Métodos Bio-inspirados Aplicados à Sistemas Autônomos de Segurança em Redes IoT

Gustavo Barros de Alcântara[1]

[1]Universidade Federal do Paraná (UFPR)
Curitiba – PR – Brazil

gba12@inf.ufpr.br

Abstract. *This paper will describe the main problems of automatic management and self-configuring concepts on IoT networks, focusing security aspects. It will describe a brief content on the state of the art for solving this kind of problems, including fresh and non-conventional manners, like bio-inspired methods for creating innovative solutions in self-configuring and IoT network security. Will present a layered security model for the IoT organization, which inspiration came from vertebrates animals immune systems. It will also be developed a survey about this theme to explore the fundamentals ideas behind these concepts of adaptive and self-configuring networks to enhance and clarify the reader view, whom can benefit of this study, for the creation of safe and autonomous IoT networks.*
Keywords: *Artificial Immune System, Bio-Inspired Networks, IoT, Internet of Things, IoT Security.*

Resumo. *Esse papel irá descrever os principais problemas do conceito de gerência automática e de auto-configuração das redes IoT, focando aspectos de segurança. Descreverá uma parte do estado da arte para a resolução de tais problemas incluindo maneiras não convencionais e emergentes, como métodos bio-inspirados para cunhar soluções inovadoras de auto-organização e segurança nas redes IoT. Apresentará um modelo em camadas de organização para a IoT, cuja inspiração vem de sistemas imunológicos de animais vertebrados. Será desenvolvido também um "survey"a respeito do tema para explorar as ideias fundamentais desses conceitos de redes adaptativas e de auto-configuração, para esclarecer e fornecer novas abordagens aos leitores que possam se beneficiar desse estudo, na criação de redes IoT autônomas e seguras.*
Palavras-chave: *Sistemas Imunológicos Artificiais, Redes Bio-inspiradas, IoT, Internet das Coisas, Segurança na IoT.*

1. Introdução

O grande aumento de tamanho e complexidade das redes globais, atualmente e nos anos vindouros, apresenta para a gerência de redes um enorme desafio de gestão. Como o recurso humano é algo caro, suscetível à falhas, e muitas vezes ineficiente, a gestão automática de tais redes não só é necessária como é crucial para a sobrevivência e evolução desses sistemas. Tudo está se tornando inteligente e conectado. As cidades irão interagir com os cidadãos e outros recursos urbanos, carros irão conversar entre si nas ruas e rodovias, as casas saberão a rotina e preferência de seus moradores, objetos e muitas outras

coisas ao redor das pessoas terão funcionalidades expandidas. A Internet das Coisas (IoT) irá criar um aumento de bilhões à trilhões de novos dispositivos wireless identificáveis na rede Internet, estimou Gartner *apud* [1] que serão 50 bilhões de dispositivos conectados até 2020, que por sua vez serão utilizados para tornarem reais os conceitos de Inteligência de Ambientes, Computação Omnipresente e Computação Persistente [2]. Todos esses novos dispositivos terão que ser gerenciados de maneira segura e eficiente. Dessa forma uma nova maneira de trabalhar com a rede precisa emergir para que o sistema consiga adaptar-se às necessidades e ameaças crescentes de forma a se auto-organizar independentemente da variedade de dispositivos de comunicação sob sua influência, assim como outros sistemas e aplicações, e ao mesmo tempo possua escalabilidade para um grande número de usuários e seja resistente à mudanças imprevistas [3].

Para gerir esses desafios de modo inteligente, seguro, automático e sem interferência humana, técnicas bio-inspiradas podem ser utilizadas em redes IoT de forma a amenizar os problemas que surgem com o aumento do tamanho e dinamismo da rede. É possível também usar algoritmos bio-inspirados em áreas que afetam as redes indiretamente, como para economizar energia em redes de sensores wireless [4], fundamentais para a comunicação entre dispositivos e transferência de dados numa IoT, ou então para roteamento e sincronização de nós. Tais técnicas também podem ser aplicadas em outros tipos de redes como: P2P, VANETS, Internet, RSSF e muitas outras. Com esses novos paradigmas torna-se possível obter resultados interessantes e muitas vezes melhores do que os resultados provenientes de métodos convencionais ultrapassados em termos de escala e dinâmica de rede. Assim esse papel abordará a aplicação de técnicas bio-inspiradas para resolução de problemas de auto-organização e segurança em redes IoT.

2. Trabalhos Relacionados

Como a rede IoT é um tipo de rede emergente, poucos trabalhos com tema específico semelhante a esse papel, foram encontrados. Porém nota-se uma grande tendência das ideias atribuídas à IoT e à segurança de redes convergindo para um mesmo local. Burange e Misalkar [2] falam sobre diversos aspectos gerais da IoT e o grande crescimento que esse tipo de rede terá no futuro em decorrência da evolução da tecnologia de hardware e sensores, assim como os problemas de segurança e privacidade que irão surgir. Outros como Duan et al [3] apresentaram ideias e conceitos bio-inspirados aplicados às redes, tendo como objetivo alcançar sistemas distribuídos, auto-organizáveis e autônomos para grandes sistemas. Basu et al [5] discutem os desafios atuais de design e segurança na IoT e várias abordagens possíveis para resolvê-los, e expõe as maiores fraquezas e perigos que esse tipo de rede provavelmente enfrentará. Uma nova forma de lidar com a segurança de redes, em geral, foi elaborado por Zhou et al [6]. Nas sessões seguintes esse conceito será melhor explorado para mostrar como pode ser aplicado no âmbito da IoT. Salvato et al [7] desenvolveram um detector de anomalias baseado em conceitos de Imunidade. E Elhaj et al [8] apresentam conceitos bio-inspirados para a criação de camadas em sistemas imunes de forma a separar grupos de tráfegos em tipos distintos. Outros autores propuseram sistemas de defesa baseados quase em sua totalidade em sistemas imunológicos, como Liu et al [9, 10] propuseram a ideia de criar um mecanismo de detecção de ameaças que evolui. A ideia geral tem como estratégia elementos básicos que detectam ameaças, aprendem e se multiplicam. Mapeiam os dados da rede em conjuntos distintos, aqueles que fazem parte do sistema e os que não fazem, nomeados como antígenos próprios e antígenos não-próprios respectivamente. Aqueles que não fazem parte do sistema são considerados

como corpos estranhos , ou seja, uma ameaça. Em Gu et al [22] são mencionados os paradigmas e aplicações mais comuns sobre sistemas imunológicos artificiais, utilizados para sistemas de detecção de invasão. Os autores também descrevem uma classe de algoritmo que teve bons resultados em diversas aplicações, esse algoritmo se chama *The Dendritic Cell Algorithm*, que de certa forma é muito parecido com o que foi usado em [9, 10]. Outros como Flauzac et al [23], propuseram uma arquitetura baseada em SDN para segurança de redes IoT. Da mesma forma como o modelo proposto neste papel. De fato sistemas baseados em SDN tem demonstrado ser uma das grandes apostas das redes do futuro por facilitar muito a administração de redes complexas.

Porém todos esses trabalhos propõem métodos esparsos em diversas áreas. No âmbito da IoT é preciso que seja feita uma abordagem holística, combinando várias dessas técnicas e conceitos de forma a aglutiná-los em sistemas maiores, mais complexos e robustos.

3. Descrição

Soluções autônomas para auto-gerência e segurança é um assunto de extrema relevância especialmente à sombra daquilo que o futuro indica que a tecnologia terá de enfrentar. As vantagens de utilizar métodos bio-inspirados são suas capacidades de serem autônomos, auto-organizáveis e dessa forma altamente escaláveis e independentes. Mas o ponto negativo é que essa é uma área com inúmeras possibilidades ainda a serem exploradas, só é possível observar um pequeno deleite das soluções que os sistemas da natureza tem para oferecer. E dessa forma, tenta-se desenvolver soluções aos problemas do cotidiano usando os conhecimentos forjados a bilhões de anos de evolução nas criaturas orgânicas.

4. Desafios

No momento atual a sociedade científica começa vislumbrar a alvorada de uma civilização futura, não muito distante, onde tudo estará conectado à Internet para criar ambientes inteligentes e de computação omnipresente. Alterando drasticamente o modo de vida das pessoas. Tal salto traz consigo consequências. A IoT logo de início trará problemas relacionados ao tamanho da rede que irá emergir, bilhões ou talvez trilhões de dispositivos introduzidos a mais na Internet. Todos com endereçamento único e tentando se comunicar o tempo todo, gerando altas cargas de transmissão no substrato tecnológico das redes atuais, sobrecarregando-o ainda mais. A infra-estrutura terá de ser ampliada, mas somente implantação de novos canais de transmissão não é o suficiente. A transmissão deve ser feita de forma eficiente e inteligente.

Como a ideia central da IoT é conectar um grande espectro de artefatos humanos, alguém pode imaginar a interação entre milhares de pessoas, roupas, eletrodomésticos, smartphones, sensores, robôs, carros e ambientes praticamente em tempo real. Um exemplo seria uma pessoa caminhando para o trabalho e ao entrar em sua cafeteria preferida o sistema rapidamente detecta sua presença, cliente conhecido, e como o sistema sabe o que o cliente geralmente gosta para o café-da-manhã logo agiliza o preparo e debita o valor em sua conta. Tal cenário é digno da palavra “eficiente”. Porém toda essa eficiência tem um alto custo. Sendo responsável por gerar um sistema altamente dinâmico, inseguro e incapaz de ser regido por métodos convencionais de gerência de redes. Em um determinado momento existirá dispositivos entrando e saindo da rede, ora transmitindo, ora ausente. Um controle centralizado e imutável de tal rede rapidamente se torna ineficiente

e impraticável, assim mecanismos de detecção e manutenção de tais comportamentos devem ser explorados mais profundamente. E principalmente devem ser autônomos. Como mencionado em [11], um fato que não pode ser negligenciado é a IoT ser implementada sobre um assoalho tecnológico heterogêneo. Dispositivos dos mais diversos compondo parcelas da comunicação via WiFi, ZigBee, Bluetooth, ethernet e outras tecnologias de forma a dificultar o dialogo transparente entre as diversas partes do sistema.

A própria arquitetura da IoT oferece um enorme desafio de gestão da segurança como um todo. De acordo com [1] as aplicações em IoT já estão começando a acontecer, mas não existem ainda padronizações que sejam claras o suficiente sobre como essas tecnologias devem ser implementados na prática. Somando se a isso existem dispositivos de diversos fabricantes disponíveis no mercado, conversando entre si usando muitos protocolos diferentes ao sabor daqueles que implementaram tais sistemas.

Geralmente essas implementações e os hardwares utilizados são deficientes em termos de criptografia por limitações computacionais e/ou energéticas. Então atribui-se a esse emaranhado de tecnologias heterogêneas e a cada dispositivos desses um endereço IP para que sejam identificáveis na Internet, obviamente essa é uma receita para desastres. Inúmeros buracos de segurança irão surgir quase que compulsoriamente até que uma tecnologia de controle ou forma de padronizar tais sistemas surja para coordenar o funcionamento de forma adequada e segura dessas micro-redes IoT. Para piorar, os problemas que tangem a IoT vão além do escopo original de segurança em que se limita somente aos dispositivos e dados locais de uma determinada pessoa ou organização. Com a IoT e a quantidade gigantesca de informações que esses sistemas irão gerar existe a possibilidade de traçar perfis não só de pessoas mas de populações como um todo. Possuindo assim o potencial de infligir sérios danos às privacidades e liberdades dos usuários e até mesmo segurança nacional de um país se essas informações forem usadas de maneira descontrolada ou maliciosa por países inimigos ou grupos terroristas, ou mesmo que sejam fomentadas por interesses econômicos ou cibercrime. Existem também sérias implicações a respeito das integridades físicas e/ou psicológicas das pessoas ao imaginar a crescente onda de crimes que podem surgir com a exploração dessa tecnologia, logo é um tema de altíssima preocupação.

Os perigos são reais e como exposto em [1] casos de "*cyberwarfare*"ou ciberterrorismo já aconteceram em alguns países no passado e a tendência é que IoT crie precedentes para o crescimento dessas ameaças. Os dispositivos também ficam fisicamente expostos, podendo ser interceptados em nível de hardware ou clonados. Algumas técnicas para lidar com isso, como *physical unclonable functions* (PUFs) , estão sendo desenvolvidas e serão discutidas mais a frente neste papel.

De acordo com [5] a mobilidade é outro fator que pode trazer problemas na situação em que um dispositivo pode momentaneamente "desaparecer"da rede devido a falta de conexão, dessa forma algum dispositivo clonado poderia, de forma ilegal, tentar co-existir numa outra rede por exemplo. Por isso todos os nós devem ser autenticados de forma que a comunicação entre máquinas seja confiável e que nenhum nó desconhecido possa lançar algum tipo de ataque como *Deny-of-Service* (DoS) para outros dispositivos e causar uma sobrecarga no sistema, sendo preciso que os nós possam confiar nos outros intermediários da rede em situações de alta mobilidade para que não surjam potenciais ataques. Também existem os diferentes mecanismos de empacotamento de dados e a necessidade do com-

partilhamento de chaves da criptografia entre os vários nós que estão trocando mensagens. O que é potencialmente perigoso para vazamento de informações e dessa forma criptografia fim-a-fim é preferível [5].

Dessa forma, no modelo proposto nesse papel sugere mais a frente no texto uma técnica capaz de impedir a intervenção de dispositivos clonados em caso de uma momentânea perda de contato com o dispositivo verdadeiro.

5. Modelos bio-inspirados

Existem diversos conceitos, métodos e algoritmos bio-inspirados que podem ser aplicados para resolver problemas complexos do ser humano. Normalmente tais ideias advém dos produtos de bilhões de anos de evolução que culminaram nas soluções mais sutis, simples e astutas que o pináculo da criação poderia contemplar até hoje. Na grande maioria dos casos tais sistemas não são conhecidos em toda sua profundidade, porém uma breve observação demonstra o grande potencial que tais sistemas tem a oferecer. No caso da segurança de redes existe uma bio-inspiração que prontamente se destaca como uma possível solução, esta são os sistemas imunológicos de animais, principalmente de mamíferos. Formados por milhões de células os sistemas orgânicos de defesa são naturalmente escaláveis, adaptativos, auto-organizáveis, curáveis, possuem memória e são altamente eficientes. Podem então analogamente serem usados para incorporar sistemas artificiais de segurança em redes de computadores, pois assim como as redes evoluem e crescem da mesma forma como um organismo vivo, tal sistema seja vivo ou artificial precisará de um sistema imunológico que consiga se adaptar e evoluir junto com o todo, que seja distribuído e capaz de neutralizar ameaças sem intervenção humana. Existe demasiada semelhança entre o arcabouço biológico e as redes artificiais.

5.1. Um sistema que evolui

A quantidade e tipos de dispositivos na IoT irá extrapolar a capacidade de compreensão humana, não será possível que um simples indivíduo ou um grande grupo de pessoas conheçam toda a cadeia de eventos nessa rede e a Internet combinadas. As pessoas e os projetistas de redes terão que confiar nas máquinas e em seus algoritmos, terão que criar um sofisticado sistema que por si só garanta a segurança como um todo precisando talvez de pequenos ajustes locais em caso de anomalias eventuais. Alguns pesquisadores já começaram a abordar o assunto, e essa área de pesquisa mostra-se promissora para o futuro. A seguir será descrito o funcionamento do mecanismo “Evolving Defense Mechanism”(EDM) proposto em [6], a inspiração para o EDM surgiu no contexto de populações orgânicas em que cada indivíduo de uma população possui uma codificação genética (genótipo) que atribui-lhe características físicas (fenótipo), e esta última determina suas relações de sobrevivência com o meio em que está inserido. A sobrevivência de um único indivíduo geralmente é muito baixa, mas ao aumentar a escala de observação a nível de população percebe-se que estas são difíceis de se extinguir. No caso de uma catástrofe que paira sobre uma população em um determinado momento, muitos irão morrer, mas existe uma chance de que uma pequena parcela sobreviva e continue a se reproduzir e perpetuar a espécie. Um exemplo de catástrofes populacionais são colônias de bactérias atacadas por antibióticos. Em alguns casos a população inteira é erradicada, porém em outros existe um único ou alguns indivíduos que possuem genótipos que

atribuem-lhes resistência ao determinado medicamento, logo sobrevivem e desenvolvem uma nova população resistente àquele medicamento, como as temíveis superbactérias.

O EDM tenta então imitar esse comportamento abstraído e projetado em uma rede virtual usando controladores SDN, os autores propuseram que as alterações do ambiente nesse modelo teórico seriam ataques de diversos tipos mapeados em subgrupos a partir de algum sistema de *Intrusion Detection System* (IDS) desenvolvido a parte. E para cada alteração do ambiente existem genótipos (configurações de rede) que promovem fenótipos (funcionamento real da rede de acordo com as configurações) que são mais aptos a neutralizar e sobreviver às ameças. Tais fenótipos incluem alterações do endereçamento de IP, roteamento variável entre hosts, alterações nas formas de criptografia dos dados, e variação das respostas de cada host. O objetivo é tornar a rede um ambiente obscuro para os atacantes de forma a impossibilitar mapeamentos de topologia e marcação de alvos fixos para ataques dos mais diversos. Em contrapartida, os mecanismos de segurança que são construídos sobre configurações estáticas de uma rede criam fraquezas no sistema [6]. De acordo com os experimentos realizados pelos autores, o EDM consegue proteger uma rede contra escaneamentos e ataques na maioria dos casos utilizando a variação do endereçamento IP e as outras técnicas citadas acima. O sistema é realmente promissor no quesito de dificultar a atuação de atacantes no geral. O EDM apresenta bons resultados desde que os hosts sob sua defesa estejam imersos numa virtualização por SDN, o problema é a necessidade de possuir um sistema de controle centralizado ou ao menos hierárquico, o que pode abrir outros tipos de brechas para futuros ataques.

Os autores em [6] não descreveram como as "tabelas de configurações"que foram propostas para uso interno no EDM, responsáveis por conter as variações de configuração, seriam preenchidas e estabelecidas. Da forma como foi exposto provavelmente seriam codificadas à mão ou usando algum tipo de algoritmo. Entretanto uma forma que provavelmente daria bons resultados seria usar um algoritmo bio-inspirado baseado também em populações genotípicas, conhecido na literatura clássica como algoritmo genético (AG). O que esse algoritmo faz é criar uma população de vetores solução (população de cromossomos), normalmente inicializados com valores aleatórios, e então utilizar procedimentos de recombinação (crossover) entre eles e também a mutação de genes, da mesma forma como acontece na natureza quando há reprodução sexuada entre seres vivos. Então cada cromossomo é testado, para observar a eficácia do seu fenótipo, usando uma função chamada *fitness*. Os melhores indivíduos geralmente são selecionados para a próxima geração de acordo com algumas regras e o restante é descartado. Diversos estudos demonstram que existe uma grande chance de obter soluções que se aproximam do ótimo global de um problema dependendo de quão bem implementado é o algoritmo para o desafio específico da aplicação, um desses trabalhos [12] aplicou o AG em redes neurais e concluíram que se obtém um melhor resultado se a população envolvida é alta e o se numero de gerações do algoritmo cresce com o tempo. Um paralelo pode ser traçado para outros tipos de aplicações além de redes neurais, apesar do AG ser computacionalmente caro ele tem potencial de obter bons resultados. Então, ataques feitos de propósito à rede em questão poderiam ser realizados enquanto um algoritmo genético busca as melhores soluções para pré-fabricar uma tabela de soluções. Obviamente o processo de evolução deve ser mantido durante todo o ciclo de vida de tal rede, mas não necessariamente 100% do tempo.

Outro algoritmo poderoso, muito conhecido, que poderia ser usado não somente para o preenchimento das tabelas, mas também para a otimização do sistema de detecção de antígenos ou do roteamento variável dos hosts é o PSO (Particle Swarm Optimization). Da mesma forma como o AG, o PSO é um algoritmo de populações, porém neste último o enxame de indivíduos "voam"sobre o espaço de soluções ao invés de sofrerem recombinações ou mutações. Normalmente o PSO tem a fama de convergir muito mais rápido e com melhor qualidade do que o AG, porém depende muito da implementação dos parâmetros e das técnicas utilizadas. A inspiração inicial do algoritmo teve suas origens em bandos de pássaros. A forma como cada indivíduo se comunica com seus vizinhos resulta numa movimentação complexa durante o voo. A cada etapa as velocidades e as posições de todas as partículas são recalculadas, usando um método matemático e um sistema de memória. Ao "lembrar"do passado torna-se possível julgar se o resultado foi bom ou não usando uma função *fitness*, ou seja, cada partícula se lembra da sua última melhor posição e a última melhor posição global (dos seus vizinhos). A melhor posição são os pontos do espaço percorrido mais próximos dos ótimos locais ou globais da função que se deseja otimizar, e a analogia feita é a de um bando de pássaros que buscam por comida no espaço, ou seja, os ótimos da função. Dessa forma as partículas se movimentam entre o ótimo da própria partícula (conhecimento individual) e o ótimo global (conhecimento social) de forma a ampliar a busca em regiões maiores e evitar que as partículas fiquem presas num ótimo local. O uso do PSO para otimizar o sistema de defesa com certeza seria útil para trazer melhorias de segurança. Em [13] os autores mostraram em um outro tipo de aplicação aplicação que é possível economizar energia em clusters de sensores sem fio na IoT usando o PSO, apesar dos resultados não terem sido tão espetaculares no experimento realizado por eles, a possibilidade de economia de energia foi evidenciada e demonstra a necessidade de mais pesquisas na área.

O EDM é um mecanismo que claramente pode ser melhorado através de um estudo mais aprofundado, experimentando e misturando várias abordagens diferentes de aprendizado e até mesmo de diversas outras áreas do conhecimento. Poderia usar, por exemplo a neuroevolução que é o uso de algoritmos evolutivos para treinar redes neurais de forma a encontrar novas configurações mais eficientes. Simulações extensivas de ataques à rede como já comentado acima seriam especialmente necessárias para que se possa evoluir as tabelas de estratégias de configurações. E como será mostrado nas sessões seguintes, o modelo proposto neste papel usa os conceitos do EDM aplicados a uma topologia distribuída de forma a tentar minimizar os efeitos negativo do modelo centralizado original.

5.2. Sistemas imunológicos artificiais multi-camada

Um sistema imunológico nunca é algo trivial e direto, apesar de algumas características inerentemente simples dos agentes formadores, é a união das qualidades que estabelecem o *status quo* da complexidade de tais sistemas. Isso logicamente se reflete nas criações artificiais.

Claramente pode-se observar que o sistema imunológico humano (HIS) e de outros animais são formados por diversas partes e camadas. No caso do HIS em um nível mais externo existe a pele que protege o organismo contra alterações de temperatura e contatos explícitos entre o meio externo e interno de forma a evitar sérios prejuízos ao maquinário orgânico, pois geralmente o ambiente externo é hostil e repleto de patógenos agressivos. Abaixo da pele existem diversos tipos de tecidos e outras camadas, e em nível molecular

existe uma quantidade de células que com certeza ultrapassam alguns bilhões ou trilhões em quantidade que compõe todos os tecidos do corpo inclusive o sistema circulatório. Cada uma dessas células também são compostas por diversas camadas como a membrana plasmática, o citoplasma, a membrana nuclear e os diversos componentes chamados de organelas que compõe cada um desses níveis e atribui-lhes uma funcionalidade. Ao tomar essa ideia biológica também como inspiração para a segurança de sistemas existe uma necessidade de copiar algumas dessas estruturas nos sistemas artificiais, não é a toa que o corpo humano é dividido em camadas e estruturas distintas, a excelência do funcionamento desse "projeto"orgânico é comprovada pelos bilhões de anos de existência e sucesso de sobrevivência desses organismos.

Os autores de [8] aplicam justamente esse conceito para o controle de tráfego e aprimoramento de sistemas de IDS em uma rede. Eles propuseram a criação de um sistema com duas camadas, a camada inata e a camada adaptativa. Esses nomes são oriundos da imunologia clássica em que a parte inata é a categorização das células que reconhecem outras células como sendo parte do organismo ou como partículas estranhas que não fazem parte do organismo, porém não são capazes de aprender sobre novas ameaças e possuem um comportamento geral de defesa. A parte adaptativa são as células que aprendem a combater um determinado tipo de antígeno e se especializam no combate a esse antígeno específico, se multiplicam e destroem a ameaça rapidamente num próximo encontro. Um exemplo seria uma pessoa que foi contaminada por uma determinada cepa do vírus *Influenza*, causador da gripe, e em pouco tempo essa pessoa se torna imune ao vírus por possuir uma grande quantidade de células de defesa que se desenvolveram contra aquele vírus específico. Porém essas células não vão combater uma cepa do mesmo vírus que sofreu mutação e modificou sua estrutura e receptores químicos. O processo de aprendizado deverá ser repetido. Em [8] os autores utilizaram um sistema especialista baseado em lógica fuzzy para agir como a camada inata e ser a primeira linha de defesa do sistema. Lógica fuzzy foi escolhida por prover meios de tomar decisões rápidas a respeito dos pacotes que estão circulando na rede usando conhecimentos de especialistas de segurança. Essa técnica permite que mesmo diante de situações incertas e com pouca informação o sistema fuzzy consegue inferir algumas decisões. Porém quando esse sistema falha em determinar o tipo de tráfego, classificado em normal, anormal e desconhecido [8], os autores sugerem que tais pacotes sejam passados para a camada adaptativa onde um processo de aprendizado será realizado sobre tais pacotes de forma a inferir se são seguros ou não.

As vantagens de trabalhar com diversas camadas se da ao fato de algumas camadas especializadas rapidamente solucionarem o problema em questão sem demasiada demora, pois geralmente grande parte do tráfego é considerado normal e legítimo. Os poucos restantes que podem ser comportamentos maliciosos são barrados para uma segunda análise. Dessa forma todo o sistema em si tem um ganho de performance considerável.

Já as desvantagens do sistema proposto é usar um mecanismo especialista formulado à mão, baseado em lógica fuzzy, por profissionais da área o que pode acarretar em implicações de segurança caso seja possível achar uma brecha e burlar tal mecanismo. Técnicas mais maleáveis deveriam ser exploradas em conjunto com a lógica fuzzy para tornar o sistema mais robusto.

5.3. Sistemas imunológicos artificiais com enxame para detecção de intrusão

A seguir será descrito uma aplicação dos conceitos de sistemas imunológicos de maneira a instaurar um sistema de detecção de intrusão (IDS) para a IoT e que também será útil para o modelo apresentado nesse papel, essa aplicação foi desenvolvida por Liu et al [10]. De acordo com o mecanismo proposto pelos autores, as células de defesa do sistema imunológico artificial denotadas por detectores devem possuir a capacidade de evoluir, aprender e se renovarem de maneira dinâmica ao contrário de outros trabalhos que utilizaram meios estáticos de análise e não são muito eficientes em ambientes dinâmicos. O objetivo é praticamente o mesmo de [8] e decidir se o fluxo de informação é normal ou anormal, porém em [10] o mecanismo é melhor elaborado e provavelmente terá um melhor resultado em ambientes maleáveis. A vantagem de [10] sobre [8] se da ao fato deste último utilizar uma abordagem fixa de lógica fuzzy, o que provavelmente terá um grande impacto na prática.

Foram definidos pelos autores três tipos de detectores classificados como imaturo, maduro e de memória. É gerada uma população de detectores imaturos que serão treinados usando as informações da própria rede, ou seja, esses detectores usam as assinaturas dos datagramas da IoT para a análise. Os datagramas comuns e legitimos da rede IoT atual são classificados como partículas pertencentes ao próprio organismo, já datagramas ilegítimos ou maliciosos são interpretados como antígenos, ou partículas invasoras. Os detectores não devem combinar e atacar as próprias células do sistema, somente devem atacar células invasoras. Dessa forma a população de detectores imaturos vai sendo treinada de forma a descartar aqueles indivíduos que detectam partículas do próprio sistema e mantém aqueles que detectam apenas células invasoras. Quando esses detectores atacam somente as partículas estranhas eles se tornam detectores maduros. Não ficou muito claro como os autores treinaram as células, porém essa forma de aprendizado é muito similar aos algoritmos genéticos ou o particle swarm optimization mencionado anteriormente.

A partir daí os próprios gerentes da rede IoT podem auxiliar no treinamento desses detectores incluindo mais datagramas de ataque á rede, até que estes estejam especializados o suficiente para que se tornem detectores de memória imortais. Os detectores maduros que não aprenderem a detectar grande número de ataques dado um intervalo de tempo morrem. Sempre que um detector maduro se torna um detector de memória todo o conhecimento desse detector é salvo numa biblioteca, e todas a as vezes que ele se combina com um antígeno conhecido ou desconhecido ele gera novas populações de detectores imaturos de forma criar novas células para aprimorar o aprendizado e defesa do sistema. A cada detecção um alarme também é enviado aos administradores da rede.

Através desse mecanismo é possível perceber que ele pode ter uma alta eficácia, mesmo se a estrutura da rede mudar, caso seja configurado de maneira adequada e astuta. Outra vantagem é o fato de ser mutável, e estar em constante desenvolvimento com o decorrer do tempo e ao estar imerso em uma variedade de ataques.

6. Sistemas bio-inspirados na IoT, e considerações de segurança

O ponto de convergência entre sistemas imunológicos ou outros sistemas bio-inspirados e a IoT se da no fato desta última necessitar fortemente de um sistema de defesa maleável e inteligente. Então a ideia de um mecanismo que funcione em larga escala e de maneira praticamente autônoma é muito atraente para engenheiros e projetistas de redes IoT.

Existirá bilhões ou trilhões de dispositivos no futuro fabricados por de diferentes empresas e com diversas tecnologias, cada um com endereçamento IP único. Todos comunicando entre si. A IoT será na verdade formada por milhões ou bilhões de "micronets"de diferentes dispositivos [1] e deverá ser agrupada numa abstração para que possa ser administrada de maneira mais fácil e segura. Isso ocorrerá devido ao processo natural de desenvolvimento da rede, em que diversas empresas irão competir pelo mercado da IoT, mas em um determinado momento algumas dessas redes terão que conversar entre si da mesma forma como diversas ISPs devem fazer ponte de comunicação umas com as outras. Para prover tal transparência e interoperabilidade seria possível a criação de um middleware como sugerido por [14], distribuídos em múltiplas nuvens e que opere sobre essa rede física de maneira virtual e acessível a todos os nós, para que assim se possa implementar protocolos e sistemas de segurança de maneira eficiente. Obviamente a infraestrutura também deve ser disponibilizada para que o middleware possa interagir com diversas redes que compõe o todo. Os dispositivos que tentarem acessar a rede IoT por fora dessa camada deve ser imediatamente destacado como um nó ilegal ou malicioso, se um dispositivo quer ingressar nessa camada ele deve através de um protocolo requisitar que seja cadastrado para usar o serviço do middleware temporariamente . Assim como células do corpo são identificadas por alguns receptores químicos específicos e patógenos por outros, a camada virtual deve, assim como um organismo vivo, saber reconhecer suas próprias células e outras invasoras. Logo um dispositivo desconhecido não poderia se comunicar diretamente com outro dispositivo legítimo sem a aprovação prévia do sistema. O acesso a cada dispositivo portanto deve ser regulado, visto que se for permitido que nós sem registro interajam na rede de qualquer forma isso poderá causar sérias ameças à privacidade e até mesmo à vida das pessoas dependendo da área em que a IoT está sendo usada. Com o advento de carros inteligentes e incorporados à rede Internet nos últimos anos, por exemplo, provaram que é sim possível burlar as segurança de tais sistemas e manipular mecanicamente o automóvel por meio de atuadores. Podendo ser usado como ferramenta para atentados à vida dos usuários. Um grande esforço de toda a comunidade de fabricantes e pessoas que irão padronizar a IoT em conjunto com os governos de cada país deve ser realizado para lidar com esses sérios problemas de maneira contundente e sincronizada.

A comunicação entre as máquinas e usuários deve ser obscura [1] para impedir acessos indevidos e roubo de informações, exceto para as entidades reguladoras do sistema que poderiam ter uma visão um pouco mais completa de todo o sistema via SDN ou outro meio de virtualização, mesmo assim algum mecanismo tecnológico ou leis deveriam ser desenvolvidos para impedir o uso abusivo das informações pessoais em âmbito de negócios. As pessoas devem ter o direito de escolher se querem ou não, e quais informações a seu respeito, desejam que sejam compartilhadas ou vendidas. Limitando assim abusos por parte das empresas que estão fornecendo os serviços. No caso de ameaças externas, se um usuário maligno quiser compreender a rede para desenvolver um ataque ele terá muito mais dificuldade pois a rede deverá ser um emaranhado de endereços que não são fixos e não são rastreáveis por vias comuns.

De acordo com o que foi mostrado anteriormente a IoT necessita de um sistema imunológico capaz de conter ameças e ao mesmo tempo prover um sistema elaborado de administração da rede, o sistema poderia ser composto por várias camadas de controle assim como em [8], porém devido à complexidade da IoT será necessário mais camadas

para diminuir a complexidade do sistema e prover maior modularização para que diversos provedores ou empresas que atuem no ramo da IoT possam inserir seus módulos no rede de forma autêntica.

7. O modelo proposto

7.1. Ideias gerais

O modelo apresentado aqui será um modelo em camadas, com algoritmos híbridos executando numa virtualização e dispositivos eletrônicos integrados numa malha de hardwares. Uma camada global seria criada e armazenada em grandes nuvens distribuídas em um território físico (o grande organismo), como um país ou uma cidade. Esse grande organismo distribuído seria composto por milhares ou milhões de sub-áreas também chamadas de células, as quais seriam compostas por organelas (fazendo analogia ao sistema biológico) ou dispositivos de hardware que integram a IoT. Então o middleware seria implementado em cada uma dessas células para fazer a intermediação entre a grande nuvem e os dispositivos e também na comunicação de dispositivo para dispositivo. Esse middleware poderia ser implementado em diversas estações poderosas em várias partes da célula. Então se um dispositivo dentro de uma célula quiser conversar com um dispositivo em outra célula, essa comunicação deve ser intermediada via middleware e o grande organismo. No caso de dispositivos com pouca capacidade computacional e energia, como sensores ou eletrodomésticos mais simples, que se comuniquem com alguma entidade externa, essa comunicação deve ser intermediada por gateways do fabricante com autorização para operar dentro da célula vigente e a partir dai os clientes ou provedores de serviço autenticados poderão acessar as informações desses dispositivos. Tal controle é necessário apesar de parecer caro tanto financeiramente quanto computacionalmente, pois ao observar a segurança da Internet percebe-se que está é frágil e responsável por grandes danos físicos ou financeiros a pessoas ou empresas quando há ataques cibernéticos ou ocorrência de cibercrime. A própria criminalidade da dark web demonstra que não há controle. Porém não se pode comparar a Internet com a IoT, nesta última a situação de segurança será muito mais frágil e delicada, pois está muito mais próxima do cotidiano e da intimidade das pessoas. De certa forma será até mesmo invasiva se as autoridades competentes não tomarem os devidos cuidados. Pessoas mesmo sem querer utilizar a IoT, vão estar imersas num mundo do qual elas não poderão fugir. A proporção de tais sistemas exigem um novo paradigma de segurança. Diferente da Internet que a pessoa podem tomar decisões para tornar o uso mais seguro ou até mesmo não usar. Criar esse sistema que englobe a IoT de forma modularizada, segura e eficiente será com certeza um grande desafio para engenheiros e projetistas de redes no futuro, caso seja provado por futuras pesquisas que este seja um caminho a ser percorrido. E dado a quantidade de dados que será gerada pela IoT, cada célula dessas junto com suas estações computacionais podem funcionar como centros de processamento do Big Data gerado pelos dispositivos além de fazer o roteamento e controle de segurança.

Nesse modelo em camadas, caso um dispositivo autônomo ou controlado por um usuário quiser conversar com outro dentro da mesma célula como por exemplo o relógio de pulso de um indivíduo e o estabelecimento em que ele está inserido, o relógio então envia uma mensagem para o estabelecimento tentando estabelecer uma comunicação e este, em resposta, entra em contato com o middleware para exigir informações sobre o IP do relógio

e saber se este é um dispositivo legítimo da rede, mas para isso o próprio estabelecimento precisa provar que também é autentico ao enviar seus tokens de segurança criptografados. A célula como reconhece todas suas organelas responde para o estabelecimento, enviando-lhe uma sequência de tokens de segurança criptografados que ele usará para confirmação da identidade do relógio, pois somente o endereço de IP do relógio não é o suficiente para provar que ele é legitimo visto que um endereço de IP pode ser falsificado dentro de um pacote mal intencionado. Então o estabelecimento pergunta para o relógio qual é sua sequência de autenticação, se o relógio responder corretamente significa que ele é realmente uma organela reconhecida pela célula, e não uma clonada, então a partir desse momento a comunicação entre relógio e estabelecimento segue ininterrupta sem precisar ser intermediada até surgir algum imprevisto, expiração de sessão ou falha de autenticação.

Mas o contrário também é possível, por exemplo, como um restaurante que envia anúncios de preços e promoções às pessoas, através de seus dispositivos vestíveis, mobiles, ou carros que passam pelas redondezas do estabelecimento. O restaurante vai detectar diversos novos endereços de dispositivos que estão ao seu alcance e pedir ao middleware que envie suas mensagens via broadcast aos usuários que permitiram comunicação automática. No âmbito da tecnologia mobile, a comunicação seja automática ou determinada pela pessoa deve ser gerida por meio de uma interface que detecta todos os dispositivos dentro de um raio físico da rede e em seguida perguntar para o usuário com qual dispositivo ele deseja se comunicar. O usuário poderia também decidir receber comunicações automáticas desde que legítimas.

Existe então a necessidade de criar um sistema de tokens ou chaves de autentificação que sejam fáceis de processar em nível de hardware da IoT, entretanto que expirem brevemente após cada comunicação. Dessa forma tornamos as identidades dos dispositivos altamente voláteis e de difícil rastreamento por entes malignos, tentando assim preservar a identidade dos elementos dentro de cada célula. Porém estudos e experimentos devem ser realizados para explorar como a eficiência e a sobrecarga causada na rede irão se comportar com a adição desses pacotes de autenticação nas comunicações.

A comunicação entre máquinas mais simples deve ser obrigatoriamente intermediada por gateways do proprietário, desde que a segurança desses dados seja necessária. Como por exemplo um fabricante de máquinas de lavar roupa ou outros eletrodomésticos que funcionem com comando de voz, como mencionado por [1] esses dispositivos irão coletar dados de som e voz de qualquer tipo das pessoas, isso inclui conversas pessoais, informações de negócios e muitas outras coisas que podem ser usadas contra essas pessoas ou com intuito de obter vantagens comerciais. Logo um fabricante que afirme que seu produto é seguro deve inserir um meio de acesso seguro à essas máquinas de forma que a comunicação com elas ainda seja possível, mas de maneira anônima e com menos probabilidade dos dados serem desviados e roubados.

Novas tecnologias que irão surgir num futuro não muito distante e que já estão começando a serem testadas em laboratório, prometem sistemas eletrônicos de transmissão RF com altíssima capacidade de comunicação e com gastos baixíssimos de energia. Essas tecnologias são descritas na parte 8 desse papel. Assim o mecanismo de autenticação descrito acima usando vários tokens, que poderia não ser adequado para dispositivos que funcionam à bateria, ou que transitem pelos backbones arcaicos da rede, assume uma nova

feição e possibilidade. A IoT deve ser projetada olhando-se para o futuro, visando um aperfeiçoamento da infra-estrutura atual, onde a segurança será mais importante do que os custos energéticos e computacionais. Obviamente isto não deve implicar num comportamento negligente por parte dos projetistas, deve-se continuar os esforços por sistemas cada vez mais eficientes em termos de energia e processamento.

7.2. Estrutura do modelo

Para o advento de uma rede obscura e de difícil mapeamento por entidades externas poderia então ser criado um mecanismo usando o EDM como base para construção da segurança, elaborado em [6], de forma a ser o regente de cada célula. Entretanto esse novo mecanismo deve ser ampliado para sanar suas limitações adicionando módulos de aprendizado que implementem o AG, PSO ou outras técnicas bioinspiradas mencionadas anteriormente. Também deve ser construído junto a um sistema de detecção de intrusão baseado em sistemas imunológicos híbridos para que se possa fazer detecção eficiente de ataques. Saber quando ocorrem e quais tipos de ataques estão sendo efetuados na célula, Butun et al [21] cita diversos outros métodos, além de inteligência artificial, que podem ser utilizados para a construção de IDS.

Dispositivos de hardware também serão necessários ao sistema. Tal modificação e ampliação do mecanismo seria implementada e executada no middleware e sobre as topologias físicas. Essa modificação será referida nesse papel como SCUDS (Syntetic Cortex for Ubiquitous Defense System). Dessa forma esse mecanismo poderá alterar o endereçamento de IP das organelas ou os caminhos de roteamento assim que um patógeno ou comportamento malicioso seja detectado nos arredores da célula pelo IDS e aumentar seu conhecimento a cada novo ataque através de uma “consciência de segurança evolutiva”das células de defesa. Contudo não é necessário alterar o endereçamento de todas as organelas numa célula, somente o subgrupo mais afetado, visto que isso poderia causar uma sobrecarga na rede caso um ataque tenha justamente esse propósito, forçar que a rede se reconfigure múltiplas vezes. Logo mecanismos de detecção de ataques desse tipo devem ser adicionados ao IDS. Mas no caso de um ataque que não seja do tipo anterior, como todos os dispositivos estão em constante contato com suas células, o endereçamento e rotas podem ser repassados e remodelados de forma a isolar a ameaça e dificultando dessa forma ataques a determinados dispositivos em específico ou à toda rede. O mesmo pode ser feito para evitar ataques às estações onde os middlewares residem, instaurando um mecanismo SCUDS no grande organismo de maneira recursiva. Tal sistema é ilustrado na Figura 1, a seguir.

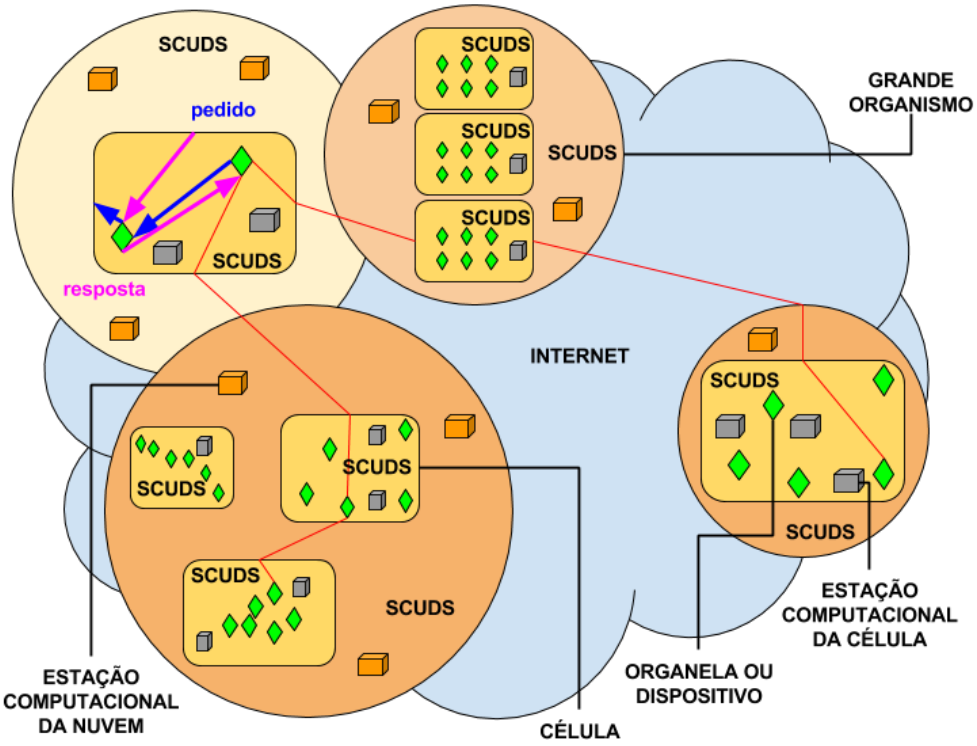

Figura 1. Sistema Imunológico em camadas

Como já mencionado, atributos físicos de infraestrutura também farão parte do SCUDS para permitir a sinergia de todo o sistema. Múltiplos dispositivos conectados à IoT baseados em FPGA (Field Programmable Gate Array) ou então em circuitos dedicados poderiam ser espalhados na borda das células com dois objetivos principais, de acordo com [15] tais dispositivos poderiam ajudar no processamento de dados para aliviar o peso computacional dos dispositivos da IoT, como por exemplo criptografia ou outras funções como implementar um sistema operacional para dispositivos menos capazes, e de acordo com [16] para proteção da privacidade dos usuários. Comunicação anônima e autenticada de maneira eficiente podem ser obtidas ao mesmo tempo de acordo com Emura et al [16] se a infraestrutura utilizar proxy's para intermediar a comunicação entre o provedor de serviços e os usuários, e então esconder o verdadeiro IP do usuário ou dispositivo por trás do endereço das proxy's. Dessa forma se utilizarmos um circuito em FPGA ou outro maquinário dedicado para intermediar comunicações dos dispositivos, usando métodos similares ao de [16] no SCUDS , com o resto da Internet ou provedores de serviço diversos a anonimidade seria conferida aos dispositivos e a privacidade das pessoas teriam uma melhoria de segurança. Dessa forma se um indivíduo está sempre circulando por uma determinada região, seu dispositivo não poderá ser associado a ele pois estará mascarado pela proxy. É importante salientar que a anonimidade se da entre usuário e o provedor de serviços ou a Internet propriamente dita, e não necessariamente ao SCUDS. Logo se um criminoso estiver tirando proveito dessa anonimidade poderá ser descoberto com pedidos judiciais de entidades da lei à empresa que implementou a arquitetura SCUDS na região, e dessa forma realizar investigações na célula onde ocorreu o incidente. A célula contendo os dispositivos de hardware é ilustrada na figura 2, a seguir.

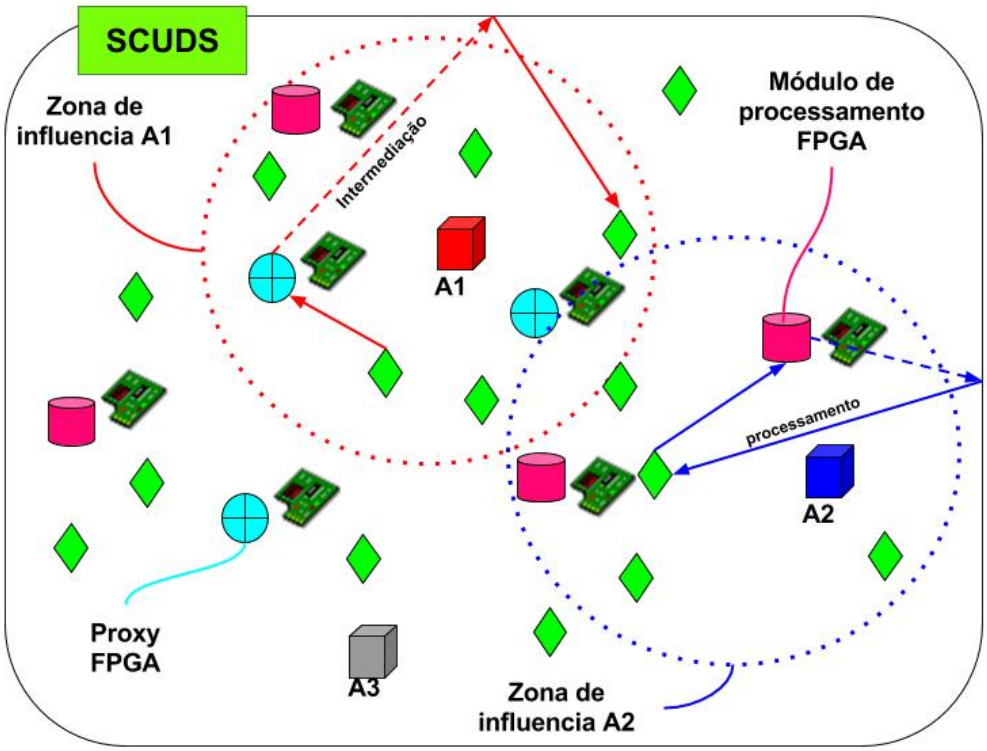

Figura 2. Dispositivos de hardware dentro de uma célula SCUDS

Tráfegos oriundos da Internet para dentro do grande organismo devem ser analisados da mesma forma que foi feito em [8], barrando comportamentos indesejados e permitindo aqueles considerados normais. Como todos os dados devem ser filtrados pelas células do sistema uma grande infra-estrutura será necessária para evitar gargalos na rede. Um controle de tráfego também pode ser instaurado para redirecionar o tráfego entre células próximas. Nada impede que existam redes IoT paralelas àquelas implementadas sob a arquitetura SCUDS e com acesso direto à Internet. Talvez para alguns tipos de aplicações isso seja mais apropriado, mas se segurança for um fator crucial para a rede a ser implementada, então técnicas similares ou melhores devem ser pesquisadas e empreendidas. A arquitetura SCUDS tem o propósito de funcionar como um *framework*, ou como uma padronização de sistemas de segurança IoT.

Uma tendência que parece prometer segurança de hardware no caso de interceptação física do dispositivo são as *physical unclonable functions* (PUFs), essas tentam garantir a integridade do software embarcado em um dispositivo no momento do boot da CPU ou outras funções críticas do dispositivo. Tais funções poderiam ser integradas aos dispositivos de infraestrutura do SCUDS e nos dispositivos commodities da IoT por parte dos fabricantes. As PUFs são funções que calculam uma chave única para fazer a criptografia dos dados usando características físicas complexas dos circuitos integrados (ICs) como temperatura, delay em transistores e circuitos lógicos entre outros. O que torna a PUF mais segura é o fato dessa informação não ser armazenada em memórias não voláteis, elas retornam um valor que depende do funcionamento interno do chip e é derivada quando o circuito é alimentado por energia. Em [17] os autores criaram uma PUF que calcula a chave de criptografia utilizando um componente eletrônico que lê o reflexo da onda de

luz emitida por LEDs em uma película plástica, o reflexo determina um aspecto único do material quando a onda eletromagnética atravessa o meio translúcido. A chave é única pois o processo de fabricação garante que as pequenas variações em cada película guie o reflexo da onda de maneira diferente. Como é praticamente impossível, ainda, produzir duas películas de plástico 100% iguais a nível atômico, os resultados serão sempre diferentes. No caso de [17], antes do sistema embarcado realizar o boot a chave é derivada pela PUF e entregue a um coprocessador de segurança implementado ao lado da CPU numa FPGA que então faz a autenticação do software que se encontra na BIOS e autentica outras partes que também são necessárias, quando todos os componentes cruciais são autenticados como originais o boot é liberado e a CPU assume o controle. O software em questão deve ser introduzido na BIOS já criptografado pela chave da PUF, provavelmente implementado durante a fabricação do dispositivo.

Existe também a possibilidade de um dispositivo ser clonado em nível de software e tentar coexistir na camada de rede, isso poderia ser impedido caso houvesse o contato frequente entre cada célula e suas respectivas organelas como comentado anteriormente. Dessa forma uma sequencia de pequenos tokens de autenticação criptografados seriam distribuídos, através de um protocolo específico da arquitetura SCUDS, para cada dispositivo ao ingressar na rede e com atualizações num intervalo de tempo aleatório. A cada recebimento de um token, o dispositivo deve responder para a célula mãe qual era o token anterior. Caso o dispositivo seja incapaz de realizar essa tarefa ele será automaticamente incluído na lista de patógenos, salvando o máximo de informações possíveis desse evento incluindo o endereço físico se disponível na arquitetura do sistema. Para dificultar ainda mais a interceptação desses tokens, a célula SCUDS poderia ter um roteamento interno aleatório, porém mapeado na estrutura interna, das mensagens de forma que a cada momento é um host (dispositivo de borda) diferente que envia um token e faz a requisição para o dispositivo. Agora, se o dispositivo nunca esteve ligado na rede e nunca possuiu um endereço IP local ele envia uma mensagem de CLAIM_TOKEN para a rede. Então a célula mãe atribui para esse dispositivo um novo endereço de IP disponível naquela rede e resume o envio dos tokens para a nova organela filha. Dessa forma se um indivíduo mal intencionado tentar clonar um dispositivo que já está em funcionamento a um bom tempo, ele teria que saber a sequencia de tokens que aquele dispositivo armazena (supondo que tais informações estejam seguras em nível de hardware). O protocolo da arquitetura SCUDS deve de alguma forma garantir que um outro indivíduo não autenticado seja proibido de pedir para outros dispositivos enviar seus tokens de segurança. Porém maiores estudos e experimentos empíricos deveriam ser feitos para validar ou aperfeiçoar tal mecanismo de segurança. O sistema de autenticação é ilustrado na figura 3 a seguir.

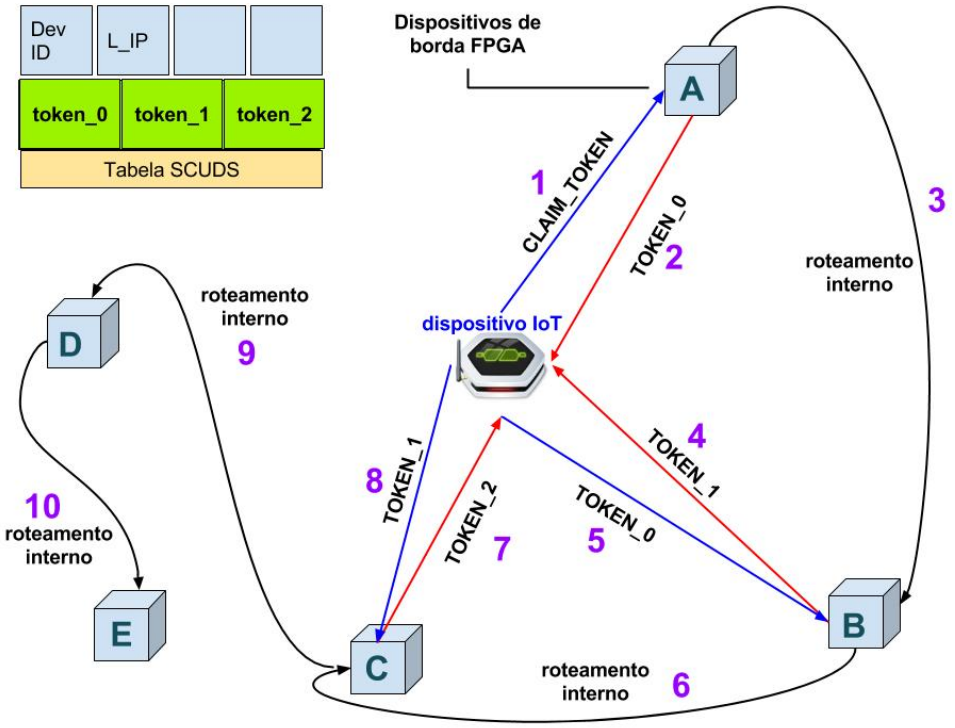

Figura 3. Identificando dispositivo com protocolo SCUDS

8. Avanços tecnológicos e novas possibilidades

Novas tecnologias de fabricação de CMOS usando como matéria prima diferentes alótropos do carbono, grafeno e nanotubos de carbono, prometem uma revolução tanto na fabricação de componentes eletrônicos como na IoT. Esses componentes irão funcionar em nível molecular, um nível superior aos circuitos quânticos (nível de átomo) do futuro, como os transistores moleculares de grafeno (G-FETs). Grafeno é uma estrutura em que uma única camada de átomos de carbono formam um retículo cristalino bidimensional, ou seja é um plano que se assemelha a uma colmeia de abelhas cuja espessura é a espessura de um átomo de carbono. A grande vantagem dos circuitos integrados feitos com esses materiais será o fato de trabalharem com um baixíssimo nível de energia por terem uma mobilidade de elétrons superior ao silício (Si) [18], principalmente no caso do grafeno, além de possibilitar fabricar dispositivos transparentes e flexíveis. Com um baixo consumo de energia a quantidade de aplicações na IoT tornam-se imensuráveis, protocolos de comunicação mais elaborados e de comunicação frequente para dispositivos à bateria podem ser desenvolvidos com altas capacidades de transmissão em transmissores de RF, “ultra-high-data rate mobile communications systems”[18], possivelmente atribuindo uma nova face às tecnologias como ZigBee, Blutooth e outras, ou então o surgimento de tecnologias completamente inovadoras. Toda uma nova gama de sensores irão emergir. Bio-sensores baseados em carbono instalados em cidades ou implantados em seres humanos poderiam detectar surtos de doenças como o ebola ou cólera com antecedência em vários países, especialmente os mais pobres e com condições insalubres de vida, e assim melhor mapear a proliferação e impedir o avanço para regiões mais críticas. Alguns trabalhos propostos como [19] tentam validar essa ideia ao tentar detectar bactérias

como a *Escherichia coli* e mostram que isso será possível no futuro. O desenvolvimento de novos cenários e tecnologias antes impossíveis pela restrição de tamanho e de energia começam a entrar no reino das possibilidades. Porém as dificuldades atuais de fabricação de G-FETs e CNT-FETs (nanotubos de carbono) e outros problemas físicos que ainda devem ser pesquisados mostram que essa tecnologia ainda vai levar um tempo até atingir sua maturidade, mas com certeza é uma promessa para a era pós-silício e para a IoT. A tecnologia dos G-FETs irá permitir também o aparecimento de dispositivos vestíveis na IoT que precisam ser ao mesmo tempo maleáveis e com alta capacidade de comunicação wireless, circuitos e antenas flexíveis construídos pela deposição de grafeno sobre substratos de poli-imida para receptores RF já estão sendo atualmente testados [20]. Outra tecnologia que poderia auxiliar numa melhor "vigilância"das organelas pelo SCUDS é a tecnologia Li-Fi que promete ser muitas vezes mais rápida do que a tecnologia wireless atual, essa tecnologia já testada usa LEDs ou lasers de alta intensidade para modular a luz de forma que essa emita padrões binários que são captados do outro lado por placas solares que convertem a luz em sinais elétricos. A ideia principal é utilizar as luzes que já existem em grande parte da infra-estrutura humana atual e que existirão no futuro para transmitir dados em grande escala.

9. Trabalhos futuros

Pretende-se estudar mais a fundo como aprimorar, testar e validar o modelo SCUDS, inclusive o protocolo de autenticação da arquitetura mencionado no texto. Realizar experimentos, simulações e implementações práticas de modelos para conferir a eficácia do sistema e fazer eventuais modificações conforme a continuação da pesquisa mostre que é necessário.

10. Conclusão

Neste papel foi discutida a aplicação de alguns métodos bio-inspirados que podem ser aplicados à segurança e a auto-configuração da rede IoT, alguns possuem qualidades que afetam o sistema diretamente e outros indiretamente como, por exemplo, os sistemas imunológicos artificiais e algoritmos genéticos respectivamente. Foi apresentado algumas das maiores dificuldades e desafios de se prover segurança à rede IoT, que com toda certeza será alvo de inúmeros perigos e ataques no futuro tanto em nível de software quando em hardware. Foi proposto um modelo teórico chamado SCUDS (Sytentic Cortex for Ubiquitous Defense System) que basicamente é uma amálgama de diversas técnicas, mecanismos e dispositivos de hardware que tentam englobar partes da IoT e sanar diversas vulnerabilidades, de forma a criar uma camada protetora que evolui como um organismo vivo ao longo do tempo, adaptando-se a condições adversas e alterações de topologia. O objetivo principal desse papel não é comprovar que esse modelo realmente funciona na prática, mas demonstrar que um sistema que forneça verdadeira segurança precisa e deve ser um sistema híbrido, composto por várias partes inteligentes e adaptáveis para vencer grande parte dos diferentes desafios encontrados. Métodos simplistas tendem a falhar em ambientes complexos, ou solucionam apenas parte do problema, como por exemplo o modelo EDM [6] sem um excelente sistema de IDS não teria bom desempenho, assim como as técnicas de IDS de [8, 9,10, 22] que também não iriam solucionar os problemas gerais das redes se operassem de maneira independente.

Novas tecnologias virão para validar ideias cada vez mais complexas e eficientes. Entretanto, nenhum sistema de segurança é completamente seguro. Muitas ameaças e problemas à segurança e funcionamento da IoT ainda devem ser melhor explorados. Existem muitas brechas e possibilidades de surgirem infindáveis "buracos de segurança"de maneira inusitada devido a falta de padronização da IoT e que podem não ser previstos em tempo de desenvolvimento de toda a arquitetura. Mas isso não deve ser visto como algo desanimador, novos mecanismos e formas de criar as redes devem continuar a serem pensadas levando em conta o tamanho e dinamismo das redes do futuro. O modelo SCUDS com certeza não é perfeito e deve ser posto à prova através de experimentos elaborados, porém as inspirações de origem natural provaram serem uma boa fonte de criatividade e inspiração e uma tendência para resolver os problemas do futuro. Talvez as técnicas atuais não sejam boas o suficiente, mas sistemas inteligentes que aprendem são a aposta para o futuro.

Referências

[1] Fink, G.A.; Zarzhitsky, D.V.; Carroll, T.E.; Farquhar, E.D., *"Security and privacy grand challenges for the Internet of Things"*, Collaboration Technologies and Systems (CTS), 2015 International Conference on Year: 2015, Pages: 27 - 34, DOI: 10.1109/CTS.2015.7210391, IEEE Conference Publications.

[2] Burange, A.W.; Misalkar, H.D.,*"Review of Internet of Things in Development of Smart Cities with Data Management & Privacy"*, Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in Year: 2015, Pages: 189 - 195, DOI:10.1109/ICACEA.2015.7164693, IEEE Conference Publications.

[3] Dongliang Duan; Liuqing Yang; Yang Cao; Jiaolong Wei; Xiang Cheng,*"Self-Organizing Networks: From Bio-Inspired to Social-Driven"*, Intelligent Systems, IEEE, Year: 2014, Volume: 29, Issue: 2, Pages: 86 - 90, DOI: 10.1109/MIS.2014.27, Cited by: Papers (2), IEEE Journals & Magazines.

[4] Hasnat, M.A.; Akbar, M.; Iqbal, Z.; Khan, Z.A.; Qasim, U.; Javaid, N.,*"Bio inspired distributed energy efficient clustering for Wireless Sensor Networks"*, Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on Year: 2015, Pages: 1 - 7, DOI: 10.1109/NSITNSW.2015.7176429, IEEE Conference Publications.

[5] Basu, S.S.; Tripathy, S.; Chowdhury, A.R.,*"Design challenges and security issues in the Internet of Things"*, Region 10 Symposium (TENSYMP), 2015 IEEE, Year: 2015, Pages: 90 - 93, DOI:10.1109/TENSYMP.2015.25, IEEE Conference Publications.

[6] Haifeng Zhou; Chunming Wu; Ming Jiang; Boyang Zhou; Wen Gao; Tingting Pan; Min Huang,*"Evolving defense mechanism for future network security"*, Communications Magazine, IEEE Year: 2015, Volume: 53, Issue: 4, Pages: 45 - 51, DOI: 10.1109/MCOM.2015.7081074, IEEE Journals & Magazines.

[7] Salvato, M.; De Vito, S.; Guerra, S.; Buonanno, A.; Fattoruso, G.; Di Francia, G.,*"An adaptive immune based anomaly detection algorithm for smart WSN deployments"*, AISEM Annual Conference, 2015 XVIII, Year: 2015, Pages: 1 - 5, DOI: 10.1109/AISEM.2015.7066840, IEEE Conference Publications.

[8] Elhaj, M.M.K.; Hamrawi, H.; Suliman, M.M.A.,*"A multi-layer network defense system using artificial immune system"*, Computing, Electrical and Electronics Engineering (ICCEEE), 2013 , International Conference on Year: 2013, Pages: 232 - 236, DOI: 10.1109/ICCEEE.2013.6633939, IEEE Conference Publications.

[9] Caiming Liu, Yan Zhang, Huaqiang Zhang, *"A Novel Approach to IoT Security Based on Immunology"*, 2013 Ninth International Conference on Computational Intelligence and Security.

[10] Caiming Liu; Jin Yang; Yan Zhang; Run Chen; Jinquan Zeng, *"Research on immunity-based intrusion detection technology for the Internet of Things"*, Natural Computation (ICNC), 2011 Seventh International Conference on Year: 2011, Volume: 1, Pages: 212 - 216, DOI: 10.1109/ICNC.2011.6022060, Cited by: Papers (3), IEEE Conference Publications.

[11] Falko Dressler , Ozgur B. Akan,*"A survey on bio-inspired networking"*, ELSEVIER, 29 January 2010.

[12] José Antonio Sánchez Guerrero, Lizet Liñero Suárez, Ricardo Ribeiro Gudwin, *"Análise da Importância de Parâmetros em um Algoritmo Genético por meio de sua Aplicação no Aprendizado de uma Rede Neural"*, Anais do II ENIA, julho de 1999.

[13] Lobao da Silva Fre, G.; de Carvalho Silva, J.; Reis, F.A.; Dias Palhao Mendes, L., *"Particle swarm optimization implementation for minimal transmission power providing a fully-connected cluster for the Internet of Things"*, Telecommunications (IWT), 2015 International Workshop on Year: 2015, Pages: 1 - 7, DOI: 10.1109/IWT.2015.7224573, IEEE Conference Publications.

[14] Gamundani, A.M.,*"An impact review on internet of things attacks"*, Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on Year: 2015, Pages: 114 - 118, DOI: 10.1109/ETNCC.2015.7184819, IEEE Conference Publications.

[15] Gomes, T.; Pinto, S.; Gomes, T.; Tavares, A.; Cabral, J., *"Towards an FPGA-based edge device for the Internet of Things"*, Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on Year: 2015, Pages: 1 - 4, DOI: 10.1109/ETFA.2015.7301601, IEEE Conference Publications.

[16] Emura, K.; Kanaoka, A.; Ohta, S.; Omote, K.; Takahashi, T., *"Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation"*, Emerging Topics in Computing, IEEE Transactions on Year: 2015, Volume: PP, Issue: 99, Pages: 1 - 1, DOI: 10.1109/TETC.2015.2400131, IEEE Early Access Articles.

[17] Vai, Michael; Nahill, Ben; Kramer, Josh; Geis, Michael; Utin, Dan; Whelihan, David; Khazan, Roger, *"Secure architecture for embedded systems"*, High Performance Extreme Computing Conference (HPEC), 2015 IEEE, Year: 2015, Pages: 1 - 5, DOI: 10.1109/HPEC.2015.7322461, IEEE Conference Publications.

[18] Rodriguez, S.; Rusu, A.; de la Rosa, J.M., *"Overview of carbon-based circuits and systems"*, Circuits and Systems (ISCAS), 2015 IEEE International Symposium on Year: 2015, Pages: 2912 - 2915, DOI: 10.1109/ISCAS.2015.7169296, IEEE Conference Publications.

[19] Yogeesh, M.N.; Saungeun Park; Akinwande, D., *"Graphene based GHz flexible nanoelectronics and radio receiver systems (Invited)"*, Circuits and Systems (ISCAS), 2015 IEEE International Symposium on Year: 2015, Pages: 2916 - 2919, DOI: 10.1109/ISCAS.2015.7169297, IEEE Conference Publications.

[20] Akbari, E.; Buntat, Z.; Afroozeh, A.; Zeinalinezhad, A.; Nikoukar, A., *"Escherichia coli bacteria detection by using graphene-based biosensor"*, Nanobiotechnology, IET Year: 2015, Volume: 9, Issue: 5, Pages: 273 - 279, DOI: 10.1049/iet-nbt.2015.0010, IET Journals & Magazines.

[21] Butun, I.; Kantarci, B.; Erol-Kantarci, M. , *"Anomaly detection and privacy preservation in cloud-centric Internet of Things"*, Communication Workshop (ICCW), 2015 IEEE International Conference on Year: 2015, Pages: 2610 - 2615, DOI: 10.1109/ICCW.2015.7247572, IEEE Conference Publications

[22] Feng Gu, Julie Greensmit,Uwe Aicklein,*"Biologically Inspired Networking and Sensing: Algorithms and Architectures"*, DOI: 10.4018/978-1-61350-092-7.ch005

[23] Flauzac, O.; Gonzalez, C.; Hachani, A.; Nolot, F.,*"SDN Based Architecture for IoT and Improvement of the Security"*, Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on Year: 2015, Pages: 688 - 693, DOI: 10.1109/WAINA.2015.110, IEEE Conference Publications.