement and control systems. *IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008)*, pages 1–499.

[Alghamd and Schukat 2020] Alghamd, W. and Schukat, M. (2020). A detection model against precision time protocol attacks. pages 1–3.

[Alghamdi 2021] Alghamdi, W. (2021). An analysis of internal attacks on ptp-based time synchronization networks.

[Alghamdi and Schukat 2020a] Alghamdi, W. and Schukat, M. (2020a). Cyber attacks on precision time protocol networks—a case study. *Electronics*, 9(9).

[Alghamdi and Schukat 2020b] Alghamdi, W. and Schukat, M. (2020b). Practical implementation of apts on ptp time synchronisation networks. pages 1–5.

[Alghamdi and Schukat 2020c] Alghamdi, W. and Schukat, M. (2020c). Slave clock responses to precision time protocol attacks: A case study. pages 1–4.

[Alghamdi and Schukat 2021] Alghamdi, W. and Schukat, M. (2021). Precision time protocol attack strategies and their resistance to existing security extensions. *Cybersecurity*, 4(1):12.

[Alghamdi and Schukat 2022] Alghamdi, W. and Schukat, M. (2022). A security enhancement of the precision time protocol using a trusted supervisor node. *Sensors*, 22(10).

[Berardi et al. 2023] Berardi, D., Tippenhauer, N. O., Melis, A., Prandini, M., and Callegati, F. (2023). Time sensitive networking security: issues of precision time protocol and its implementation. *Cybersecurity*, 6(1):8.

[DeCusatis et al. 2020] DeCusatis, C., Lynch, R. M., Kluge, W., Houston, J., Wojciak, P. A., and Guendert, S. (2020). Impact of cyberattacks on precision time protocol. *IEEE Transactions on Instrumentation and Measurement*, 69(5):2172–2181.

[Fotouhi et al. 2023] Fotouhi, M., Buscemi, A., Jomrich, F., Koebel, C., and Engel, T. (2023). Evaluation of ptp security controls on gptp.

[GOV.BR 2023] GOV.BR (2023). Segurança de infraestruturas críticas.

[Howard 2023] Howard (2023). Ntp vs. ptp—which is right for your application?

[Itkin and Wool 2020] Itkin, E. and Wool, A. (2020). A security analysis and revised security extension for the precision time protocol. *IEEE Transactions on Dependable and Secure Computing*, 17(1):22–34.

[Jahan 2023] Jahan, Z. (2023). Colonial pipeline hack explained: Everything you need to know. Acesso em: 14 de Abril de 2024.

[Loveless, Jacob and Stoikov, Sasha and Waeber, Rolf 2013] Loveless, Jacob and Stoikov, Sasha and Waeber, Rolf (2013). Online algorithms in high-frequency trading. the challenges faced by competing hft algorithms.

[Meinberg a] Meinberg. Meinberg protocol simulation remote control.

[Meinberg b] Meinberg. Ptp track hound.

[Mizrahi 2014] Mizrahi, T. (2014). Security requirements of time protocols in packet switched networks.

[Moradi and Jahangir 2021] Moradi, M. and Jahangir, A. H. (2021). A new delay attack detection algorithm for ptp network in power substation. *International Journal of Electrical Power Energy Systems*, 133:107226.

[Moussa et al. 2020] Moussa, B., Kassouf, M., Hadjidj, R., Debbabi, M., and Assi, C. (2020). An extension to the precision time protocol (ptp) to enable the detection of cyber attacks. *IEEE Transactions on Industrial Informatics*, 16(1):18–27.

[Rezabek et al. 2023] Rezabek, F., Helm, M., Leonhardt, T., and Carle, G. (2023). Ptp security measures and their impact on synchronization accuracy. In *Proceedings of the 18th International Conference on Network and Service Management*, CNSM '22, Laxenburg, AUT. International Federation for Information Processing.

[Tidy 2022] Tidy, J. (2022). Bbbnewsbrasil. Acesso em: 25 de maio de 2023.