# Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach [*]

Xiaoxin Wu
Intel China Research Center Ltd
Beijing, China
xiaoxin.wu@intel.com

David K. Y. Yau
Department of Computer Science
Purdue University
West Lafayette, IN 47907, USA
yau@cs.purdue.edu

## ABSTRACT

Defending against denial-of-service (DoS) in a mobile ad hoc network (MANET) is challenging because the network topology is dynamic and nodes are selfish. In this paper, we propose a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification. Since nodes are selfish, they may not perform the verification so that they can avoid paying the overhead. A bad packet that escapes verification along the whole network path will bring a penalty to all its forwarders. A network game can be formulated in which nodes along a network path, in optimizing their own benefits, are encouraged to act collectively to filter out bad packets. Analytical results show that Nash equilibrium can be attained for players in the proposed game, in which significant benefits can be provided to forwarders such that many of the bad packets will be eliminated by verification.

## 1. INTRODUCTION

The dependencies between dynamic, mutually untrusted neighbors in a mobile ad hoc network (MANET) create important security concerns in such networks. Among the attacks documented in the literature, denial-of-service (DoS) attacks are particularly damaging since both communication bandwidth and node resources are scarce in MANETs. In addition to their ability to take down a network quickly, DoS attacks directed at bandwidth and end node resources are easy to launch; e.g., by simply injecting useless traffic into the network.

DoS mitigation techniques designed for wireline networks will not work well in an ad hoc environment where the routes and the set of forwarders on a routing path are highly dynamic and are selfish. Secure routing protocols designed for ad hoc networks [3] build secure routes to support end-to-end communication. If link layer security is applied [4], these protocols can mitigate DoS attacks. Illegitimate packets will be discovered as outside attackers do not know the keys shared between the hops. However, an inside attacker, i.e., an attacker who is a member of the end-to-end path, can still launch an attack. Without using signatures, it is difficult to identify the attacker even if the attacker is known to be an insider. In addition, in networks where packet delivery is route-based, these secure routing protocols cannot be applied because the path can change from packet to packet.

Motivating nodes to serve each other is another fundamental issue in MANETs. Specifically, as communication endpoints rely on intermediate nodes to forward their traffic, incentives for the forwarders have to be provided. Traditional incentive systems have used nuggets [2] and reputation credits [1] to encourage nodes to function as forwarders. The incentive issue becomes even more relevant in the security context, when security measures may require certain nodes to expend more resources to better defend other nodes. The incentive issue as it relates to the security issue has been less addressed by the research community.

In this work, we propose a DoS mitigating technique for MANETs that jointly considers the security and incentive issues. The technique is designed to work in a packet-switching network environment. The idea is based on an attacker's goal to avoid detection and being identified. Hence, we protect legitimate packets by requiring them to be signed by their respective senders. A forwarder verifies a packet's sender signature when the packet is received. If the verification fails, the packet is dropped. Otherwise, it is forwarded.

We assume that network nodes are selfish but rational. Incentive for a node to forward packets is given by a reward the node will obtain after the packets are successfully delivered to their final destinations. A forwarder may also choose to forward a packet without verification, since the operation carries a cost. To motivate a forwarder to verify, a penalty is assessed for a "lazy" node each time it forwards an attacker packet that finally reaches the destination. We will investigate the properties of the resulting game, as forwarders independently attempt to play a best forwarding / verification strategy that will maximize their own payoffs, while the network is subject to given inputs of attacking and legitimate traffic.

We use game theory to study how a system of forwarders can be motivated to forward good packets while filtering out bad packets cooperatively by verification. We will propose solutions that address jointly the security and incentive issues. We will discuss how practical cost functions can be assigned for sending, forwarding, receiving, and verifying

[*] Research supported in part by the U.S. National Science Foundation under grant number CNS-0305496.

*ASIACCS'07,* March 20-22, 2007, Singapore.
Copyright 2006 ACM 1-59593-574-6/07/0003 ...$5.00.

packets.

# 2. GAME THEORETIC DOS MITIGATION IN MANET

## 2.1 Mitigating DoS in MANET

We require that legitimate sources digitally sign their packets. Other than the network level routing information and the application level data payload, each packet will also carry a signed MAC (Message Authentication Code), including a certificate for the originator's public key. The signed MAC with the certificate is used to verify that the packet is from the claimed legitimate source. If the MAC carried in the packet does not match the MAC a forwarder generates from the received packet, the packet is classified as a bad packet and therefore dropped.

The signature-based defense is prone to the replay attack. An attacker can replay a legitimate packet a large number of times to generate a high load of useless traffic. These packets will pass the verification step. To deal with the replay attack, a packet should be stamped with its generation time. In addition, each packet has a given lifetime. A packet whose life time has expired will be dropped. To prevent a malicious node from sending a legitimate packet to different next hops during the packet's lifetime, a neighbor monitoring technique can be used. In neighbor monitoring, a node reads the complete header, including both the MAC and network level headers, of every packet even if the node is not the packet's next hop. The node stores the header read until the corresponding packet's lifetime expires. Upon hearing a packet whose lifetime has not expired, the node will compare the header read with the headers currently in the node's local store. By doing this, the node can detect a replayed packet and drop it before further damage to the network happens. Since only the packet header, but not the whole packet, has to be read, the cost of monitoring will be kept low. If the packet lifetime is not too long, which is normally the case in ad hoc networks, a node will not need to store too many packet headers, which reduces the storage cost. Note that the monitoring technique will not be effective in a wireline network if attackers select different routes for sending different replayed packets, since one forwarder will then be unable to monitor packets destined for another forwarder.

Fig. 1 shows the proposed packet format. In the figure, the previous hop is the node forwarding the packet, and the next hop is the node designated as the receiver of the forwarded packet.

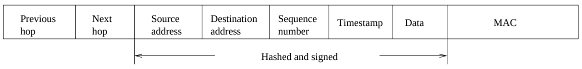

**Figure 1: packet format.**

If every forwarder verifies packets before forwarding them, any attack traffic will be discovered and dropped to limit its damage to the network. In particular, end servers are expected not to receive any attack packet. Network bandwidth will also be largely protected. However, verifying every packet at every forwarder causes unnecessarily high loads at the forwarders, especially when a large fraction of the packets is legitimate.

To reduce the costs of verification, without severely compromising its effectiveness, a forwarder may decide to probabilistically verify a packet. Since nodes are selfish, we need to incentivize them to verify with sufficiently high probabilities.

## 2.2 Incentives and game rationality

We apply a reward system in which nodes are given credit for acting as forwarders. Specifically, a forwarder is credited for forwarding a packet if the packet successfully arrives at the destination.

We assume the existence of an accounting system, similar to a "central bank", for securely keeping track of the rewards, and preventing cheating in claiming false rewards. In our DoS mitigation approach, the signed MAC of each forwarded packet is stored at the forwarder. The stored MACs can be presented to the accounting system as evidence for collecting rewards.

In the DoS resilient forwarding game, a node's payoff is the reward for forwarding minus the forwarding costs. The costs account for all expended resources in the forwarding, such as the energy consumed for packet receive and transmission, and for performing any required cryptographic operation.

In the DoS defense, forwarders verify the MACs of received packets. A selfish forwarder may try to maximize its payoff by not verifying, but rely on another forwarder on the packet's route to verify and accomplish the job of filtering out any attack packet. Clearly, if every forwarder reasons in the same way and avoids all verification, then all attack packets will be allowed to reach their destinations. To avoid the degeneration of the DoS defense into a system in which no verification is performed at all, a forwarder is punished for forwarding a bad packet that successfully makes it to the destination. Hence, if a forwarder presents the MAC of a bad packet in claiming its reward, a penalty instead of a reward will be given. The penalty subtracts from the node's total credit for forwarding other good packets.

We formulate the DoS resilient packet forwarding system as a multiplayer game between forwarder nodes in a MANET. Forwarder nodes take part in the same game if they are on the same route between a sender and receiver. Since routes in a MANET can be highly dynamic, the set of nodes playing against each other can change often. As discussed, a player's payoff in the game is its reward for forwarding the good packets, less its penalty for forwarding the bad packets and its costs of forwarding and verification. A player's strategy is its probability of verifying a received packet. The player's strategy may be adaptive so that the probability of verification may change over time.

## 2.3 Game Formulation: Reward, cost, and penalty

A forwarder may perform the following operations: (1) forwarding a packet without verification, (2) verifying and forwarding a legitimate packet, and (3) verifying and dropping a bad packet. Let $G$ be the reward for a forwarder if it has forwarded a legitimate packet, and the packet is successfully delivered to the destination. Let $C_p$ be the penalty for a forwarder if it has forwarded a bad packet without verification, and the packet reaches its destination. Let $c_r$, $c_t$, and $c_v$ be the costs for packet receive, transmit, and signature verification, respectively.

When a forwarder forwards a legitimate packet, its payoffs are $g_1 = G - c_r - c_t$ and $g_2 = G - c_r - c_t - c_v$ for the cases of verification and no verification, respectively. If a forwarder verifies a bad packet and then drops it, the forwarder has a payoff of $g_3 = -(c_r + c_v)$. If a forwarder forwards a bad packet without verification, its payoff is either (1) $g_4 = -(c_r + c_t)$, if the packet is verified and dropped by a forwarder later in the route, or (2) $g_5 = -C_p - c_r - c_t$, if the packet finally arrives at the destination.

## 2.4 $n$-player game

In formulating the $n$ player game, we assume that each forwarder on a network path knows that the path has $n$ hops. However, a forwarder does not know its position on the path; i.e., it does not know how many hops it is away from the source or the destination. In the game, each forwarder plays against the other $n-1$ forwarders. Since all the forwarders know the same information, they are treated as homogeneous and hence will use the same strategy.

We denote $p_{att}$ as the probability that a packet is an attacking packet. We assume that upon receiving a packet, a forwarder verifies the packet with probability $p_v$. Nash equilibrium will be reached only if under $p_v$, the expected payoff for the forwarder remains the same whether it verifies the packet or not. Mathematically, the relationship can be given as follows:

$$\begin{aligned}(1-p_{att})g_2 + p_{att}g_3 = (1-p_{att})g_1 + \\ p_{att}((1-p_v)^{n-1}g_5 + (1-(1-p_v)^{n-1})g_4).\end{aligned} \tag{1}$$

The left hand side is the expected payoff when the forwarder verifies the packet. The right hand side is the expected payoff when it does not verify the packet, while the remaining forwarders will verify with probability $p_v$. The number of forwarders on the path is $n$. Based on Eqn. (1), $p_v$ can be calculated as

$$p_v = 1 - \left(\frac{(1-p_{att})(g_2-g_1) + p_{att}(g_3-g_4)}{p_{att}(g_5-g_4)}\right)^{\frac{1}{n-1}} \tag{2}$$

The expected payoff of a player in this game can be calculated as

$$G = (1-p_{att})g_2 + p_{att}g_3. \tag{3}$$

Notice that the expected payoff of each forwarder is the same as the expected payoff if the forwarder verifies every packet. However, under the proposed game, a forwarder obtains the same gain with less consumed resources because the payoff deduction is partially caused by the penalty. This keeps the forwarders operational in the network for a longer time, by conserving nodal resources.

## 2.5 Analytical Results

In Fig. 2 we show the payoffs at a forwarder, and in Fig. 3, we show the probability that an attacking packet can reach the destination. For comparison, we also show the cases when the optimum strategy is used under the assumption that nodes are collaborative, and when the worst strategy is used under the assumption that a node just forwards packets without doing anything. The results indicate that the game-theoretic approach can successfully mitigate DoS attacks.

# 3. CONCLUSIONS

We have proposed a signature-based DoS mitigation system for mobile ad hoc networks. The system defines a game in which forwarders will probabilistically verify packets received for forwarding, and hence will have a chance to drop bad packets sent by attackers. We have formulated different forms of the game for different network scenarios, and analyzed the corresponding payoff, effectiveness, and Nash equilibrium properties. We have showed that the games can induce useful DoS mitigation effects. It is also shown that key game parameters, such as the penalty for forwarding a bad packet without verification, can affect the probability that a node will verify a received packet.

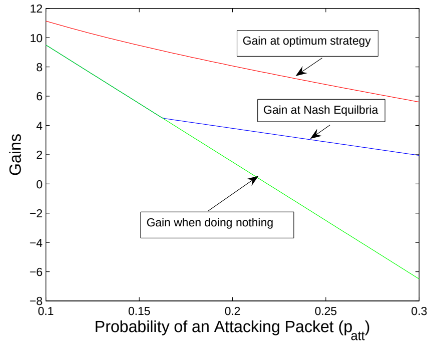

**Figure 2: Payoffs at Nash equilibria.**

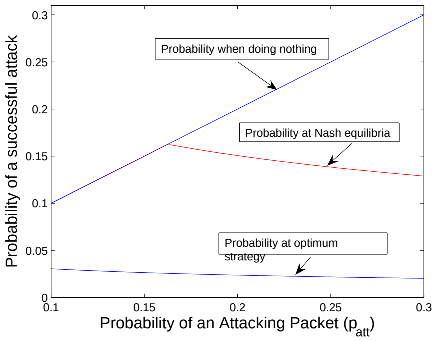

**Figure 3: Probabilities of a successful attack.**

# 4. REFERENCES

[1] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the confidant protocol. In *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002.

[2] L. Buttyan and J. Hubaux. Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks. In *Technical report, EPFL*, 2001.

[3] Y.-C. Hu, D. B. Johnson, and A. Perrig. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of Mobicom*, 2002.

[4] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proceedings of ICNP*, 2001.