República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) PI 0808619-2 A2

(22) Data de Depósito: 19/03/2008
(43) Data da Publicação: 12/08/2014
(RPI 2275)

(51) Int.Cl.:
H04L 29/06
H04L 12/22

(54) Título: MÉTODO E PROGRAMA DE COMPUTADOR PARA RASTREAMENTO DE PACOTES EM REDES SEM FIO OU REDES DE SENSORES

(57) Resumo:

(30) Prioridade Unionista: 30/03/2007 US 11/694,388

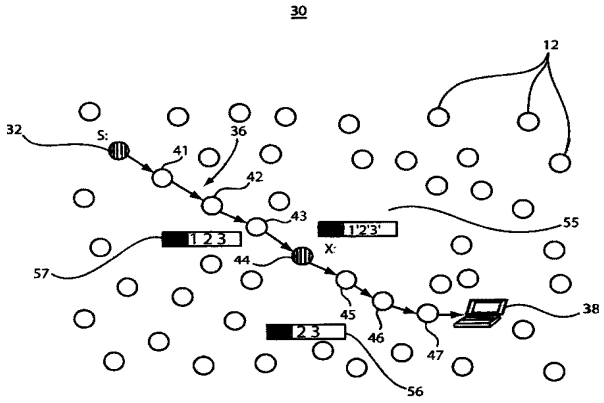
(73) Titular(es): INTERNATIONAL BUSINESS MACHINES CORPORATION

(72) Inventor(es): FAN YE , HAO YANG, ZHEN LIU

(74) Procurador(es): Ricardo de Andrade Bergamo da Silva

(86) Pedido Internacional: PCT EP2008053325 de 19/03/2008

(87) Publicação Internacional: WO 2008/119672de 09/10/2008



MÉTODO E PROGRAMA DE COMPUTADOR PARA RASTREAMENTO DE PACOTES EM REDES SEM FIO OU REDES DE SENSORES

CAMPO DA INVENÇÃO

A presente invenção refere-se às redes de comunicações e, mais particularmente a equipamentos e métodos de rastreamento em redes para identificar e evitar a injeção de dados falsos.

ANTECEDENTES DA INVENÇÃO

Rastreamento de pacotes é uma técnica para identificar a verdadeira origem de um pacote e o caminho que ele percorreu em uma rede. É amplamente utilizado para combater ataques de negação de serviço emergente (DoS), onde o endereço de origem de pacotes de ataque é geralmente "forjado" pelos atacantes para esconder suas identidades.

Existem numerosos esquemas de rastreamento de pacotes IP para a Internet com fios. Foi proposto, por exemplo, um esquema de marcação probabilística de pacote (PPM). Nos esquemas de PPM, com certa probabilidade, um roteador "marca" com algumas informações o pacote que o roteador passa para a frente. A informação porta/transmite a identidade do roteador, ou o link entre dois roteadores adjacentes. Depois de coletar as marcações de diferentes roteadores, o destino pode reconstruir o caminho que os pacotes percorreram.

Foi proposta uma abordagem algébrica onde a informação do caminho foi codificada em um polinômio f (x), cujos coeficientes são determinados pelas identidades dos roteadores ao longo de um caminho. Cada pacote carrega uma amostra x, e todos os roteadores ao longo de um caminho irão computar coletivamente f (x). Após a coletar suficiente pares de valores (x, f (x)), o destino pode derivar os coeficientes e, eventualmente, inferir as identidades dos roteadores.

Em outras técnicas, cada roteador é solicitado a armazenar os pacotes previamente enviados para um período de tempo prolongado. Ao consultar os roteadores se eles transmitiram um pacote no passado, o destino pode reconstruir o caminho de encaminhamento. Os roteadores também podem enviar mensagens de rastreamento fora de banda para a origem ou destino com pequena probabilidade. Coletar essas mensagens permite ao destino construir o caminho.

Estes esquemas foram concebidos sob um modelo de ameaça limitado, o que se torna insuficiente em muitas aplicações, por exemplo, em redes de sensores e malha sem fio. A maioria destas técnicas convencionais considera que os nós intermediários (roteadores) não estejam comprometidos. Isto pode não ser verdade, na realidade, especialmente em redes de sensores ou malha sem fio, onde os nós são vulneráveis à captura física e comprometimento. Nestes esquemas, mesmo um único nó intermediário comprometido pode impedir a verdadeira origem de pacotes de ser identificada.

O nó comprometido pode até forjar a marcação e enganar a vítima para que rastreie para origens incorretas arbitrárias.

Além disso, muitos esquemas exigem a coleta de um grande número de pacotes, ou que os nós intermediários armazenem grandes quantidades de traços de auditoria para identificar com precisão a localização de seus perpetradores. Estes podem não ser um problema na Internet, mas enfrentam graves obstáculos práticos em redes de sensores e malha sem fio, que tem recursos rigorosos de largura banda, energia e armazenamento.

REVELAÇÃO DO INVENTO

Um equipamento e método para rastreamento de pacotes em uma rede inclui a manutenção de um número de identidade (ID) para cada nó de uma rede e a geração de uma assinatura, por exemplo, um código de autenticação de mensagem (MAC), colocada em um pacote em cada nó de encaminhamento, de forma determinística ou probabilística, usando uma chave secreta compartilhada entre o nó de encaminhamento e uma pia. Ao receber um pacote, a pia verifica a veracidade das assinaturas (MACs) no pacote na ordem inversa em que as

assinaturas (MACs) foram adicionadas. A primeira assinatura inválida (MAC), revela um nó comprometido, que injetou um relatório falsos ou adulterados com um pacote legítimo durante o trajeto.

Um método para rastreamento de pacotes em uma rede inclui a manutenção de um número de identidade (ID) para cada nó de uma rede, a geração de uma assinatura em cada nó de encaminhamento usando uma chave secreta compartilhada entre este nó e uma pia, ao receber um pacote na pia, a verificação da veracidade das assinaturas de cada pacote pela pia na ordem inversa em que as assinaturas foram adicionadas e a determinação da validade da assinatura no caminho de transmissão para determinar a localização de uma fonte de injeção de dados falsos e / ou um nó comprometido em conluio.

Outro método para rastreamento de pacotes em uma rede de sensores ou malha sem fio inclui a manutenção de um número real de identidade (ID) para cada nó da uma rede, a computação de um ID anônimo do ID real com base em uma chave secreta conhecida apenas por um nó atual e uma pia, a geração de um código de autenticação de mensagem (MAC) usando a chave secreta para cada nó em um caminho de encaminhamento para marcar cada pacote com pelo menos duas probabilidades, o rastreamento do caminho de volta para descobrir fontes de injeção de dados falsos por meio de: determinação da identidade real do ID anônimo para os nós da rede, reconstrução de uma rota do nó usando marcas presentes em cada pacote, e verificação da exatidão do MAC de cada pacote de volta através de cada nó do caminho de transmissão usando a real identificação e a chave secreta para determinar o último MAC válido no caminho de encaminhamento.

Essas e outras características e vantagens serão visíveis a partir da seguinte descrição detalhada das concretizações ilustrativas da mesmo, que deve ser lido em conjunto com os desenhos que a acompanham.

BREVE DESCRIÇÃO DOS DESENHOS

A exposição irá fornecer detalhes da seguinte descrição das concretizações preferidas com referência às seguintes figuras onde:

A FIG. 1 é um diagrama que mostra um caminho de encaminhamento de nós em uma rede sem fio, de acordo com uma concretização;

A FIG. 2 é um diagrama que mostra uma janela limitada de números de seqüência atualmente em circulação para determinar se um número de seqüência de pacote recebido está dentro dos limites aceitáveis para verificar se o pacote é legítimo ou um "replay";

A FIG. 3 mostra uma rede ilustrativa tendo um caminho de encaminhamento através dela com fonte de colusão e moles de encaminhamento (por exemplo, nós comprometidos), que são detectados em conformidade com os princípios aqui presentes;

A FIG. 4 é um diagrama de bloco / fluxograma mostrando uma forma ilustrativa de reconstrução da ordem dos nós em conformidade com os princípios aqui presentes;

A FIG. 5 mostra um ciclo criado pela troca de identidade, que é detectável em conformidade com os princípios aqui presentes;

A FIG. 6 é um diagrama que mostra três categorias de nós;

A FIG. 7 é um diagrama que mostra um último nó com MACs válido em um caminho de encaminhamento;

A FIG. 8 é um gráfico que mostra resultados de análise de probabilidade de que as marcas de todos os n nós de encaminhamento são recolhidos após uma pia receber x pacotes;

A FIG. 9 é um gráfico que mostra os resultados da simulação de probabilidade de que as marcas de todos os n nós de encaminhamento são recolhidos após uma pia receber x pacotes;

A FIG. 10 é um gráfico que mostra o número médio de nós cujas marcas são coletados por uma pia nos primeiros x pacotes;

A FIG. 11 é um gráfico que indica a fonte de candidatos estabelecendo mudanças ao longo do tempo para um caminho de nó 40;

A FIG. 12 é um gráfico que mostra, em 100 corridas, quantas não funcionam para identificar de forma inequívoca a fonte como uma função do comprimento total do caminho, onde 200, 400, 600 e 800 curvas correspondem ao número de pacotes em cada corrida;

A FIG. 13 é um gráfico que mostra número médio de pacotes necessários para identificar de forma inequívoca a fonte como uma função do comprimento total do caminho, onde 800 pacotes são recebidos na pia em cada corrida, e

A FIG. 14 é um diagrama de bloco / fluxograma ilustrativo mostrando um equipamento / método de rastreamento e localização de mole de acordo com uma concretização ilustrativa.

DESCRIÇÃO DETALHADA DAS CONCRETIZAÇÕES PREFERIDAS

Em conformidade com as presentes concretizações, equipamentos e métodos são fornecidos que podem identificar com precisão a localização de nós agressores na presença de perpetradores múltiplos, coniventes. As presentes concretizações são particularmente aplicáveis para redes de sensores e malhas sem fio, onde a ameaça é mais grave e os recursos são mais rigorosos. Em contraste com a tecnologia anterior, as presentes concretizações trabalham na presença não só de nós comprometidos, mas também de nós encaminhamento comprometidos e identifica suas localizações.

Isto é mais do que adicionar autenticadores em marcações para impedir marcas falsificadas. Múltiplos nós comprometidos, coniventes, podem ainda enganar a vítima para rastrear a nós inocentes na técnica anterior. Em conformidade com os princípios presentes, o rastreamento resiliente é conseguido usando menos recursos, e o rastreamento pode ser alcançado até o perpetrador utilizando apenas um único pacote.

Espera-se que muitas redes de sensores sem fio trabalhem em um ambiente possivelmente adverso, ou mesmo hostil. Devido às suas operações autônomas, é fácil para um adversário pegar fisicamente e comprometer nós sensores, obtendo seus dados armazenados, incluindo as chaves secretas. Estes "moles" comprometidos podem lançar vários tipos de ataques, um dos mais importantes sendo a injeção de dados falsos. Uma única *toupeira* pode injetar grandes quantidades de tráfego falso para inundar a pia, levando a falhas no aplicativo e desperdício de recursos de energia e de largura de banda ao longo do caminho de encaminhamento. Pesquisas recentes têm proposto uma série de esquemas para detectar e soltar essas mensagens falsas em rota. No entanto, eles são todos passivos, pois apenas mitigam os danos dos ataques. Eles não fornecem meios ativos para revidar e eliminar a causa raiz dos ataques.

A descrição seguinte trata do revide ativo, ou seja, como localizar moles em redes de sensores. Ao se conhecer os locais de toupeiras, as toupeiras podem ser isoladas ou removidas da rede, assim, erradicar a causa raiz do ataque.Localizar moles representa um grande desafio de pesquisa. Em primeiro lugar, em contraste com a Internet onde os roteadores são mais protegidos e relativamente mais confiável do que os hospedeiros finais, todos os nós sensores em uma rede de sensores são igualmente acessíveis pelo adversário e uniformemente desprotegidos. Qualquer nó pode transmitir pacotes, não há infra-estrutura relativamente confiável de encaminhamento que possa ser aproveitada. Em segundo lugar, as toupeiras pode pactuar. As toupeiras não só podem compartilhar suas chaves secretas, mas também manipular os pacotes de uma forma coordenada para encobrir seus rastros. Tais ataques manipulados são muito mais sofisticados do que simplesmente aumentar a quantidade de tráfego falso. Os sistemas de rastreamento existentes no Protocolo de Internet (IP) para a Internet não consideram essas toupeiras em conluio e tornam-se ineficazes sob tais ataques.

De acordo com concretizações particularmente úteis, é apresentado um esquema de marcação aninhado para localizar conluio de moles em ataques de injeção de dados falsos. A marcação de pacotes é empregada para deduzir a origem real dos pacotes: um nó marca sua identidade nos pacotes que transmite.

Mediante a coleta de tais marcas, a pia pode inferir a rota e, assim, os locais de origem do tráfego.

Embora a marcação de pacote tenha sido utilizada na Internet, a sua aplicabilidade contra conspiração de toupeiras de sensor, no entanto, nunca foi estudada segundo nosso conhecimento. Os esquemas de marcação para rastreamento de IP pode ser facilmente derrotado por uma toupeira de conluio intermediária, que danifica as marcas para esconder os verdadeiros locais de origem e a si própria, ou até mesmo levar a pia a rastrear nós inocentes.

O esquema de marcação aninhado atual suporta o rastreamento de um único pacote. Cada nó de encaminhamento marca os pacotes de forma aninhada tal que a sua marca proteja as marcas de todos os nós de encaminhamento anteriores. Ele garante que não importa como a toupeira de conluio manipule as marcas, tampouco revela a localização da fonte, ou a da sua própria.

A necessidade de segurança pró-ativa contra toupeiras em redes de sensores é examinada, no âmbito da marcação de pacote, em relação a vários ataques em conluio que as toupeiras possam lançar. A segurança da marcação do pacote inclui que a marcação aninhada seja tanto suficiente quanto necessária: se porções das marcas de nós anteriores não estiverem protegidas (como em muitos projetos aparentemente óbvios), existem ataques em que uma toupeira de conluio pode ocultar a localização da fonte e em dela mesmo, ou enganar a pia para o rastreamento de nós inocentes. A eficácia da marcação aninhada é mostrada aqui por meio de avaliações analíticas.

Um esquema de Marcação Aninhada Probabilística (ou PNM) de acordo com os presentes princípios obtém um rastreamento seguro e eficaz contra o conluio de moles utilizando duas técnicas, ou seja, marcação aninhada e marcação probabilística. A marcação aninhada suporta o rastreamento de um único pacote. Cada nó de encaminhamento marca os pacotes de forma aninhada tal que a sua marca proteja as marcas de todos os nós de encaminhamento anteriores. Ela garante que não importa como uma toupeira de conluio manipule as marcas, tampouco revela a localização da fonte, ou a sua própria. A marcação probabilística reduz a sobrecarga por pacote para atender os recursos limitados

dos sensores. Cada nó deixa uma marca com certa probabilidade, assim, um pacote carrega apenas algumas marcas. Diferente dos esquemas de marcação da Internet, onde uma nova marca pode substituir uma já existente, novas marcas são simplesmente anexadas ao pacote.

A eficácia e eficiência da PNM são demonstradas aqui por meio de avaliações analíticas e empíricas. A PNM tem um rápido rastreamento: dentro de cerca de 50 pacotes, a pia pode localizar uma toupeira até 20 saltos (roteadores) de distância. Ela praticamente impede as moles de lançarem ataques de injeção de dados eficaz, pois eles serão capturados antes de poderem injetar uma quantidade significativa de tráfego de ataque.

Um equipamento e método de Marcação Aninhada Probabilística (PNM) são fornecidos para que sejam seguros contra ataques em conluio. Não importa como moles coniventes manipulem as marcas, a PNM pode localizar as toupeiras, uma por uma. A marcação aninhada é tanto suficiente quanto necessária para resistir a ataques de conluio. A PNM tem também rápido rastreamento, por exemplo, dentro de cerca de 50 pacotes, ele pode rastrear uma toupeira até a 20 saltos de distância de uma pia. Isso praticamente impede qualquer ataque de injeção de dados: as toupeiras serão capturadas antes de terem injetado qualquer quantidade significativa de tráfego falso.

Concretizações da presente invenção podem assumir a forma de uma concretização totalmente de hardware, uma concretização totalmente de software ou uma concretização incluindo tanto elementos de hardware quanto de software. Em uma concretização preferida, a invenção é implementada em software, o que inclui, mas não está limitado a firmware, software residente, microcódigo, etc. Além disso, a invenção pode assumir a forma de um produto de programa de computador acessível a partir de um meio usável ou legível por computador que forneça o código do programa para uso por ou em conexão com um computador ou qualquer outro equipamento de execução de instruções. Para efeitos da presente descrição, um meio legível ou utilizável por computador pode ser qualquer aparelho que possa incluir, armazenar, comunicar, propagar, ou o transportar o programa para uso por ou em conexão com o equipamento,

aparelho ou dispositivo de execução de instruções. O meio pode ser um registro eletrônico, magnético, óptico, eletromagnético, infravermelho, ou equipamento de semicondutores (ou aparelho ou dispositivo), ou um meio de propagação. Exemplos de um meio legível por computador incluem semicondutores ou memória de estado sólido, fita magnética, disquete removível de computador, uma memória de acesso aleatório (RAM), memória somente leitura (ROM), disco magnético rígido e disco óptico. Exemplos atuais de discos ópticos incluem disco compacto - Read Only Memory (CD-ROM), disco compacto - leitura / gravação (CD-R / W) e DVD.

Um equipamento de processamento de dados adequados para a armazenar e / ou executar código de programa pode incluir pelo menos um processador acoplado direta ou indiretamente, a elementos da memória através de um barramento de sistema.

Os elementos de memória podem incluir memória local usada na execução efetiva do código do programa, o armazenamento de massa, e memórias cache que fornecem armazenamento temporário de pelo menos algum código do programa para reduzir o número de vezes que o código for recuperado do armazenamento de massa durante a execução. Dispositivos de entrada / saída ou de I / O (incluindo mas não limitados a teclados, monitores, dispositivos apontadores, etc.) podem ser acoplados ao sistema, quer diretamente quer através da intervenção dos controladores de I / O.

Adaptadores de rede também pode ser acoplados ao equipamento para permitir que o sistema de processamento de dados seja atrelado a outros ou sistemas de processamento de dados, impressoras remotas ou dispositivos de armazenamento através de redes privadas ou públicas intervenientes. Modems, modem de cabo e placas Ethernet são apenas alguns dos tipos disponíveis atualmente de adaptadores de rede.

Referindo-se agora aos desenhos onde os números representam os mesmos elementos ou similares e, inicialmente, a FIG. 1, uma rede de 10 inclui uma pluralidade de nós 12. Alguns nós 12 podem ser localizados como um caminho de encaminhamento 14. Cada nó 12 pode compartilhar uma chave (K)

com um nó sorvedouro (Pia) e manter um número de seqüência monotonicamente crescente. Quando um nó de origem (Fonte) A envia uma mensagem M, ele acrescenta sua identificação e número de seqüência e, em seguida calcula uma assinatura (por exemplo, um código de autenticação de mensagem). A fonte envia o pacote inteiro para um nó próximo de salto 1 e incrementa seu número de seqüência. Da mesma forma, o nó 1 acrescenta a sua identificação e número de seqüência, e ainda outra assinatura ao pacote, e em seguida, passa o resultado para o próximo salto e incrementa o seu número de seqüência. Eventualmente, o pacote chega ao nó de pia (pia). O pacote a chegar inclui a mensagem original M, bem como os IDs, números de seqüência e as assinaturas de todos os nós no caminho.

Através das identificações no pacote, o nó de pia (pia), sabe o caminho alegado que o pacote parece ter atravessado. Ele verifica esse caminho em ordem inversa, a partir do último nó de salto. Para cada nó no caminho, a pia usa a chave compartilhada com esse nó para recalcular a assinatura e verifica se a assinatura no pacote está correta. A pia também verifica se o número de seqüência é válido. Se ambas as verificações forem bem-sucedidas, ela continua a verificar o salto anterior. Eventualmente, a pia para se tiver verificado todas as assinaturas / números de seqüência corretamente, ou para na primeira assinatura incorreta / número de seqüência incorreto. Um nó agressor está na vizinhança de um salto do nó onde a pia para de verificar.

Como as assinaturas são calculadas e elas protegem a mensagem camada por camada, do mesmo jeito que uma "cebola" (uma camada de cada vez), nenhum nó pode forjar ou modificar a mensagem de saltos anteriores sem ser detectado. Como cada pacote carrega um número de seqüência de por salto, um perpetrador não pode repetir o tráfego legítimo passado sem ser detectado. Quando há vários nós em conluio, a localização do último perpetrador no caminho é descoberto primeiro, x, então o segundo ao último, e assim por diante. Enquanto esses nós continuarem a injetar mensagens falsas e manipular as marcações, as suas localizações serão descobertas uma por uma. Em contrapartida, as soluções existentes não lidam com nós intermediários

comprometidos, ou perdem a proteção quando vários nós comprometidos estão em conluio.

Em conformidade com os princípios presentes, de um regime de rastreamento resiliente é fornecido para se defender contra os ataques lançados em conluio por vários nós comprometidos. Cada nó de encaminhamento utiliza uma assinatura para proteger a sua própria marca, assim como as marcas de todos os nós de encaminhamento anteriores, de forma aninhada. Isto pode rastrear a localização do nó comprometido que estiver atacando, mesmo que haja conluio de nós. Em uma concretização, a marcação determinista é empregada. No entanto, como cada nó de encaminhamento deixa uma marca no pacote, podem resultar mensagens aumentadas e a sobrecarga na comunicação quando o tamanho da rede ficar grande. Portanto, em uma concretização alternativa, um esquema de marcação aninhada probabilística (PNM) é empregado, que pode reduzir a sobrecarga de comunicação por pacotes para um nível constante, preservando a segurança de defesa contra ataques de conluio.

Na concretização PNM, cada nó de encaminhamento marca o pacote com uma pequena probabilidade p. Como resultado, em um caminho de transmissão de n nós, um pacote só carrega n * p marcas, em média, ao invés de simplesmente n marcas do esquema de marcação aninhada alternativa. Embora aparentemente uma simples extensão, ela acaba por envolver-se mais devido a duas questões.

Primeiro, a simples extensão probabilística acima no esquema de marcação aninhada pode abrir uma brecha de segurança. Ela pode ser vulnerável a ataques ocorrendo seletivamente, em que um nó de encaminhamento comprometido pode enquadrar qualquer nó inocentes entre ele e a fonte verdadeira, ao atacar com um conjunto seletivo de pacotes. Para derrotar tais ataques seletivos, técnicas de anonimato podem ser empregadas para esconder as identidades do nó em suas marcas.

Em segundo lugar, cada pacote pode transportar apenas amostragens parciais de um caminho completo. Um método de reconstrução de caminho é fornecido ao destino para reconstruir o caminho, usando um pequeno número de

pacotes de ataque. O destino pode usar o caminho reconstruído para identificar os nós agressores.

Os presentes princípios podem trazer uma defesa muito mais forte do que os esquemas convencionais de marcação. As concretizações atuais podem resistir a vários ataques em conluio, incluindo os sofisticados ataques seletivos que ocorrerem, lançados por vários nós coniventes comprometidos para encobrir seus rastros. Em concretizações preferidas, os benefícios incluem a redução da sobrecarga de comunicação e escalabilidade melhoradas, o que o torna aplicável para escala média x ou mesmo para redes de grande escala.

Referindo-se novamente a FIG. 1, considere o caminho A-1-2 ...- Z-Z + L-...- tinta, em que A é a fonte. Cada nó 12 compartilha uma chave K com a pia, por exemplo, A tem K a, 2 tem K 2, e assim por diante. Além disso, cada nó mantém um número sequencial, que registra o número de pacotes que gerou ou enviou até agora. O número de seqüência é inicialmente zero quando o nó 12 é implantado, e incrementado de um sempre que o 12 nó enviar um pacote.

Cada nó 12 também mantém um número de seqüência de pacotes monotonicamente crescente. Quando A envia uma mensagem M, ele acrescenta a sua identidade e seu número de seqüência, calcula uma assinatura (por exemplo, introduziu um Código de Autenticação de Mensagem (MAC)), envia então o pacote M inteiro para o próximo salto. Cada salto semelhantemente acrescenta sua própria identidade, número de série e a assinatura antes que passar o pacote para o próximo salto. Quando o nó A tem uma mensagem M para enviar, ele acrescenta a sua identidade e o seu número de seqüência atual (seqnum), em seguida, calcula uma assinatura que protege toda a mensagem: A-> B: M_a = M|A| seqnum | H_ka(M|A|seqnum) onde H_ka (x) denota uma assinatura d e x usando KeyK_a, "|" denota concatenação. Este pacote todo pode ser denotado como M_a. A envia M_a para o próximo salto 1, e então incrementa seu número de seqüência seqnum. O Nó 1 executa operações semelhantes e envia o pacote seguinte para o nó 2: 1 -> 2:M_a|2| seqnum2 | H_k2(M_a|2|seqnum2) e assim por diante.

Em geral, por dois nós consecutivos Z, Z +1 no caminho, depois de Z enviar Mz para Z+1, Z irá enviar Mz+1 para o próximo salto como Mz+1=Mz|Z+1|seqnumZ+1|H_kz+1(Mz|Z+1|seqnumz+1). Quando a pia receber essa mensagem, a partir dos IDs de nó ela pode recuperar o caminho alegado que o pacote parece ter atravessado. Ela verifica esse caminho em ordem inversa dos pacotes anexados, a partir último nó.

Sem perder a generalidade, considere-se o caso em que a pia verifica o nó V. O nó tem a mensagem Mz+1 que é a seguinte: Mz|Z+1|seqnumz+1|H_kz+1(Mz|Z+1|seqnumz+1). Depois de recuperar a identidade Z+1, a pia primeiro verifica se a assinatura está correta, utilizando os conhecimentos de K_z+1. Em seguida, ela verifica se o número de seqüência seqnum z + 1 está correto. *****Para fazer isso, o coletor de 25 mantém uma janela deslizante de números de seqüência para cada nó. Esta é a personificação determinista marcação.

Referindo-se a FIG. 2 com referência continuou a FIG. 1, 12 para cada nó, uma janela atual 22 tem um limite superior máximo (ligada) e um limite inferior (mínimo). A parte superior max (ligado) é o número de seqüência máximo que tenha sido recebida a partir deste nó, eo limite inferior min () é o menor número de seqüência que ainda é válido para este nó. The window 22 maintains which valid and out-of-order sequence numbers are yet to be received. Cada pacote é suposto para ter um tempo máximo para permanecer na rede e esta vida útil máxima (T máx) é utilizado para atualizar a janela 22.

Inicialmente, o mínimo e o máximo são ambos O quando o nó 12 é implantado. Quando o coletor recebe um pacote com um número de seqüência de d a partir deste nó, existem três casos possíveis:

1) d min <: o número é inválido, uma vez que já expirou.

2) ≤ d min ≤ max: Se D não tenha sido recebida antes, então ele é válido e uma marca é definida para D, indicando que ele foi usado. A pia também min atualizações para o número de seqüência inferior ao válida que

não foi recebida. Se d tenha sido recebida (por exemplo, se D é marcado), no entanto, é uma repetição, assim, um inválido número sequencial.

3) d max>: Neste caso, o número é válido. Além disso, o coletor define max = d, e iniciar um temporizador associado com número de seqüência d. O temporizador expira depois de T max, que é o tempo de vida máximo de um pacote dentro da rede. Quando esse tempo expirar, o coletor de conjuntos min = D, por exemplo, todos os pacotes com número de seqüência inferior d deveria ter morrido na rede.

Um nó no caminho passa a verificação pia se e somente se sua assinatura está correta e seu número de seqüência é válida. Neste caso, a pia continua a verificar a hop anterior por recuperar o anterior hop ID e verifica a assinatura e número de seqüência. Eventualmente, a verificação pára quando todas as assinaturas / números de seqüência são verificados corretamente, ou um assinatura incorreta / inválido número seqüência é encontrado. Em qualquer caso, um nodo comprometido está localizado dentro de um um-hop de bairro, onde pára o coletor. Por exemplo, quando o coletor tem verificado corretamente todos A seqnuma). O| | seqnuma H (M | | |nós, incluindo o primeiro salto M A verdadeira fonte está localizada em um bairro de um hop de A. nó alternativa, se a qualquer hop, a assinatura ou número de série é inválido, um nodo comprometido está dentro de um bairro hop a partir do nó inválido. Por C_X H.| | | |exemplo, quando X hop verificar: X M_w O coletor de considerar C_X), pode concluir-se que um nó está| |que não corresponde H H (M _w ¬ X comprometida em um bairro hop nó de X. Ou seja, ou X é o autor (X forja um H lixo intencional), ou um de seus vizinhos, como Y é (por exemplo, Y pela H X da assinatura, mas deu a assinatura correta para sua própria mensagem).

A proteção de segurança oferecido inclui muitas características. Primeiro, um criminoso que adultera o tráfego legítimo pode ser detectado. Como a mensagem é protegido por assinatura, a camada por camada, um autor que modifique a mensagem fará a verificação da assinatura de todos os saltos anteriores falharem, a partir da nascente até à hop imediatamente anterior. Em

segundo lugar, um atacante que tenta injetar pacotes de ataque de negação de serviço não pode corretamente forja origens remotas, porque ele não tem conhecimento das chaves. O coletor pode acompanhar as informações deixadas por nós normais após o autor para rastrear a sua localização. Terceiro, porque a mensagem é protegido por um número sequencial por hop, um criminoso não pode repetir o tráfego legítimo anterior, porque não pode produzir assinaturas corretas para os números de seqüência incrementado em pacotes de idade. Par quando vários nós em conluio atacando o mesmo caminho, a localização do autor passado, que modifica o tráfego legítimo ou injeta tráfego falso, continuarão a ser identificado. O coletor pode ainda instruir os outros nós para se comunicar com os nós de ataque identificadas, e descobrir o resto de nós um autor por um.

Modelos e pressupostos: sistemas e modelos de ameaça são descritas, e uma taxonomia de ataques maliciosos é apresentada no âmbito do pacote de marcação.

Referindo-se a FIG. 3, um modelo de sistema é representado por uma rede de sensores estáticas 30, que é considerado sensor onde nós 12 não mova uma vez implantado. Esses nós 12 sentido o ambiente nas proximidades e produzir relatórios sobre eventos de interesse, que incluem o tempo, localização, descrição, etc (por exemplo, as leituras de sensores) dos eventos. Os relatórios são enviados para um dissipador de 38 por nós intermediários através 41-47 multi-canais hop wireless. O coletor de 38 é uma poderosa máquina com computação e recursos suficientes de energia. O encaminhamento é assumido como sendo relativamente estável. Rotas não mudam com freqüência em curtos períodos de tempo. Quando as rotas são estáveis, cada nó 12 tem apenas um vizinho próximo salto em um caminho de encaminhamento de 36 e encaminha todos os pacotes para o coletor de 38 com este vizinho. Isso é consistente em qualquer árvore de roteamento baseado em protocolo ou protocolos de roteamento geográfico, que são conhecidos no art. Suponha que cada nó sensor 12 tem uma identificação única e partes uma única chave secreta (K) com pia 38. A chave de identificação e podem ser pré-carregado em um nó de 12 antes de ser implantado. O coletor de 38 pode manter uma tabela de referência para todos os IDs nó e chaves. Enquanto nós pode estabelecer outras chaves

para fins de autenticação vizinho, PNM não exige tais chaves para trabalho. O sensor de nós 12 podem ser recursos limitados e têm pouco poder computacional, capacidade de armazenamento e abastecimento de energia. Por exemplo, os motes conhecido Mica2 bateria são alimentados e equipados com apenas um processador 4MHz e 256K de memória. Embora a criptografia de chave pública pode ser implementado em dispositivos como low-end, que é muito caro no consumo de energia. Assim, apenas eficiente criptografia simétrica (por exemplo, funções de hash seguro) é considerada pela simplicidade aqui. No cenário atual de exemplo FIG. 3, toupeiras S (fonte 32) e X (caminho de encaminhamento do nó 44) trabalham em conjunto para cobrir seus rastros para injetar tráfego do ataque, S injeta relatórios falsos. X 44 recebe um pacote com, os nós 1, 2, 3 marcas (57). X pode manipular as marcas de várias maneiras, tais como alterar essas marcas para 1 ', 2', 3 '(55), ou removendo a marca de (56) nó 1.

O objetivo das toupeiras é ocultar a sua localização, ou levar a faixa pia para nós inocentes.

Modelo e Attack Threat Taxonomy: O adversário pode comprometer nós sensores através da captura física ou bugs de software, assim, ganhar o controle cheio deles. O adversário tem acesso a todas as informações armazenadas, incluindo as chaves secretas, e pode voltar a programá-los a se comportar de uma maneira maliciosa. Moles poderá coordenar a maximizar o dano. O coletor de 38 geralmente é bem protegido. Apesar de possível, pias comprometidos são menos prováveis e não são considerados pela simplicidade. O contexto de rastreamento é a ameaça de injeção de dados falsos. Um mol S 32 funciona como uma fonte e injeta uma grande quantidade de falsos relatórios de sensoriamento na rede. Esses relatórios não só interromper a aplicação do usuário, mas também desperdício de recursos de rede (por exemplo, a energia, largura de banda) gastos em sua transmissão. Traceback é o primeiro passo para a defesa ativa. Ela permite a pia para identificar a verdadeira origem dos relatórios. O coletor pode, então, expedição forças-tarefa para esses locais, remover moles fisicamente, ou não notificar seus vizinhos para encaminhar o tráfego a partir deles. O mecanismo exato pode variar, e o foco atual está no

traceback aqui. O desafio para um sistema eficaz de marcação é um conluio X mole 44 ao longo do caminho de encaminhamento pode mexer com as marcas de forma arbitrária. The X mole 44 pode se esconder tanto a sua localização ea toupeira de origem (32) a localização, ou mesmo enganar o coletor de rastreamento para nós inocentes. Escondendo os locais permite a injeção contínua sem ser preso ou punido. Essa dissimulação é necessária para a injecção de causar danos significativos. Vazamento de qualquer de suas posições levará a punição como o isolamento de rede ou remoção física. Enganando o coletor de rastreamento para nós inocentes é um bônus extra em que o coletor de nós pune inocentes, assim cortando un recursos contaminados e efetivamente punir-se. A taxonomia de conluio ataques contra-marcação de rastreamento baseado em dois moles de conluio, S que injeta relatórios falsos, e X no caminho de encaminhamento são fornecidos os seguintes.

1) Não Ataques-Mark: A toupeira pode não marcar o relatório a todos.

2) Ataques marca de inserção: Ambos mole a fonte e o encaminhamento mole pode inserir uma ou várias marcas falsificadas nos relatórios.

3) Os ataques Mark Removal: A toupeira encaminhamento pode remover as marcas deixadas pelos actuais upstream nós nos relatórios.

4) Marcos Re-ordenação Ataques: Uma toupeira encaminhamento pode reordenar as marcas existentes nos relatórios.

5) Os ataques Mark modificação: Uma toupeira encaminhamento podem alterar marcas existentes nos relatórios e torná-los inválidos.

6) Os ataques Dropping seletiva: A toupeira pode encaminhar seletivamente soltar os pacotes que, se recebida pelo coletor, levaria o traceback para eles.

7) Os ataques de Identidade Permuta: S e X podem conhecer uns aos outros é a chave e representar o outro. Por exemplo, a FIG. 3 mostra uma cadeia de 7 nós de encaminhamento (41-47) entre a fonte S mole e 32 pia 38. Nó X 44 é

a toupeira conluio. Nó 44 recebe mensagem de V3, que Inclui 3 marcas válidas 1, 2, 3, deixada por nós V1, V2, V3. Nó 44 pode alterar estas a 1 ', 2', 3 ', tornando-os inválidos, assim afundar o rejeita estas marcas. Nó 44 pode remover marca 1 e deixar apenas 2,3, portanto, o traceback pára em nós inocentes.

Tabela 1

S mole A fonte

M Mensagem gerada pela fonte de S. mole Contem evento, | |local, data / hora. M = T E L

X O VX conluio mole na hop x

Vi Os nós de encaminhamento, em hop 1 a n

ki A chave secreta compartilhada entre o VI e o dissipador

Mi A mensagem enviada por Vi nó para seu próximo hop vizinho Vi 1

A marca de mi acrescentado pelo nó i ao Mi_I. Pode incluir ID Vi e MAC

Para auxiliar a apresentação, a Tabela 1 inclui as notações empregadas a seguir. Uma fonte S mole injeta 32 relatórios falsos que obedecer a um formato legítimo. Cada relatório inclui uma M E o caso, localização L e T Timestamp (ie, " denota a concatenação). |, onde "| |M = E L T

Os relatórios podem não incluir todos exactamente o mesmo conteúdo, caso contrário, eles são considerados redundantes e ser abandonado por nós encaminhamento legítima. M é transmitido ao longo de uma cadeia de n nodos intermediários (Vi) (i = 1, ..., n) para a pia 38.

Vi cada nó tem um ID exclusivo e que partes ki uma chave única, com a pia. O nó pode usar sua chave para gerar um Message Authentication Code (MAC) ou a assinatura de outros para os pacotes que gera ou para a frente, utilizando um eficiente e segura de função hash com chave Hk (), onde k é a chave. Especificamente, VI adiciona uma marca de Mi para a mensagem que

recebe da anterior hop Vi-1 para construir sua própria mensagem mi mi podem incluir ID Vi I e MAC MACI. Vi, então, envia Mi para o próximo salto Vi 1.

Transmissão nó Vx (1 <x <n) é uma toupeira conivente e é indicado como X (44). X pode manipular as mensagens que recebe de Vx-I de forma arbitrária e, em seguida, passar a mensagem para VX-1. Mole X pode usar qualquer um ou uma combinação de ataques descritos acima para ocultar a localização de S (32) e ela própria, ou levar o traceback para nós inocentes.

Autenticar os regimes de marcação (AMS), da arte prévia não fornecer segurança suficiente, visto que a marca adicionado por um nó não proteger a sua relação com as marcas deixadas por nós anterior. Cada marca pode ser manipulado individualmente sem afetar a validade das outras marcas. A nested marcação, em conformidade com os princípios presentes estabelece uma ligação entre cada marca e todas as marcas anteriores e marcação probabilística fornece um recurso adicional, o anonimato de identificações, para derrotar os ataques selectivos caindo.

PNM pode localizar conluio moles em dados falsos ataques de injeção, dentro da precisão de um bairro único suspeito. Isso inclui um nó e seus vizinhos de um hop. Uma toupeira, origem ou encaminhamento, está entre eles. PNM inclui duas técnicas, ou seja, aninhadas marcação e a marcação probabilística aninhados. A nested marcação é o mecanismo básico. Ele garante que o coletor pode rastrear a uma toupeira usando somente um pacote. No entanto, tem uma desvantagem de sobrecarga de mensagem grande, pois cada nó de encaminhamento deve colocar uma marca em o pacote. Em redes de sensores grandes isto pode não ser eficiente.

Posteriormente, probabilística marcação é empregada para espalhar a mensagem de sobrecarga sobre múltiplos pacotes. Cada nó de encaminhamento coloca uma marca com certa probabilidade. Assim, um pacote carrega apenas algumas marcas e por sobrecarga de pacotes é bastante reduzido. Este comércio fora do poder de detecção de sobrecarga de mensagens. O coletor pode precisar

de vários pacotes para identificar as toupeiras, que é razoável, desde que as toupeiras são identificados antes de causar danos significativos.

Basic Nested marcação: Marcação de pacotes: Cada nó de encaminhamento Vi acrescenta ao pacote seu ID i e um MAC segura usando o ki chave secreta que compartilha com a pia. O I). | MAC protege toda a mensagem que recebe de Vi-1. Isto é, MACI Hki = (Mi-1 Como exemplo, o mensagens enviadas por nós vizinhos são:

S -> V1: M

V1 -> 1) | Hk1 (M | | V2: M1 = Mi 1

V2 -> Hk2 (M | 2 | V3: M2 = M1 2) ... |

VI -> I). | Hki (Mi-1I | | Vi + L: Mi = Mi i

Em cada salto, i) provar que o | o que indica a presença de ID do nó i na rota, o Hki MAC (Mi-1 dissipador é certamente nó i que envia mensagem de Mi, e qual foi o nó recebe Mi-1. Pode ser visto que o MAC adicionado por ~ protege não só a sua própria identificação, mas a mensagem inteira do salto anterior. Este é o lugar onde o nome de nested marcação vem. O MAC protege as identificações e MACs de todos os nós anteriores, e sua ordem relativa. Qualquer interferência com as identificações anteriores, ou Macs, ou a sua ordem, tornará inválido o MAC.

A seguir a análise de segurança formal será empregado para mostrar que aninhados marcação são necessários e suficientes para o rastreamento seguro. Ou seja, ele pode resistir a todos os ataques da concertação, mas qualquer projeto mais simples não pode. Por exemplo, na AMS alargada apenas a mensagem original M e ~ 's ID estão protegidos, mas não a marca de 1 ligação a marca anterior em Mi. É por isso que AMS falhar quando as marcas são manipulados individualmente.

Traceback: Depois de receber pacotes de Mn, o coletor verifica as marcas aninhadas para trás. Primeiro, ela recupera a identificação do n hop

passado e usa os kn tecla correspondente para verificar a última MAC MACN. Se MACN está correta, ele recupera a identificação do n hop anterior - 1 e verifica MACN-1. O coletor continua este processo até que se tenha verificado todos os Macs como correto, ou ele encontra um MACX incorreta. Uma toupeira (fonte de um ou encaminhamento) está localizado dentro do bairro de um hop do nó com o MAC passado verificado (incluindo este próprio nó).

Por exemplo, na FIG. 3, se X mol altera a marca de 41 nós, as marcas de nós 41, 42 e 43, se tornarão inválidos. Quando X não deixar uma marca ou deixa uma marca inválida, o traceback pára em 45 nós e uma toupeira (X) está entre os vizinhos de um hop desta paragem nós quando o X deixa uma marca válida, o traceback pára no nó X ea mole é esse nó parar.

Probabilistic Nested Marcação: Probabilistic Nested Marcação permite que cada marca nó de encaminhamento do pacote com uma pequena probabilidade p. Assim, em um caminho de transmissão de n nós, em média, uma mensagem carrega marcas np. A probabilidade p pode ser ajustado de tal forma que a sobrecarga de marcas NP é aceitável.

Uma extensão incorreta: Estendendo a uma marcação probabilística pode parecer simples à primeira vista. No entanto, ele acaba por ser não-trivial. Basta deixar que cada marca nó com probabilidade p (veja a seguir) é vulnerável a ataques selectivos queda que pode levar o traceback para nós inocentes.

S -> V1: M

V1 -> V2 (com p): 1)| Hk1 (M | |M1 = M 1

V2 -> 2 ...| Hk2 (M | 2 |V3 (com l-p): M2 = M1

VI -> Hki (Mi-1)| |Vi +1 (com p): Mi = Mi-1 i

VI -> Vi +1 (com l-p): Mi = Mi-1. (1)

Considere o exemplo na Figura 3. Desde a identificação da lista está em texto puro, o X conluio toupeira pode ver quais VI, V2, V3 marcaram o pacote.

Mole X pode soltar todos os pacotes, incluindo marcas de V1 e encaminhar apenas aqueles que ostentem marcas S de V2, V3. Quando o coletor de vestígios de volta, ela vai parar em V2, cujo um bairro hop não inclui qualquer toupeira. Na verdade, X pode levar o rastreamento de qualquer nó inocentes entre ela ea toupeira fonte.

Este ataque funciona porque em marcação probabilística, cada pacote carrega apenas parcial "amostras" de nós no caminho de encaminhamento. Devido ao texto sem identificação, a toupeira pode seletivamente passar alguns "samples" de modo que o coletor vê apenas um caminho parcial que terminou em uma de X 's nós upstream. Este ataque não se aplica na base aninhados marcação (marcação determinísticos), em conformidade com os princípios presentes, porque cada pacote carrega as marcas que constituem o caminho completo. Não existe nenhum parcial "amostras" para a seletiva caindo. Para derrotar os ataques selectivos caindo, é desejável que nenhum nó de encaminhamento é capaz de dizer os outros nós que marcou um pacote. Desta forma, a toupeira conluio não é possível saber quais os pacotes a cair. No entanto, a afundar ainda precisa descobrir o que deixou marcas para verificar as marcas. Na descrição seguinte, a assimetria da pia é explorado, que fornecem informações adicionais sobre todas as chaves secretas e recursos de computação suficiente para resolver o problema.

Probabilistic Nested Marcação: Ao invés de usar a sua real identificação i, um nó legítimo Vi usa um ID anônimo i 'no pacote. O mapeamento do I Real ID para ID anônimo i 'depende do ki secreto, conhecido apenas por ~ e afundar o. A toupeira conluio não possuem o conhecimento do ki de descomprometido ~, portanto, não se pode deduzir a identidade real de um anônimo.

S -> V1: M

V1 ->)|'), sendo que 1 '= H'k1 (M I | Hk1 (M I | 1 '|V2 (com p): M1 = M

V1 -> V2 (com 1-p): M1 = M...

VI -> Hki (/ | ' | Vi +1 (com p): Mi = Mi-1 i i') | Mi-1 i) | onde i = 'H'ki (M

VI -> Vi +1 (com 1-p): Mi = Mi-1. (2)

No exemplo acima, H '() é uma outra forma segura de função que calcula o ID anônimo. O anônimo ID i 'é obrigado a M tal que se muda para cada mensagem distinta Vi frente. Lembre-se que para evitar ser considerados como cópias redundantes e caiu, relatórios forjados pelos mole fonte deve ter conteúdo diferente). Isso evita um mapeamento estático que pode ser acumulado ao longo do tempo pelo atacante. Comparado com o AMS estendida, ela tem duas aninhadas marcação e identificação anônimo.

Marca de verificação: Com o ID anônimo, a verificação na pia se torna diferente. O coletor primeiro precisa saber a identidade real, então o dissipador pode usar a chave secreta correspondente para verificar o MAC. O poder de computação abundante na pia pode ser explorado para usar uma busca exaustiva para encontrar a identidade real. Depois de receber de Mn Vn nó, o primeiro coletor computa todas as identificações de anônimos para cada nó na rede. Saber M, ele pode construir uma tabela para mapear todos os IDs para i i '. Ao olhar para cima i ', ele conhece a identidade real i. Então, ele pode usar o ki tecla correspondente para verificar o MAC. Desta forma, o coletor pode verificar todos os Macs, um por um. A busca exaustiva é viável dado o poder de computação da pia ea baixa taxa de dados em redes de sensores. Para cada mensagem distinta M, o coletor deve-se calcular uma tabela diferente para fazer a pesquisa. Tendo em conta que um cálculo de hash pode ser feito a nível microssegundo (por exemplo, um 1.6G CPU pode fazer 2,5 milhões hashes por segundo), a construção desse quadro, mesmo para uma rede razoavelmente grande (por exemplo, a alguns milhares de nós) deve assumir o ordem de alguns milissegundos. Assim, o coletor pode verificar várias centenas ou mais pacotes por segundo. Porque o coletor recebe de um sensor de cada vez, a taxa de dados de entrada é limitada por uma taxa de rádio de sensores. Várias centenas de pacotes já é muito maior do que a taxa de dados atual em hardware sensor típico (por exemplo, 12Kbps para motes Mica2, em 100 pacotes por segundo). Traceback: toupeiras Localizando-se um processo de duas etapas. Primeiro, o

coletor precisa reconstruir a rota através da recolha de marcas a partir de um número suficiente de pacotes (o número de nós a serem analisados serão abordadas a seguir). Então, ele identifica quais nós temos moles em sua vizinhança um hop. Um método ilustrativo 1 que descreve como o coletor pode localizar moles onde probabilística marcação é utilizada, é apresentada no pseudo código abaixo.

Método 1 algoritmo para localizar Moles

1: Ii Inicialização

toupeira candidato set 5 = <1>, a fim relação matriz M é O x O, nó 0 = <1>, laço nó conjunto \. Se = < I >

2: sub-rotina II para adicionar uma relação i ~ j em upstream e atualizar a RE / matriz ation II

1 representa Vi a montante a vice-V j '-1 versa, O é indecisos, 2 é ambíguo

AddLink (i, j) (if (M (i) [j] == -1) IlifVi tem sido mostrada a jusante 'VJ

M [i] = UJ MU] [i] = 2 II para jogos entre Vj, 'Vjto beambiguous

else if (M [i] [j] == 0 & & M (j) [i] == 0) II, se a ordem não está decidido

M [i] = 01 MU] [i] = -1; II define VI, a montante para Vj

para cada k EO II recursive / y atualizar as ordens ofVjJ Vj para outros nós

if (M (k) [i] == 1 II M (k) (i) == 2) ifVk II é a montante Vk Vi "é a montante 'VJ AddLink (k, j); If (m (j) (k) == 111 M [j] (k) == 2) II if'Vj está a montante Vi Vk 'é a montante Vk

AddLink (i, k);

fim para

)

3: II Dada uma nova forma / ação da matriz M, identificar nós em um oop / identidade por troca de ataques.

Encontre o loop (

)

para cada Q ViE

para cada O vje

if (M [iJ [j] == 2)

\. Se = \. If U (i, J1

4: II Após a verificação de k corrigir marcas aninhadas de nós (Vi7, VI2 ~ ~ ... ~ VJK).

)

Marcas incorretas são descartados.

Processo Packet O (

If (i7 ~ Q)

5 = 5 U (i) 7

para cada ij fi. O

Q = Q U (~)

adicionar uma nova linha e uma nova coluna para ij em M

Ali conjunto de novos elementos de M a O

endfor

para cada linkVj. + Vj. 7 STMi • i • 711 IlupdateM recordV para, •

Upstream é a V, •. 7 J ~ 1 ~ J ~

Adicionar Link (IJ '~ 7);

endfor

para cada IE 5, Sila ifthere3Vj E s.t.Mj.i Q = 1

Se 50,5 = 5 - (i) II remover os nós com nós upstream

fim para

Eu continuo na próxima página

)

WO 2008/119672

/ / Procedimento principal para localizar moles

O principal)

22

/ / Isso garante marcas bastante são recebidos para reconstruir a rota

O processo de execução de pacotes para um número suficiente de pacotes recebidos

if (S = ~) / / se existem nós sem nós upstream

5 contém nós cujo um bairro hop tem moles

else (

executar FindLoopO para remover os nós do circuito

remover de m linhas e colunas correspondentes aos nós em 'f'

PCT / EP2008/053325

/ / Entre nós não no loop, o mais a montante tem toupeiras em um

bairro hop

encontrar os nós mais a montante em M

)

Referindo-se a FIG. 4, um bloco diagrama de fluxo / descreve um sistema / método para localizar moles, de acordo com uma encarnação. Uma rota pode ser reconstruído por encontrar a ordem relativa de nós (que está a montante para o qual) no caminho de encaminhamento. No bloco 110, uma rota é reconstruído através da determinação de todos os seus nós de montante. A matriz M de empregados para manter as ordens de parente. A matriz é inicialmente vazio. Quando um MAC correto para um novo nó é Vi Verificou, mais uma linha e mais uma coluna correspondendo a ~ é adicionado à matriz no bloco 112. Sempre que dois MACs consecutivos, MACI, MACj dentro de um pacote são verificadas como corretas, ~ deve ser a montante Vj, e M [i, j] registra essa relação (por exemplo, i, j é definida como 1. -1 Significa Vj a montante a VI, e O é indeterminado) na matriz no bloco 114. Desde que há 10 é mais do que um nó no caminho da transmissão, vários nós podem ter marcado o pacote quando virar a moeda com probabilidade p (ver equação 2). Estes nós não pode ser um segmento contínuo no caminho, eles podem ser disjuntas no caminho de encaminhamento. Quanto mais pacotes são recebidos, a pia continua atualizando esta matriz. Atendendo pacotes suficientes, o coletor será capaz de descobrir a relação montante entre todos os nós de encaminhamento, assim, a rota 15 completa. O coletor será capaz de reconstruir a dois tipos de rotas: aqueles que não têm laços, ou aqueles que têm laços. O primeiro tipo ocorre quando toupeiras usar ataques que não trocar de identidade, este último quando toupeiras trocar suas identidades para deixar marcas. No primeiro caso, localizando moles é equivalente a encontrar o nó mais a montante. Porque uma toupeira fonte produz pacotes por si só, não receber pacotes de outros e que pode ser o nó mais a montante. Uma toupeira encaminhamento pode "aparecer" para ser o mais a montante, se retira marcas deixadas por seus nós upstream. Em ambos os casos, uma fonte de encaminhamento é mole ou no prazo de um bairro hop do nó mais a montante. As toupeiras podem utilizar a

troca de identidade para criar loops (ver FIG. 5), o que não existe uma mais "nó" upstream. Referindo-se a FIG. 5, S AndX pode usar uma da outra chave para deixar marcas válido para alguns pacotes, causando assim um ciclo, incluindo todos os nós entre S e X (incluindo os nós) quando o pia reconstrói a relação montante entre nós. O coletor pode ainda traceback para onde o laço quebra a ligação e identificar um mo le dentro desse bairro. Uma fonte S mole e um redirecionamento do X mole podem deixar marcas válido usando a chave do outro para alguns pacotes, e usar suas próprias chaves para alguns outros pacotes. O coletor de achar que wili S aparece antes de X para alguns pacotes, e afier X para outros pacotes. O coletor wili também achar que nós all entre S e X (incluindo o S e X) formam um circuito fechado 130. Para quaisquer dois nós de U, V, xsuch um loop, U aparece tanto a montante como a jusante V. No entanto, esta anomalia pode ser facilmente identificadas: o coletor pode encontrar o resto de nós de uma forma linha do loop para si. Uma toupeira está localizado dentro do um-ofthe bairro hop mais nó a montante desta linha (ou seja, quando o ciclo se cruza com a linha).

Security Analysis: a força de segurança ofPNM é comparado a altemative regimes de marcação. A análise mostra que aninhados marcação é tanto preciso e necessário. PMN pode rastrear moles dentro de uma região do bairro hop colluding apesar dos ataques, mas qualquer projeto mais simples falha em certos ataques. A marcação probabilística aninhada pode rastrear moles dentro uma área-hop asymptotically bairro como o coletor recebe número suficiente de pacotes ao longo do tempo.

Segurança Marcação ofNested: Duas propriedades para os regimes de marcação são primeiro definidas, ou seja, um salto de precisão e rastreabilidade consecutivos, e em seguida, se for provado que eles são equivalentes. Então, se for provado que o nosso regime aninhados básica é uma marcação precisa-hop, mostrando seus rastreabilidade consecutivos.

Definição 1 (One-hop precisão): Um sistema de marcação de uma precisão de hip hop em traceback se sempre pode rastrear a qualquer nó da fonte ou bairro uma toupeira colluding de um hop.

Definição 2 (Rastreabilidade consecutivas): Considere dois nós consecutivos legítimo U e V em um caminho de encaminhamento (ou seja, V recebe mensagens de U e em seguida, encaminha-los). Com um sistema de rastreabilidade consecutivos marcação, se o dissipador tem seguido a V, pode sempre mais de rastreamento a U.

Teorema 1: Um esquema de marcação é um hip-hop precisa se e somente se ele é rastreável consecutivos.

Suficiência Prova: Suponha que o traceback pára em um nó V, que é o último nó (em na ordem inversa de envio), que tem um MAC válido. V não pode ser um nó que é legítimo não no caminho da transmissão, porque nós, como não irá gerar Macs para mensagens que não para a frente, e que o atacante não sabe as suas chaves secretas. Assim, o mapa ou uma toupeira, ou um nó legítimo no caminho de encaminhamento. Se V é uma toupeira, a suficiência detém. Em seguida, o caso em que V é um nó de transmissão é considerado legítimo. Vamos Ube o salto anterior do V, ou seja, a partir de U Vreceives Existem apenas duas possibilidades: ou U é uma fonte (mole ou conluio) ou U é um nó legítimo. No primeiro caso, a suficiência lds ho porque V é na vizinhança de um mo le U Por outro lado, pela definição de rastreabilidade consecutivo, o traceback irá proceder a U e não vai parar V Assim, o segundo caso não pode acontecer. Isto conclui a prova de suficiência. Em seguida, a necessidade é provado pela contradição. Suponha um esquema de marcação não é consecutivo rastreáveis. Ou seja, existem casos em que o coletor tem seguido a uma legítima nó V, mas não pode proceder à anterior legítimo nó U Assim, o traceback pára em V, não necessariamente a fonte OFTHE bairro ou uma toupeira conluio. O regime não é um hip-hop precisa, por definição.

Referindo-se ao FI G. 6, existem duas categorias de nós no caminho de encaminhamento.

Categoria 1: moles e suas hop imediato seguinte; Categoria 2: nós legítimos que foram imediatas próximo hop anterior legítima. Devido à rastreabilidade consecutivo, o rastreamento não pode parar na categoria 2. Para a categoria 3 nós (os nós legítimos não no caminho de encaminhamento), eles

fazem não deixar marcas para a mensagem de que não para frente. Assim, o rastreamento pode parar apenas na categoria 1 nós. Um salto de precisão, o traceback pára na primeira categoria; consecutivo rastreabilidade, o rastreamento não pode parar dentro da segunda categoria - ou seja, ele tem que parar dentro do primeiro.

Teorema 2: O regime de nested marcação é rastreável consecutivos. Prova: Considere dois nós consecutivos encaminhamento legítimo U e V Vamos ser o Mu que envia mensagem de U a V, V e VI HKV envia Mui MUI (V) para o próximo salto. Suponha que o coletor traçou a V Isso significa que ele deveria ter verificado MAC'v, em uma mensagem M'ul VIMAC'v, e descobriu que o MAC recomputorizados (HKV (M'ul V)), é o mesmo que o incluído MAC'vo Porque o atacante não sabe kv, v MA C 'deve ser o MA C / V Assim gerado por u M', Mu e ele deve o mesmo, caso contrário, o MAC recomputed não combinaria que produziu por V Mu Porque é enviada por um nó legítimo U, a última marca de Mu devem realizar um válido MAC a partir de U Portanto, ao verificar esse MAC, o coletor pode rastrear mais de U

Corolário 1: O esquema de marcação é uma nested-hop precisa. Necessidade ofNested Marcação:

Teorema 3: Qualquer esquema de marcação que protege os campos menos do que a marcação não está aninhada consecutivos rastreáveis.

Prova: Na nested marcação, um nó 's MAC protege tanto a sua própria identificação e toda a mensagem que recebe do salto anterior. Agora, considere um r altemative esquema de marcação, em que o MAC protege menos campos do que o MAC aninhados. Deve existir um nó A, cuja identificação ou MAC não está totalmente protegida por todos os nós afier ela, caso contrário, se tornaria o r esquema de marcação aninhados.

Referindo-se a FIG. 7 °, X altera os bits em um não é protegido por marca V Assim marca o V é ainda está correto, mas não D's. Então, o coletor remonta ao V, mas não pode mais rastrear a U Let Ube o último nó que protege o 's ID e MAC completamente, e Vbe o próximo salto de U (Ver FIG. 8). Isto é, há

alguns pedaços inA 's não marca protegida por MAC V. Vamos considerar uma toupeira a jusante após V mole O apropriadamente assinala o relatório, e que altera a bits em um não é marca protegida por V 's MAC. Neste caso, os MACs de todos os nós depois V (incluindo V) estão corretas, assim, o coletor pode rastrear a V, no entanto, porque um 's marca é adulterado pelo mole, MAC U's parece inválido, assim, o coletor não pode mais rastrear a U Em outras palavras, r não é rastreável consecutivos.

Corolário 2: Qualquer esquema de marcação que protege os campos menos do que a marcação não está aninhada um-hop precisa. Segurança Marcação ofProbabilistic aninhadas:

Teorema 4: A probabilística aninhados marcação é assintoticamente um hip-hop precisa.

Prova: Existem dois casos possíveis quando o coletor reconstrói a relação entre a montante nós: ou não existem laços, ou existem laços. Quando não há laços, a prova é semelhante ao 2 ofTheorem. Vamos considerar dois nós consecutivos legítimo U, von caminho de encaminhamento. Devido à marcação probabilística, estes dois nós nem sempre ambos deixar marcas no pacote. No entanto, com número suficiente de pacotes, a probabilidade de que que não quer deixar marcas no mesmo pacote, (LP? n, torna-se cada vez menores, como o n aumenta número de pacotes. Assintoticamente, haverá pacotes onde ambos U, V Deixar marcas. A toupeira de encaminhamento pode ser capaz de ignorar esses pacotes. No entanto, porque o uso OFTHE de identificações anônimo, que nem sempre podem adivinhar corretamente e solte todos esses pacotes. Assintoticamente, o coletor vai receber pacotes com marcas de ambos U e V, na sequência raciocínio semelhante no Teorema 2, uma vez que o coletor tem seguido a V, pode ainda traçar a U. Assim, o rastreamento não vai parar no V Assim, o rastreamento tem que parar, no máximo, a montante nó, que tem pintas no seu bairro um hop (incluindo este próprio nó). Quando existem laços, nós provamos que o ponto de união (X) nó loop OFTHE a linha (ver FIG. 6) têm um molar dentro do seu bairro hop (incluindo este nó próprio) contradição. Suponha que todos os 4 nós de dentro desta um bairro hop

(XS, A, B) são nós legítimos. Porque os pacotes chegam ao coletor de X para A, deve ser o próximo salto vizinho no caminho X encaminhamento. Porque o loop representa também a relação entre a montante nós, X deve também enviar pacotes para um de seus vizinhos sobre o loop (S ou B). Assim Xhas próximos dois vizinhos hop em seu caminho de encaminhamento. No entanto, qualquer nó legítimo deveria ter apenas um vizinho próximo salto no seu caminho de encaminhamento quando as rotas são estáveis. Assim, estes 4 nós não podemos ser nós ali um ofthem legítima e deve ser uma toupeira. A intuição por trás dessa prova é que deve haver algum comportamento anormal em torno de onde o ciclo se conecta à linha. Para nós legítimos, eles não fazem loops quando as rotas são estável. Assim, tal comportamento anormal só pode ser explicado pela presença ofmoles. Nota mo les que podem lançar um ataque em troca de identidade de base aninhados marcação, mas desde que todos os nós deixam marcas em cada pacote, o coletor não precisa de rastreamento através do upstream relacionamento e ele sempre pode rastrear diretamente para as toupeiras.

Avaliação de Desempenho: Analise N, o número de pacotes necessários para o dissipador para coletar pelo menos uma marca de cada OFTHE nós encaminhamento VI, ... Vno Podemos calcular a probabilitythat isso é feito dentro. Os pacotes L, P (N ::::; L) = (1 - l-p) Tenente Referindo-se a FIG. 8, um gráfico ilustra a probabilidade de que pelo menos uma marca de n nós são recolhidos no prazo de pacotes x. A média do número de marcas np um pacote carrega é fixado em 3. Para um caminho que contém 10 nós, depois de receber 13 pacotes, o coletor tem cerca de 90% fibrobroncoscopia probabilidade coletadas todas as marcas. Leva 33 e 54 pacotes para atingir os 90% confiança para os caminhos de 20 e 30 saltos, respectivamente. Os resultados mostram após um relativamente pequeno número de pacotes, que não desperdiçou significativo de energia e largura de banda recursos, o coletor terá recolhido as marcas de todos nós.

Resultados da Simulação: Referindo-se a FIG. 9, simulações foram realizadas para verificar a análise e uma avaliação mais aprofundada métricas que são difíceis de analisar. A probabilidade p é ajustado para diferentes

comprimentos de trajeto em um n tal 3 pacote carrega as marcas, em média. Os resultados da análise foram previamente verificados. O número de n nós foi definido para 10, 20, 30. 200 pacotes são gerados a partir da fonte em cada corrida e nós média dos resultados de 5000 é executado. A probabilidade de que as marcas de todos os nós são recolhidos afier o coletor recebe pacotes x é mostrado na FIG. 9. Este resultado corresponde ANÁLISE DA of FIG. 8 muito bem.

FIG. 10 mostra a parte de nós cujas marcas são coletados pelo coletor após pacotes x. Quando há 10 nós, em média de 9 pontos nós "pode ser recebida no prazo de 7 pacotes. Para caminhos de 20, 30 nós, leva cerca de 14, 22 pacotes de recolher marcas de 90% dos gânglios. Dentro de algumas dezenas de pacotes, o coletor de nós sabe o que são os nós de encaminhamento. Desempenho do algoritmo de reconstrução de rota em marcação probabilística (método 1), foi também avaliada.

FIG. 11 mostra como a fonte de candidatos que muda conforme mais e mais pacotes são recebidos para uma corrida de 40-caminho de nó, O nó que está sendo a toupeira fonte. Na primeira, S nó está no candidato lista. Quanto mais marcas são recebidas, novos nós 8,11,9, 18 anos, no início ofpartial caminhos são acrescentou. Como seus nós upstream são descobertos mais tarde, eles são removidos da lista. O O fonte real é adicionada no pacote 2lth. Após o pacote de 80, não há mais candidatos nós O que não permanecem no conjunto. Quando o conjunto de candidatos mantém-se inalterado por um longo tempo, o coletor pode identificar de forma inequívoca uma toupeira. Sem número suficiente de pacotes, o coletor não pode ser capaz de reduzir de forma inequívoca a fonte candidatos que só toupeiras real. Para testar quantos pacotes são necessários, nós mudamos o número de pacotes da pia recebe como 200, 400, 600 e 800. Para cada quantidade de tráfego, corríamos a simulação de 100 vezes sobre cada um dos 10 comprimentos de trajeto diferente de 5 a 50. Nós obtidos quantas vezes o coletor não inequivocamente identificar a fonte.

FIG. 12 ilustra o número offailed funciona como um comprimento caminho função oftotal, para o 4 diferentes quantidades de tráfego. Podemos ver que 200 pacotes são suficientes para comprimentos de trajeto até 20.

O método 1, quase sempre de forma inequívoca identifique a fonte em cada série, *400 pacotes são suficientes para caminhos de até 30*. Apenas para trajetos muito longos (por exemplo, 50 nós), uma grande número de pacotes (por exemplo, 800) são necessários para reduzir a freqüência não inferior a 5%. Nós escolhemos 800 como a quantidade de tráfego para medir o número médio de pacotes na pia deve receber de forma inequívoca para identificar a fonte.

FIG. 13 mostra os resultados como uma função caminho de comprimento total, de todos os que executa com êxito identificar a fonte. Para comprimentos caminho menos de 20, em média, leva cerca de 55 pacotes para identificar de forma inequívoca a fonte. Este praticamente coincide com o resultado na FIG. 9, onde, com 55 pacotes, o coletor tem mais de 99% probabilidade fibrobroncoscopia marcas coletadas em todos os 20 nós. Mesmo para trajetos longos, como 40 nós, afier cerca de 220 pacotes da pia pode identificar de forma inequívoca a fonte. Os resultados PNM demonstrar que quase impede moles de lançamento efectivo injeção dados falsos ataques: eles estarão localizados antes que eles tenham causado danos suficientes para a rede.

Traceback Precisão: PNM pode traceback moles de um bairro-hop, que inclui um nó e seus vizinhos de um hop. Um ofthem é uma toupeira, ou uma fonte, ou um encaminhamento. A precisão não é único nó porque uma toupeira fonte pode reivindicar identidades diferentes quando injetando relatórios. Seu vizinho próximo salto não pode dizer que a identidade é verdadeira. PNM não requerem chaves emparelhadas entre vizinhos para trabalhar. No entanto, a existência de chaves emparelhadas pode ajudar a melhorar a precisão traceback. Tracebacks PNM um mol de uma vez. A expectativa é de que algum mecanismo de isolamento mole trabalhará em conjunto com PNM. Ela isola a toupeira identificadas em cada rodada. Assim, ao longo do tempo, esses moles são isolados da rede, um por um.

Impacto Dynamics ofRouting: A toupeira algoritmo localizar funciona bem quando o percurso é relativamente estável. Desde moles geralmente oftraffic injetar grande quantidade em curto espaço de tempo para maximizar o dano, coletando pacotes suficiente não precisa de muito tempo. Por exemplo, se moles injetar na taxa máxima de rádio, dentro de dez segundos, o coletor pode recolher cerca de 300 pacotes, o suficiente para localizar as toupeiras 40 saltos de distância. O percurso é muito provável que se mantenha estável durante este curto período de tempo.

Replay Reports: A toupeira fonte relatórios podem repetir com o mesmo conteúdo várias vezes, assim, o mapeamento entre IDs real e anónimo vai ficar fixo para cada nó de encaminhamento. A toupeira conluio podem acumular tais mapeamentos sobre o tempo, mas atlacks como pode ser facilmente contrariados pela supressão local de mensagens redundantes. Um nó de encaminhamento pode simplesmente deixar cair relatórios OFTHE mesmo conteúdo. Isto pode ser feito através da manutenção das assinaturas (por exemplo, um hash conteúdo) resultado do regime (ou seja, o evento, localização e timestamp) ofrecently visita mensagens e comparando os recebeu contra eles.

A toupeira de origem pode também relata replay legítimo de um nó real fonte de informação. O conteúdo do relatório ainda apresenta informações corretas. Para detectar e soltar mensagens, o mesmo supressão local pode ser usado. Há AIs o de outras técnicas. Um deles é fazer com que cada nó de manter um número de ordem crescente, para cada mensagem que envia ou encaminha, mas inclui o número de seqüência como marca OFTHE parte e protege-lo usando o MAC.

A pia pode detectar que os pacotes repetidos têm a mesma seqüência de números. Essa técnica tem sido explicado acima. Porque nós usam chaves diferentes, as identificações anônimo oftwo diferentes nós podem colidir (por exemplo, H'klMuli) = H'k / mujj). Uma função hash criptográfica som pode minimizar tal colisões; quando eles acontecem, o coletor pode simplesmente excluir esses pacotes de verificação. No PNM, moles também pode provocar maior por pacotes aéreos inserindo marcas mais falso ou usando uma

probabilidade mais elevada do que o solicitado. No entanto, isso faz com que apenas a redução de alguns eficiência; o coletor pode ainda traceback para eles. Podem existir múltiplas fontes moles todos enviando tráfego de ataque.

A nested básico marcação, devido à marcação de todos os nós de encaminhamento no caminho, ainda pode identificá-los. Quando os caminhos de transmissão desses moles de múltiplas fontes são disjuntos, o PNM pode construir caminhos diferentes individualmente e localizar as toupeiras. Essas toupeiras também podem trocar os seus identidades para criar laços, mas a linha reta que liga o coletor para estes laços ainda pode ser usado para identificar esses moles um de cada vez.

Referindo-se a FIG. 14, um bloco / fluxograma mostra um sistema / método de rastreamento no redes sem fio. Em uma rede de nós, cada nó é atribuído e mantém uma identidade Número (ID) (opcionalmente, um número de uma seqüência, como descrito acima na FIG. 2) no bloco 202.

No bloco 204, para uma modalidade, a (real) ID é opcionalmente mapeado para um ID anônimo ID do uso de uma chave conhecida por um nó atual e da pia ou por outros meios. O mapeamento do ID anônimo inclui o uso de um pacote de mensagem atual para mudar o ID anônimo para cada mensagem enviada. O mapeamento deve usar o conteúdo do pacote, tal que a mudança de mapeamento para cada pacote. Isso evita um mapeamento estático que pode ser acumuladas pelos Aprendida por atacantes Este é o preferido na encarnação PNM.

No bloco 206, uma chave secreta compartilhada entre o nó e o dissipador é empregado para calcular ou não determinar uma assinatura, por exemplo, um código de autenticação de mensagem (MAC). Um MAC é determinado para cada pacote que passa pelo caminho de encaminhamento.

No bloco 208, o pacote ou uma mensagem de um nó anterior pode ser hash de acordo com a chave para gerar o MAC. O MAC pode incluir uma versão de hash de uma mensagem recebida em um pacote. A identificação indica uma presença de nó no caminho de encaminhamento e do MAC prova que o nó enviou

o pacote associado com o ID. Os pacotes são marcados no bloco 209. A versão de hash pode ser considerada a marcação pacotes, os pacotes marcados são utilizados posteriormente para proporcionar um fim nó através da caminho de encaminhamento.

Para reduzir a sobrecarga por pacote, a marcação pode ser feita probabilisticamente em cada nó de encaminhamento. Em vez de sempre colocar uma marca no pacote, um nó de transmissão marca os pacotes com probabilidade p. Acrescenta que sua identificação anônimo e MAC, como de costume.

Com Ip probabilidade, não faz nada e simplesmente encaminha o pacote para o próximo salto.

O próximo hop usa a mesma probabilidade p de decidir se acrescenta uma marca, ou simplesmente continua passando o pacote como é. Variantes de marcação podem incluir base determinista marcação, onde cada nó coloca uma marca, e probabilística de marcação, onde cada nó coloca uma marca com certa probabilidade.

Na categoria 210, os pacotes são recebidos através de um caminho de encaminhamento de uma pia. O coletor reconstrói a ordem dos nós baseado na marca de um número suficiente de pacotes no bloco 211.

Ao receber cada pacote na pia, a correcção do MAC é verificado através de volta cada nó do caminho de encaminhamento.

A última MAC válido no caminho de transmissão é empregado para determinar uma fonte de injeção de dados falsos ou que todo o caminho é verificado (por exemplo, sem falsa fontes de injeção. Isso pode incluir a recuperação de um ID de um nó hop passado no bloco 214, cálculo do MAC para o nó hop passado no bloco 216, verificando o MAC do último salto nó no bloco 218, e repetir até que o MAC último válido é determinada no bloco 220.

Quadras 216 e 218 podem utilizar a janela deslizante descrito na FIG. 2 para verificar a número sequencial. Em uma modalidade, na quadra 213, os IDs

real são determinadas a partir das identificações anônimo para nós no caminho de transmissão (ou todos nós) antes de verificar o MAC.

No bloco 222, o MAC último válido indica a localização dentro ofmoles um hop. No PMN, reconstrução de rota (ver, por exemplo, FIG. 4) pode ser realizada para localizar toupeiras. A rota ofFIG reconstrução. 4 não é necessário para a abordagem determinista básicas de marcação. Moles estão localizados no caminho de encaminhamento e removido do caminho de transmissão no bloco 224.

Em incorporações particularmente útil, as toupeiras incluir uma pluralidade de moles de conluio no caminho de encaminhamento. Essas toupeiras podem ser fonte de nós, ou nós o encaminhamento e os tipos de ataques podem incluir a inserção de marca-ataques, ataques a remoção da marca, marca re-ordenando ataques, ataques marca alterando, ataques selectivos caindo, trocando ataques de identidade ou qualquer outro ataques.

Vantajosamente, pintas podem ser localizados em conformidade com o presente Principies dentro de uma toupeira hop do microfone.

REIVINDICAÇÕES

1. Um método para rastreamento de pacotes em uma rede, composta de: manutenção de um número de identidade (ID) para cada nó em uma rede; geração de uma assinatura em cada nó de encaminhamento usando uma chave secreta compartilhada entre este nó e um lavatório; Ao receber um pacote na pia, a verificação da veracidade das assinaturas de cada pacote pelo coletor na ordem inversa em que as assinaturas foram adicionados e determinar a validade da assinatura no caminho de transmissão para determinar uma localização de uma fonte de dados falsos injeção e / ou um nó conluio comprometida.

2. O método como relatado na reivindicação 1, onde o ID indica a presença de um nó no caminho de transmissão e da assinatura prova que o nó enviou o pacote associado com o ID.

3. O método como relatado na reivindicação 1, que compreende mais de hash o pacote em sua totalidade a partir de um nó anterior, em conformidade com a chave para gerar a assinatura.

4. O método como relatado na reivindicação 1, onde determina a validade da assinatura inclui a recuperação de um ID de um nó último salto, o cálculo da assinatura para o nó hop passado e verificar a assinatura do nó último salto, e repetir até que a última assinatura é válido determinado.

5. O método como relatado na reivindicação 1, onde mantém um número de identidade (ID) inclui o mapeamento de um ID anônimo do ID usando uma chave conhecida por um nó atual e da pia.

6. O método como relatado na reivindicação 5, em que o mapeamento do ID anônimo inclui o uso de um pacote de mensagem atual para alterar o ID anônimo para cada mensagem enviada.

7. O método como relatado na reivindicação 6, onde a verificação inclui a determinação do ID da ID anônimo para nós no caminho de encaminhamento.

8. O método como relatado na reivindicação 1, que inclui ainda a marcação de pacotes para proporcionar um fim nó através do caminho de encaminhamento.

9. O método como relatado na reivindicação 8, onde a marcação de pacotes inclui a marcação de pacotes probabilisticamente, com uma probabilidade, em cada nó de encaminhamento.

10. O método como relatado na reivindicação 8, onde a marcação de pacotes inclui deterministicamente marcação de pacotes em cada nó e fornecer um número de seqüência incrementado para cada pacote.

11. O método como relatado na reivindicação 1, onde a verificação da veracidade das assinaturas de cada pacote inclui o emprego de uma janela deslizante de determinar a seqüência de números válidos.

12. O método como relatado na reivindicação 1, que compreende mais moles, a partir do caminho de encaminhamento.

13. O método como relatado na reivindicação 1, que inclui ainda a localização de uma pluralidade de moles de colusão no caminho de encaminhamento.

14. O método como relatado na reivindicação 1, que compreende mais moles localizando dentro de um salto da toupeira.

15. Um produto de programa de computador para rastreamento de pacotes em uma rede que inclui um computador médio utilizável, incluindo um programa informático, em que o programa informático quando executado em um computador faz com que o computador para executar as etapas de: manutenção de um número de identidade (ID) para cada nó em uma rede; geração de uma assinatura em cada nó de encaminhamento usando uma chave secreta compartilhada entre este nó e um lavatório; Ao receber um pacote na pia, a verificação da veracidade das assinaturas de cada pacote pelo coletor na ordem inversa em que as assinaturas foram adicionados e determinar a validade da

assinatura no caminho de transmissão para determinar uma fonte de injeção de dados falsos.

16. Um método para rastreamento de pacotes em uma rede sem fio ou redes de sensores, incluindo: manutenção de um número real identidade (ID) para cada nó em uma rede; computação um ID anônimo do real identificação com base em uma chave secreta conhecida apenas por um nó atual e um lavatório; gerando um código de autenticação de mensagem (MAC) usando a chave secreta para cada nó em um caminho de encaminhamento para marcar cada pacote com pelo menos duas probabilidades; remontando o caminho para descobrir fontes de dados falsos por injeção: determinar a identidade real do ID anônimo para nós na rede; reconstrução de uma rota do nó usando marcas presentes em cada pacote, e verificar a exatidão do MAC de cada pacote de volta através de cada nó do caminho de transmissão usando a identificação real e da chave secreta para determinar um MAC último válido no caminho de encaminhamento.

17. O método como relatado na reivindicação 16, onde o ID indica a presença de um nó no caminho de transmissão e do MAC prova que o nó enviou o pacote associado com o ID.

18. O método como relatado na reivindicação 16, compreendendo mais de hash o pacote de um nó anterior, em conformidade com a chave secreta para gerar o MAC.

19. O método como relatado na reivindicação 16, onde inclui a verificação de regularidade recuperar a identidade real de um nó hop passado; cálculo do MAC para o nó hop passado e verificar o MAC do nó último salto, e repetir até que o último válido MAC é determinado.

20. O método como relatado na reivindicação 16, compreendendo ainda a localização de uma pluralidade de moles de colusão no caminho de transmissão, e remover as toupeiras de colusão.

21. O método como relatado na reivindicação 16, onde localizar moles é realizado dentro de um salto da toupeira.

22. Um produto de programa de computador para rastreamento de pacotes em rede sem fio ou redes de sensores que compreende um suporte electrónico utilizável, incluindo um programa informático, em que o programa informático quando executado em um computador faz com que o computador para executar as etapas de: manutenção de um número real identidade (ID) para cada nó em uma rede; computação um ID anônimo do real identificação com base em uma chave secreta conhecida apenas por um nó atual e um lavatório; gerando um código de autenticação de mensagem (MAC) usando a chave secreta para cada nó em um caminho de encaminhamento para marcar cada pacote com pelo menos duas probabilidades; remontando o caminho para descobrir fontes de dados falsos por injeção: determinar a identidade real do ID anônimo para nós na rede; reconstrução de uma rota do nó usando marcas presentes em cada pacote, e verificar a exatidão do MAC de cada pacote de volta através de cada nó do caminho de transmissão usando a identificação real e da chave secreta para determinar um MAC último válido no caminho de encaminhamento.

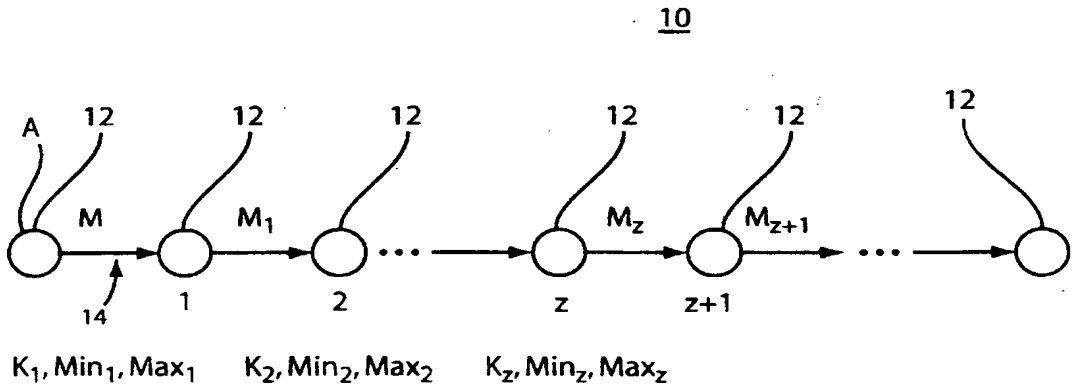

10
A
12
12
12
12
12
12
M
M1
Mz
Mz+1
14
1
2
z
z+1
K1, Min1, Max1
K2, Min2, Max2
Kz, Minz, Maxz

FIG. 1

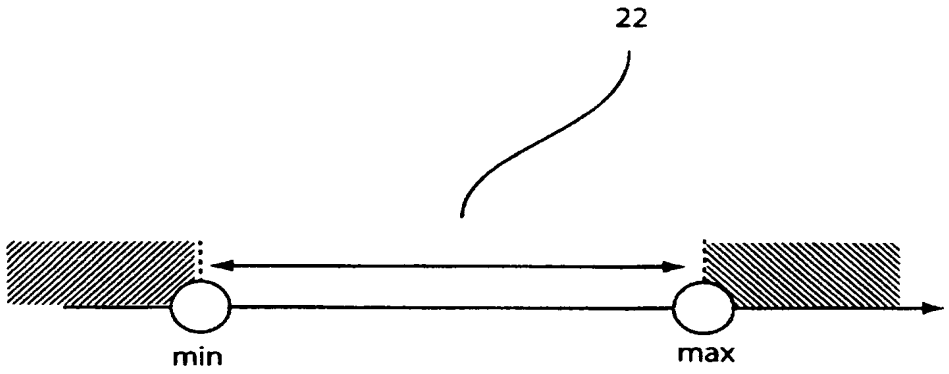

22
min
max

FIG. 2

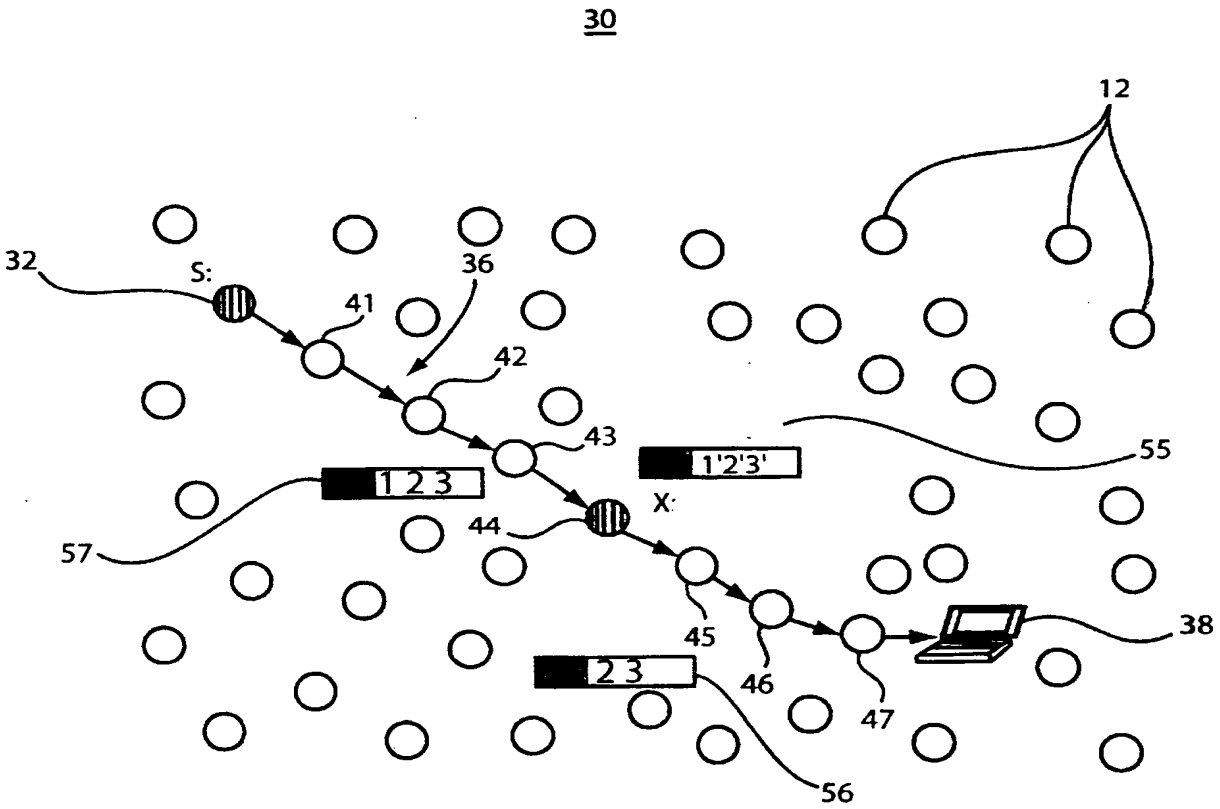


FIG. 3

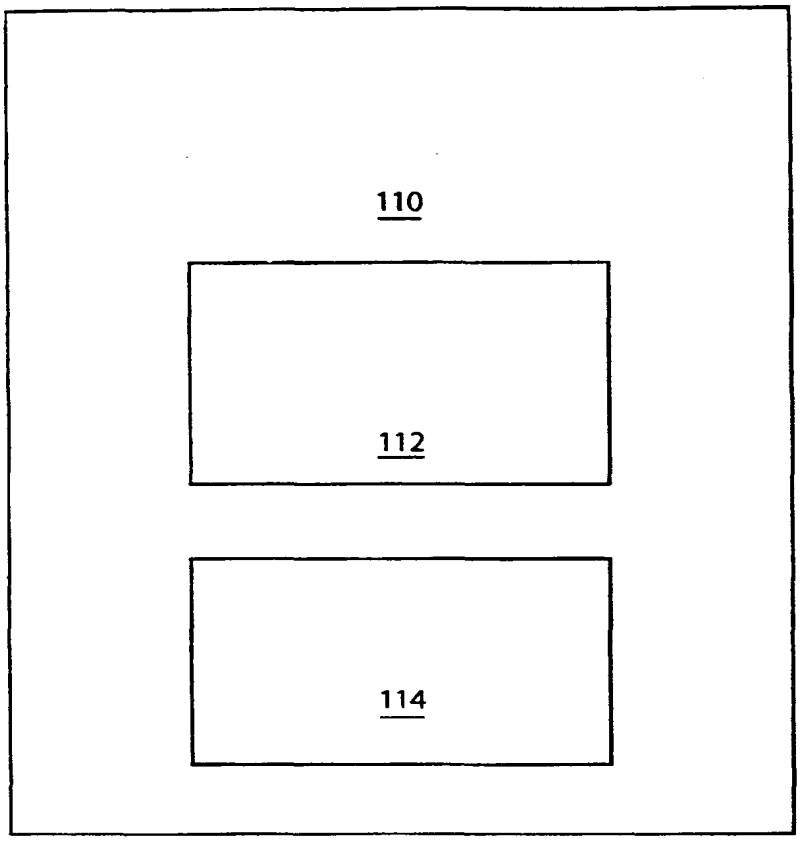


FIG.4

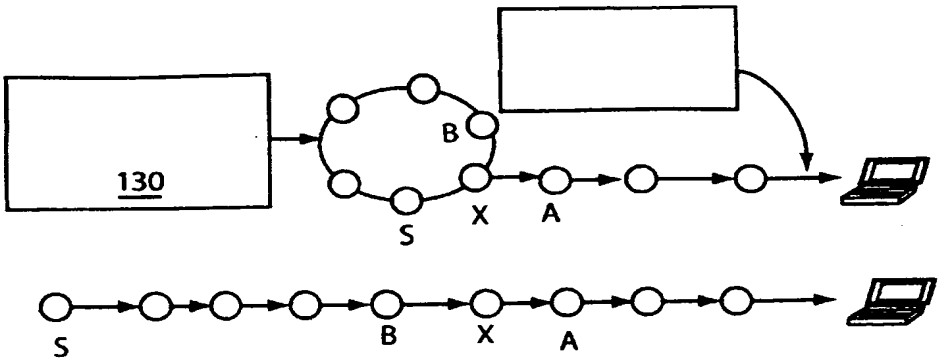


FIG. 5

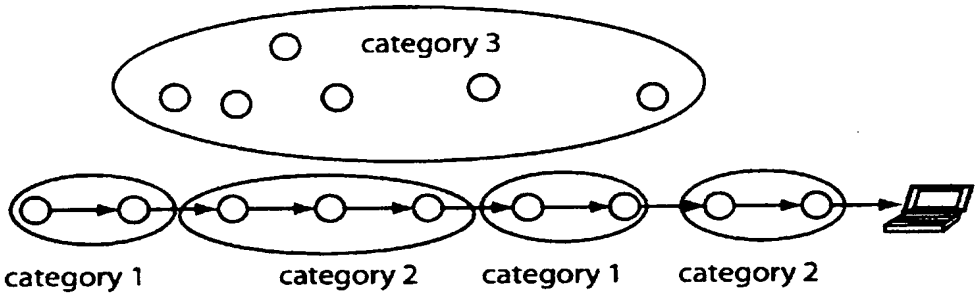


FIG. 6

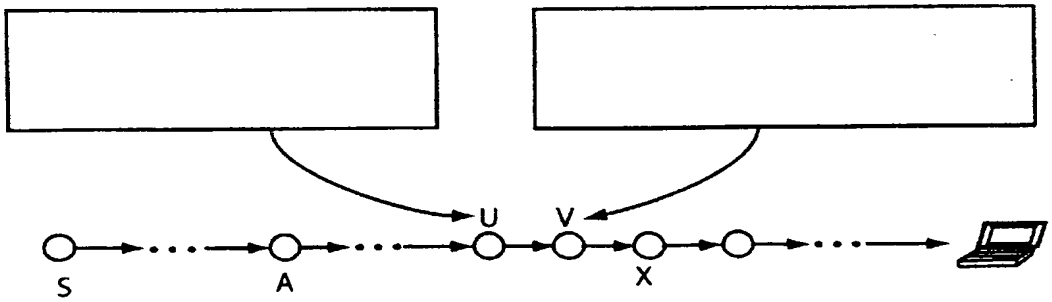


FIG. 7

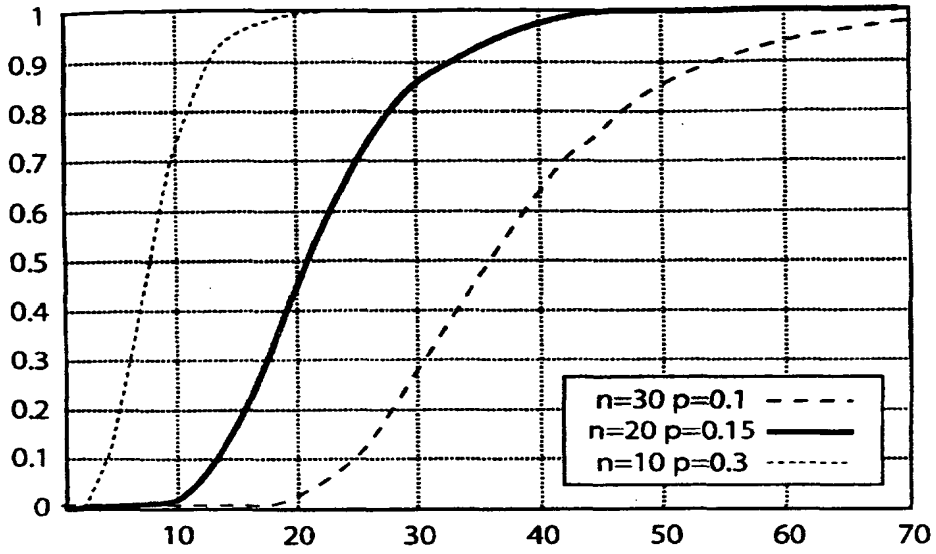

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
10
20
30
40
50
60
70
n=30 p=0.1
n=20 p=0.15
n=10 p=0.3

FIG. 8

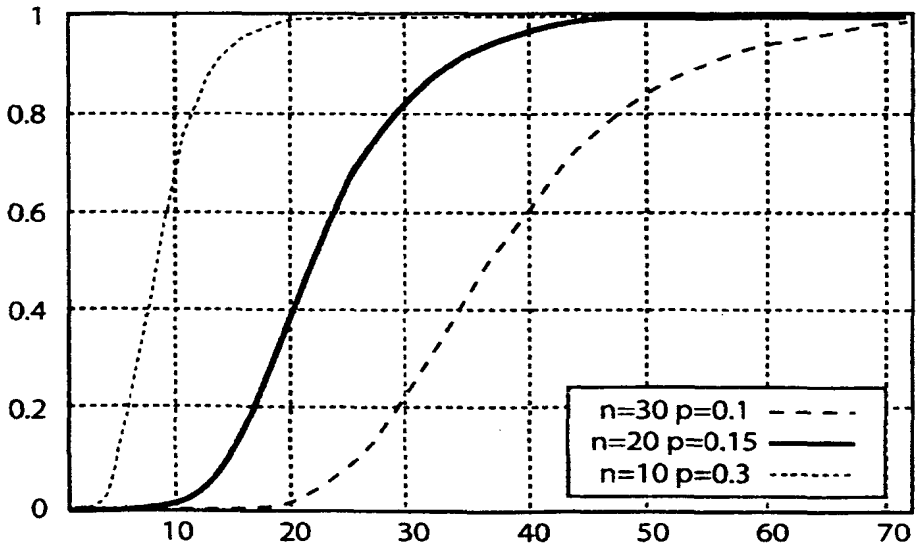

1
0.8
0.6
0.4
0.2
0
10
20
30
40
50
60
70
n=30 p=0.1
n=20 p=0.15
n=10 p=0.3

FIG. 9

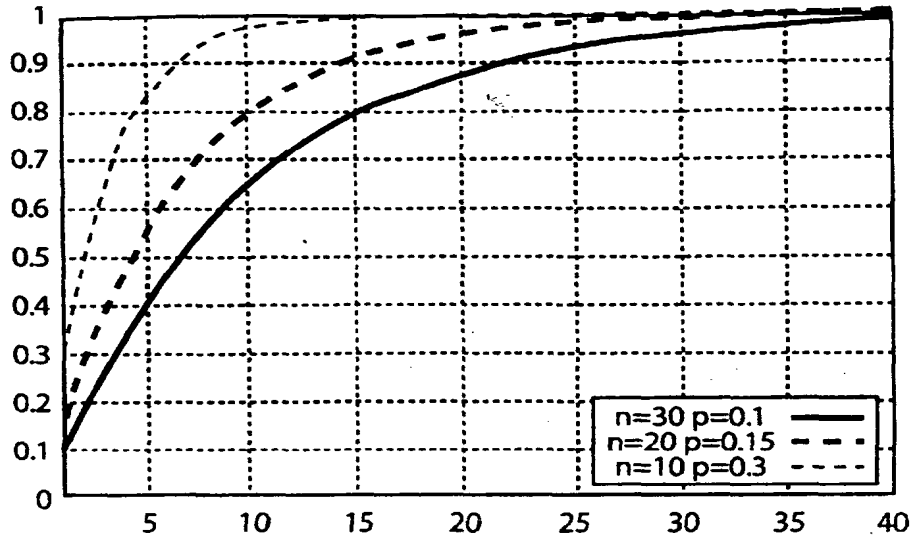

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
5
10
15
20
25
30
35
40
n=30 p=0.1
n=20 p=0.15
n=10 p=0.3

FIG. 10

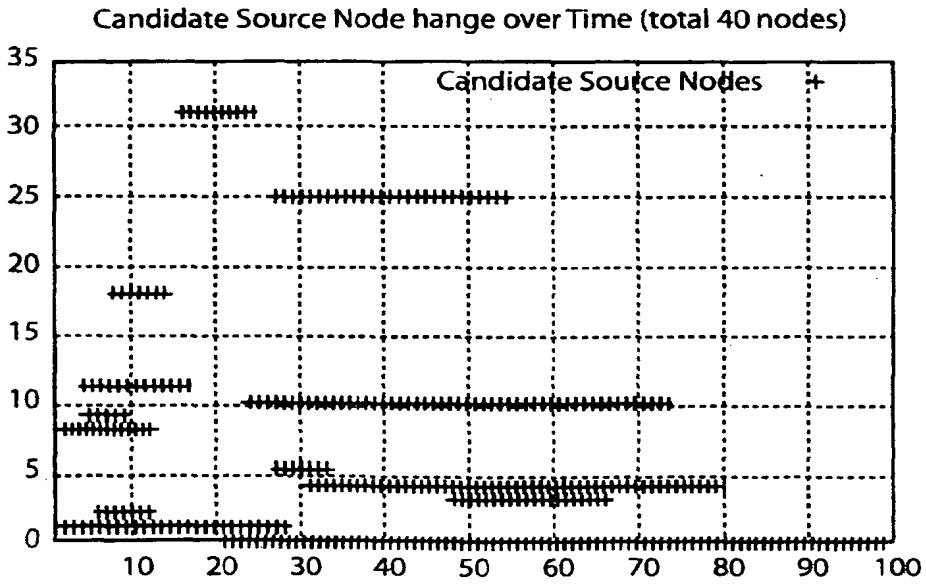

Candidate Source Node hange over Time (total 40 nodes)
Candidate Source Nodes
35
30
25
20
15
10
5
0
10
20
30
40
50
60
70
80
90
100

FIG. 11

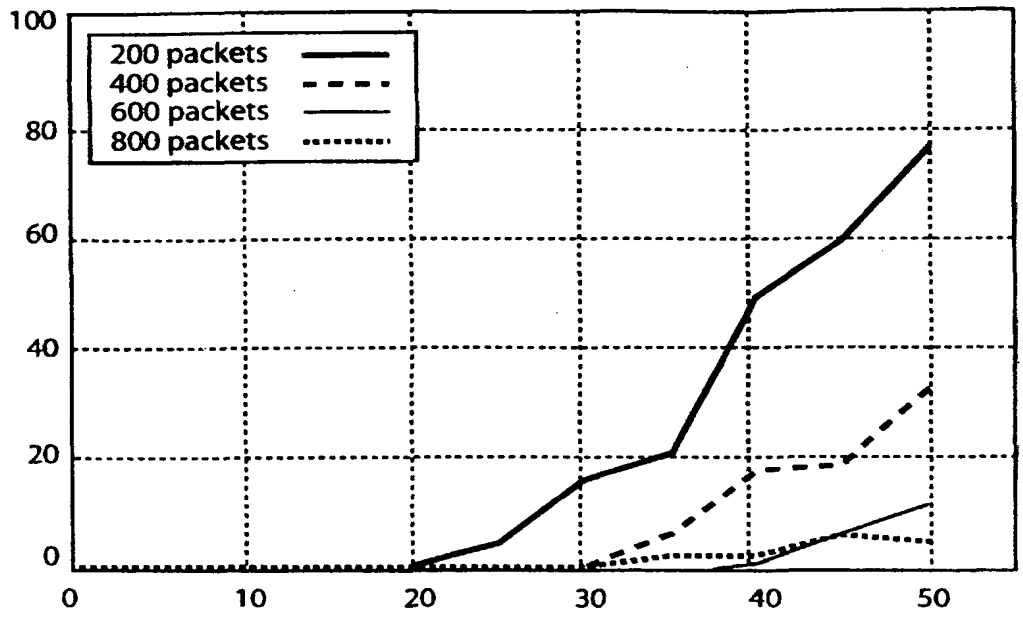

100
80
60
40
20
0
0
10
20
30
40
50
200 packets
400 packets
600 packets
800 packets

FIG. 12

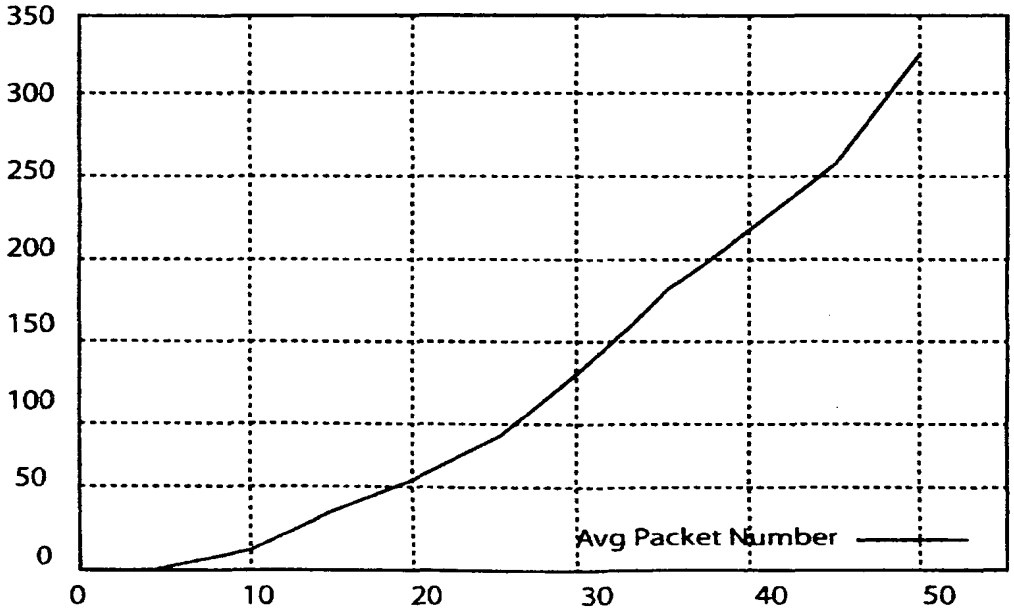

350
300
250
200
150
100
50
0
0
10
20
30
40
50
Avg Packet Number

FIG. 13

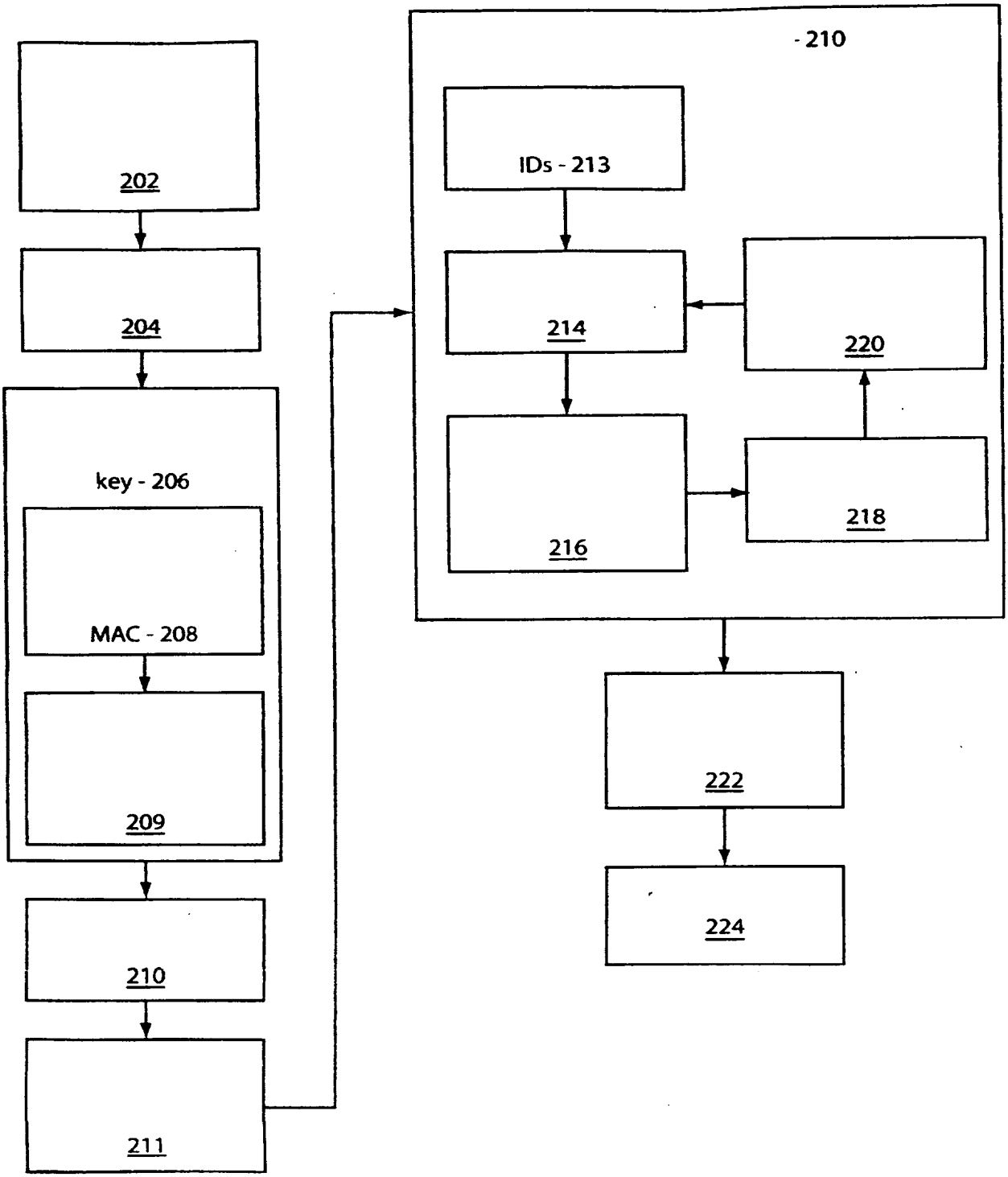

202
204
key - 206
MAC - 208
209
210
211
- 210
IDs - 213
214
220
216
218
222
224

FIG. 14

RESUMO

Um sistema e método para rastreamento de pacotes em uma rede inclui a manutenção de um número de identidade (ID) para cada nó em uma rede e gerando uma assinatura (por exemplo, um código de autenticação de mensagem (MAC)) usando uma chave secreta compartilhada entre cada nó em um caminho de encaminhamento e uma pia. Cada nó de encaminhamento deixa uma marca, anexando seu ID e uma assinatura no pacote, quer de uma forma determinista, ou com uma probabilidade. Ao receber um pacote na pia, correção das assinaturas em cada pacote é verificada na ordem inversa em que essas assinaturas foram acrescentados. A última MAC válido é determinada no caminho de encaminhamento para determinar a localização dos gânglios comprometidos que conspiram em dados falsos ataques de injeção.