




Arranque Seguro de Redes 6LoWPAN para prevenir Ataques Vampiro na Internet das Coisas




Problema

As comunicações entre os dispositivos de baixos recursos presentes em ambientes da Internet das Coisas estão sujeitas a múltiplos ataques. Entre eles os **Ataques Vampiro** onde os atacantes se focam em drenar as baterias dos dispositivos e colocar a rede *offline*. Apesar de existirem estratégias de mitigação para estes ataques, a ampla gama de brechas faz com que a detecção de todas as hipóteses seja demasiado pesada para os dispositivos em questão. Para dar resposta a este problema propomos uma nova forma de arranque seguro de redes 6LoWPAN que garante comunicações seguras desde a primeira mensagem ao mesmo tempo que impede o acesso de vampiros à rede.

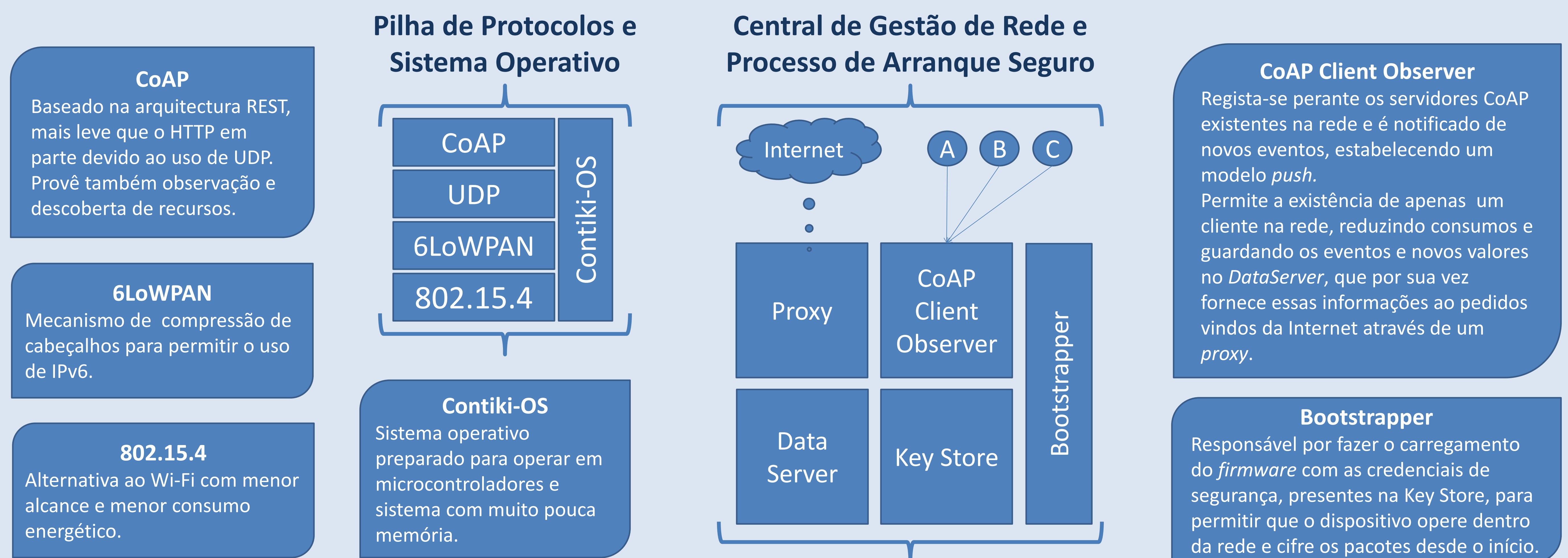
Objectivos

-  Ter uma solução com um baixo consumo energético para permitir que os nós da rede, movidos a baterias, possam ter uma longa duração de vida.
-  Manter as garantias criptográficas normalmente encontradas em protocolos usados em dispositivos com maiores recursos.
-  Criar uma solução que possa ser incorporada em sistemas já existentes e que permita a alguém sem conhecimentos técnicos usar o sistema.

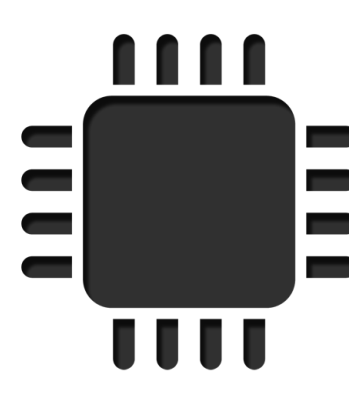


Desafios

-  A potência e alcance dos rádios usados é não só inferior ao comumente utilizado Wi-Fi, como é ainda sujeito a interferências por parte deste.
-  Para manter um baixo custo, a capacidade dos dispositivos utilizados é muito reduzida e requer sistemas operativos e protocolos dedicados.
-  Todas as credenciais criptográficas têm de estar presentes no dispositivo antes de este iniciar operações para todos os pacotes seguirem cifrados.

Solução



Resultados

-  **Aplicabilidade ao Hardware:** O *firmware* modificado com a adição de mecanismos de mitigação apresenta um aumento de apenas **3.02%** de memória flash e **1.02%** de memória RAM, num total de **61.36KB** de flash e **13.38KB** de RAM. Tais valores são compatíveis com o tipo de *hardware* de desenvolvimento usado em aplicação da Internet das Coisas.
-  **Consumo Energético:** A solução apresentada permite os rádios da rede possam estar desligados **99%** do tempo de uso. Quando estão ligados consomem apenas **0,15 Watt**, pelo que a solução é aplicável aos ambientes da Internet das Coisas.
-  **Facilidade de Uso:** O sistema apresentado foi criado para que qualquer pessoa sem conhecimento técnico possa adicionar um novo dispositivo à rede, e o tempo médio para conduzir o processo do início até ao fim demora apenas **12 segundos** por dispositivo pelo que vários podem ser adicionados num curto espaço de tempo.

Referências

- E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad Hoc sensor networks," IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 318–332, 2013.
- O. Bergmann, S. Gerdes, S. Schafer, F. Junge, and C. Bormann, "Secure bootstrapping of nodes in a CoAP network," 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 220–225, 2012.
- L. M. Oliveira, J. J. Rodrigues, C. Neto, and A. F. de Sousa, "Network Admission Control Solution for 6LoWPAN Networks," Proceedings of the 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 472–477, 2013.
- Fischer, K., Gener, J., Fries, S.: Secure Identifiers and Initial Credential Bootstrapping for IoT@Work. 2012 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (2012) 781–786
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials PP(99) (2015)

Agradecimentos



This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2013