O impacto das fragilidades da comunicação 802.11 em competições de robótica

Júlio C. M. de Resende[1], André F. J. Santos[1], Thiago S. Gomides[1], Massilon Lourenço[1], Flávio L. Schiavoni[1], Marcos A. M. Laia[1]

[1]Departamento de Ciência da Computação
Universidade Federal de São João Del Rei (UFSJ), MG – Brasil

{julio.cmdr,andrefelipes,gomides,massilon,fls,marcoslaia}@ufsj.edu.br

Abstract. *The robot competitions had served as a scenarios for the study of several areas on computer science field. In these competitions, the quest for real-time control can have a side effect that is little concern for network communication security and performance. In this paper, a communication breakdown identified in a tournament pointing out the possible causes of the problem. This vulnerability scenario can be extended to allow a broader discussion involving the communication of embedded systems with the 802.11 protocol.*

Resumo. *As competições de robôs têm servido de cenário para o estudo de diversas áreas da ciência da computação. Nestas competições, a busca por um controle em tempo real pode trazer um efeito colateral que é a pouca preocupação com a segurança e o desempenho da comunicação em redes. Neste artigo, apresentamos uma falha de comunicação identificada em um torneio apontando as possíveis causas do problema. Este cenário de vulnerabilidade pode ser ampliado para permitir uma discussão mais ampla envolvendo comunicação de sistemas embarcados pelo protocolo 802.11.*

1. Introdução

Atualmente, diversas as aplicações utilizam os sistemas embarcados, como, por exemplo, os segmentos da robótica e o futebol de robôs. Esta modalidade esportiva, apresentada na Seção 2, atua de maneira interdisciplinar envolvendo conceitos computacionais em conjunto com outras áreas de conhecimento como visão computacional, inteligência artificial, programação de sistemas, robótica, redes de computadores e sistemas distribuídos. Na área de estudo de redes de computadores, o futebol de robôs tem motivado as pesquisas sobre a sincronização e controle da comunicação de sistemas em tempo real.

No Brasil, a *Latin American and Brazilian Robotics Competition* (LARC) é exemplo de torneio da comunidade nacional de robótica. Nossa equipe, a UaiSoccer VSS da Universidade Federal de São João del-Rei, teve a oportunidade de participar do LARC–XVII (2018), conforme apresentado na na Seção 2.1. Durante a competição, foram identificados problemas com a comunicação sem fio e este trabalho motiva-se na discussão deste tema.

Motivados na compreensão das falhas de comunicação enfrentadas e na busca por possíveis soluções, este trabalho apresenta uma discussão sobre a segurança das redes sem fio em competições de robótica. Os ataques de comunicação ao meio sem fio nestes

eventos são proibidos e, consequentemente, a preocupação com segurança é ignorada. Em contrapartida, devido a ausência dos registros da comunicação sem fio durante o evento, a tarefa de analisar as falhas de comunicação ocorridas ou mesmo recriar o ambiente é de extrema complexidade. No entanto, é possível descrever algumas circunstâncias que poderiam ter colaborado para possíveis vulnerabilidades. Ainda assim, devido à sobrecarga da rede, acreditamos que as falhas enfrentadas pela equipe UaiSoccer VSS podem ser resultado de causas naturais inerentes ao espectro de problemas enfrentados na área de segurança de redes de computadores. Por outro lado, este cenário nos permite discutir sobre ataques hipotéticos que poderiam ser realizados, conforme apresentado na Seção 3.

Na Seção 4, discutimos a segurança dos sistemas embarcados com enfoque em competições de robótica. Apesar da unicidade destes eventos, acreditamos que as circunstâncias aqui relatadas podem ser aplicadas para outras situações de controle de dispositivos embarcados que utilizam fortemente a sincronização em redes. Por fim, trazemos na Seção 5 algumas considerações finais e trabalhos futuros.

2. Futebol de Robôs

Entre as aplicações em que o uso de sistemas embarcados se faz necessário, estão a cooperação e competição de robôs móveis. Nesta área, destaca-se o futebol de robôs: um ambiente de topologia dinâmica e de tempo real que engloba conhecimentos de áreas como visão computacional, aprendizado de máquina, controle e redes de computadores [Buttazzo 2011].

Esse tipo de sistema demanda uma comunicação de dados de extrema confiabilidade, que são gerados a partir de eventos harmônicos ao estado atual do sistema. Atualmente, a competição de futebol de robôs está dividida em várias categorias que são praticadas em todo mundo. Entre as diversas competições existentes no mundo, destaca-se a LARC (*Latin American and Brazilian Robotics Competition*), um evento de robótica que ocorre uma vez ao ano em algum país da América do Sul, habitualmente o Brasil. A LARC abrange entusiastas da robótica que vão desde estudantes do ensino fundamental até doutores e pós doutores. Além do futebol, dentro do evento são praticadas categorias de robótica em que robôs autônomos realizam atividades como resgate de vítimas em ambientes desastrosos, auxílio doméstico, dança, corrida, dentre outras. Na LARC, as competições de futebol de robôs são divididas em categorias como simulação, robôs humanoides e robôs que utilizam rodas. Dentre todas, a categoria *IEEE Very Small Size Soccer* (IEEE VSSS) [IEEE 2009] se destaca por utilizar robôs que usam rodas de tamanho reduzido e controlados remotamente por um computador.

Nesta categoria, cada equipe tem direito a colocar até três robôs em campo. Uma câmera suspensa sobre o campo atua como entrada do sistema e a informação que detalha qual ação a ser tomada é enviada para os robôs a cada instante durante o jogo. Por isto, as vulnerabilidades na comunicação entre o computador e os robôs configuram um sistema distribuído de tempo real em que qualquer falha de comunicação pode resultar no não funcionamento do sistema.

2.1. A equipe UaiSoccer VSS e sua participação na LARC 2018

A UaiSoccer VSS é uma equipe de robótica que compete na categoria de futebol de robôs IEEE Very Small Size Soccer. O projeto teve inicio no ano de 2016 por uma iniciativa de membros do Departamento de Ciência da Computação (DCOMP) da UFSJ, que tinham

como objetivo o desenvolvimento e a aplicação de algoritmos de navegação em robôs reais.

A proposta da equipe para o LARC 2018, realizado em João Pessoa - PB, foi utilizar uma arquitetura de software separada em módulos, permitindo assim fácil manutenção. O primeiro módulo, de Visão Computacional, foi responsável por adquirir as imagens de uma câmera conectada ao computador via USB e processar estas imagens identificando a posição e a angulação de todos os robôs presentes no campo e da bola. Este módulo processa 60 fps, e a cada quadro processado uma cadeia de caracteres contendo todas as informações retidas do ambiente é enviada via socket UDP para o próximo módulo, que é executado no mesmo computador.

O segundo módulo, de navegação e controle, implementa estratégias de jogo, gera trajetórias para os robôs e envia comandos de velocidades para as duas rodas de cada robô. Cada comando é enviado para o seu respectivo robô 60 vezes por segundo, através de um socket UDP. Os robôs possuem um microcontrolador ESP8266, que conta com uma antena WiFi 2.4GHz acoplada para o recebimento dos comandos. O processamento do robô é dividido entre receber um pacote e executar a ação correspondente.

Esta necessidade de comunicação em tempo real para o controle dos robôs se mostrou uma estratégia passível de falhas durante a participação da equipe UaiSoccer VSS no LARC 2018. Muitas vezes, esta comunicação foi comprometida e impediu o funcionamento correto dos robôs. Entendendo que tal dificuldade de comunicação estava ocorrendo por falhas na rede, a UaiSoccer VSS optou por jogar com apenas um dos três robôs nos horários de maior movimentação no evento pois assim havia uma redução no número de pacotes trafegando pela rede, e consequentemente melhor desempenho na partida. Nos jogos e treinos que ocorreram na parte da noite, quando muitos competidores já haviam deixado o evento, foi possível colocar os 3 robôs para jogar e apresentar um desempenho próximo ao obtido em laboratório sem interferência externa, o que possibilitou vencer algumas partidas. O problema apresentado por nossa equipe também foi notado por outras equipes que participavam em outras modalidades, como as que envolviam Drones e/ou robôs de maior porte.

3. Exploração das Vulnerabilidades

Em competições de robótica, a exploração das vulnerabilidades dos protocolos de comunicação ou ataques destinados a eles é proibida. Por outro lado, o comitê organizador destes eventos não oferece mecanismos que permitem identificação ou defesa desta prática. Portanto, esta seção considera algumas das vulnerabilidades passíveis de exploração a partir dos ataques de comunicação. Neste contexto, os ataques destinados a interferências de sinais, como os *Jamming Attacks*, poderiam ser responsáveis pela sobrecarga do canal sem fio e, dessa forma, causariam falhas de comunicação entre robôs e servidores. Assim, nos ataques de interferência de sinal, um atacante busca proporcionar instabilidades nos dispositivos de rede baseados no protocolo 802.11. A partir de um conjunto de ferramentas, o atacante pode emitir também ruídos nas frequências de operação do protocolo e, com isso, interromper a comunicação entre os dispositivos. Além disso, os ataques de *Jamming* são de grande abrangência, indo desde a emissão de ruídos até a replicação de pacotes de desautenticação da rede sem fio.

Além disso, outras vulnerabilidades podem ser exploradas nos casos em que as

equipes não se preocupam ou desconsideram uma boa configuração do ponto de acesso. Assim, os ataques de falta de configuração (*Misconfiguration Attacks*), acontecem quando um roteador é configurado usando a configuração padrão, credenciais fracas ou algoritmos de criptografia fracos, podendo o invasor adentrar facilmente na rede e proporcionar instabilidade ou completa ausência de comunicação [Eshete et al. 2011]. Além destes, devido as restrições de processamento comuns aos dispositivos IoT, este cenário é ideal para o ataque do gêmeo do mal [Yang et al. 2012]. Este ataque tem por objetivo comprometer a conexão a partir da configuração de um ponto de acesso falso, com o mesmo SSID. Nesse sentido, o invasor que define configurações semelhantes ao de um AP seria capaz de solicitar detalhes da autenticação do ponto de acesso original e, assim, controlar as funções dos robôs em todo o ambiente.

4. Discussões

As falhas de comunicação que podem ocorrer em eventos como competições de robótica são apenas um exemplo de falhas em redes sem fio que podem ocorrer com qualquer dispositivo IoT com pouca ou nenhuma segurança. A pilha de protocolos TCP/IP praticamente não possui segurança implementada em seus protocolos de baixo nível, deixando a responsabilidade de garantir segurança da comunicação para a camada de aplicação. Com o tempo, os principais protocolos de aplicação não seguros foram substituídos por protocolos seguros, como a troca do TELNET pelo SSH, HTTP por HTTPS, entre outros. No entanto, com o surgimento da IoT, a computação e a comunicação em rede parece muitas vezes ter voltado à condição anterior de ser um ambiente ingênuo em relação à segurança, talvez por estar conectado atrás de um NAT ou em uma LAN.

As competições de robótica são exemplos de ambientes em que as conexões embarcadas geralmente acabam ignorando as questões de segurança para tentar melhorar o desempenho da comunicação. Todas as verificações de segurança usualmente são deixadas de lado pois atrasos de pacotes não são toleráveis neste cenário. Assim, não é comum nesses ambientes verificações sobre o remetente do pacote, ou controle de ordenação dos pacotes recebidos. No entanto, assim como aconteceu com equipes como a UaiSoccer VSS, a preocupação com o desempenho acabou por comprometer o funcionamento do sistema e robôs passaram a atuar de maneira incoerente com o estado atual do ambiente.

Para diferir ataques de causas naturais, a organização do evento poderia monitorar o tráfego da rede para que fosse possível uma auditoria e, assim, possibilitar a detecção de problemas. Já para evitar falhas na comunicação, alterações nas frequências de comunicação poderiam ser realizadas e, assim, reduziriam a interferência de comunicação. Este é o caso da comunicação em 5GHz que, por não ser utilizada por dispositivos Bluetooth e telefones sem fio, por exemplo, é menos suscetível à interferências. Nesse sentido, recorrer diretamente às camadas mais baixas da pilha TCP/IP, como, por exemplo, a camada de enlace, também é um ponto a ser considerado, pois assim seria reduzida a complexidade dos pacotes como também a influência de outras redes na comunicação entre os robôs.

5. Conclusão

O número de dispositivos capazes de se comunicarem através da rede e fornecerem soluções e inovações para as mais diversas aplicações tem crescido nos últimos tempos. No entanto, grande parte das aplicações envolvendo sistemas embarcados e IoT possuem

limitação física, de processamento e memória [Satyadevan et al. 2015], o que pode resultar em um sistema que não leva em consideração as questões de segurança para tentar garantir um melhor desempenho em sua comunicação.

Neste artigo, apresentamos uma situação que faz o uso de sistemas embarcados que, por não possuir preocupações explícitas em relação a segurança, pode estar suscetível a ataques, além de sofrer com causas naturais. Apesar de esta parecer uma situação isolada, tal cenário pode ser expandido para outros cenários, como escritórios e condomínios residenciais, onde a quantidade de dispositivos competindo pelo mesmo canal de transmissão tem aumentado dia após dia.

Este cenário pode ilustrar o tipo de falha de comunicação e sincronização que pode ocorrer em uma situação semelhante, como, por exemplo, a expansão da internet das coisas em todos os ambientes cotidianos e os possíveis ataques e falhas que estes dispositivos podem sofrer. Grandes transtornos podem ocorrer se situação semelhante acontecer com câmeras de segurança e monitoramento de veículos autônomos, por exemplo. Nestas situações, fica evidente a necessidade do uso de protocolos de rede que proporcionem segurança e eficiência em diferentes enlaces, pois a Internet, em princípio, não é segura.

Para trabalhos futuros, pretende-se utilizar ferramentas capazes de analisar por completo o tráfego de informações durante as competições a partir de log de dados. Isso proporcionará análise e identificação das sobrecargas e vulnerabilidades encontradas no cenário aqui apresentado. Além disso, o monitoramentos de tráfego em eventos similares seria adequado para a análise posterior dos dados da comunicação. Estes dados permitiriam também a criação de punições em casos de ataques e criação de regras referentes à rede para que não ocorram problemas.

Agradecimentos

Os autores gostariam de agradecer a Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) sob concessão No.: APQ-03120-17. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Referências

Buttazzo, G. C. (2011). *Hard real-time computing systems: predictable scheduling algorithms and applications*, volume 24. ElsevierSpringer Science & Business Media.

Eshete, B., Villafiorita, A., and Weldemariam, K. (2011). Early detection of security misconfiguration vulnerabilities in web applications. In *2011 Sixth International Conference on Availability, Reliability and Security*, pages 169–174. IEEE.

IEEE, L. A. (2009). Ieee very small size rules. *CBR Robótica*.

Satyadevan, S., Kalarickal, B. S., and Jinesh, M. K. (2015). "security, trust and implementation limitations of prominent iot platforms". In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pages 85–95, Cham. Springer International Publishing.

Yang, C., Song, Y., and Gu, G. (2012). Active user-side evil twin access point detection using statistical techniques. *IEEE Transactions on Information Forensics and Security*, 7(5):1638–1651.