Short Paper: Fellowship in Mobile Ad hoc Networks

Venkatesan Balakrishnan and Vijay Varadharajan

Information and Networked System Security Research Group
Department of Computing
Macquarie University
Sydney Australia
{venkat, vijay}@ics.mq.edu.au

Abstract

Security issues are paramount in mobile ad hoc networks even more so than in wired networks. Though there have been many works in the recent years on secure routing protocols for mobile ad hoc networks still ad hoc networks are prone to specific attacks such as packet drop attacks. In this paper, we bring out the vulnerabilities and seriousness of the packet drop attacks. We propose an obligation based enforcement approach called “fellowship” to defend the packet drop attacks in mobile ad hoc networks.

1. Introduction

Mobile ad hoc network’s distinct advantage relies on its ability to establish communication in the absence of an infrastructure and the capability to communicate beyond a node’s wireless transmission range. However security issues are still a major concern in mobile ad hoc networks.

Nevertheless, many approaches [1-4] are proposed to secure the communications in order to achieve secure delivery of information; still ad hoc networks are susceptible to specific attacks such as packet drop attacks. Actually the packet drop attack hinders achieving a secure and reliable communication. The severity of packet drop attack is such that if performed by both malicious and selfish nodes, it may bring down a functional mobile ad hoc network to a stand still.

Our main objective in this paper is to address the packet drop attack launched by malicious and selfish nodes. In doing this, we propose an obligation based enforcement technique, which we call as the fellowship to mitigate packet drop attacks.

Section 2 addresses the seriousness of packet drop attacks in the presence of secure routing approaches. Section 3 explains our proposal and how packet drop attacks can be defended. We put forth our extensions in Section 4 and the provide some concluding remarks.

2. Seriousness of Packet Drop Attack

In general, the approaches [1- 4] proposed to secure routing in ad hoc networks assume that the participants hold pre-shared information before the initial stages of network deployment. Then the proposals take advantage of the pre-shared information to establish a new approach to secure routing. However, these approaches do not deal with packet drop attacks. Like the base routing protocols, secure routing approaches also anticipate the participating nodes to contribute significant amount of their resources to forwarding others’ packets.

In reality, the intensity of the packet drop attack in mobile ad hoc networks rises due to the presence of selfish nodes. These nodes, unlike other normal nodes, withdraw from performing the network operations to save their resources. Though their intention is completely different from malicious nodes, their actions are in coherence with the malicious nodes in this regard. The gravity of the packet drop event exponentially increases when selfish nodes coupled with malicious nodes exploit the persisting vulnerabilities of the medium such as the sporadic links and the dynamic topology. This portrays the impact of each node’s participation on the functioning of network. The magnitude of this issue in fact makes it even a higher priority than securing the network because security is needed only when the network is functional to begin with.

3. Proposed Approach

3.1. Background

Very few researchers have proposed solutions to handle the packet drop attacks. Nuglets[5] stimulates nodes to forward others packets using virtual currency. The use of tamper-resistant hardware makes this proposal unattractive in spite of its efficiency.
Alternatively, Sprite [6] eliminates the use of tamper-resistant hardware to stimulate cooperation among the selfish nodes. The need to have a central authority and falling short to consider malicious node’s packet drop causes Sprite to be a non-generic proposal. On other hand CONFIDANT [7] targets to achieve secure routing amidst packet drop attacks. However, the likelihood of selective misbehaviours by malicious nodes due to list blow-up and lack of well-defined trust management to resolve the conflicts arising when two friends report each other to be malicious, make this proposal somewhat ineffective.

Unlike CONFIDANT, we distinguish the requirements for secure mobile ad hoc networks at two levels: availability and security [8]. We believe that addressing packet drop attacks assures the availability of the network ultimately yielding an operative functional network. Once the network is operational, any secure routing approach can be deployed over the available ad hoc networks to achieve security.

3.2. Overview

In this paper, we propose a mechanism based on enforcement and obligation to attain a functional network. The enforcement function is built on the fact that every participating node in the network is “obligated” towards the operation of the network. In return, this obligation enables each participating node to derive mutual contribution from other peers. The enforcement ends in a condition where nodes share similar interests, ideals, or experiences, as by reason of participating in the network on equal terms. Indeed, neighbourhood monitoring technique serves as the catalyst to achieve all these.

All the nodes operate in promiscuous mode embraced due to the broadcast nature of the radio channel, which makes each transmission to be received by surrounding neighbours. The network may contain heterogeneous nodes with different energy level and computational power. We consider source initiated on-demand protocol for the base routing operations.

3.3. Fellowship of the Network

The assumption that the neighbours will forward the transmitted packets fails to hold particularly in resource-constrained mobile ad hoc networks. In general, a packet may be dropped for various reasons [9]. For any node to deliver a packet, contribution from the neighbourhood (which is a network service) is essential. In return to stay as a member in the network, we enforce the participant to render similar service to the neighbourhood for the exploited services, which is actually an obligation towards the neighbouring nodes. Thus there is no need to charge a node or to pay incentives. The obligation lays the seed for significant level of sociability in the network. To the question as to how this obligation is enforced, our approach relies on the neighbourhood monitoring: intentional packet drops are uniquely identified and the non-contributing node is given demerit points, so that the node is excluded from deriving more network services. We collectively call this as the “fellowship of the network”.

The fellowship also helps to increase the average lifetime of the network.

Formally we define the “fellowship of the network” as, “the obligation enforced on the participating node to contribute a significant level of its own resources for the functioning of the network, in order to derive similar service from the network’s sociability. The contribution is proportional to the node’s potential, the period it stays in network and the type of association it has with requesting node. Alternately, detection of intentional non-contribution invites severe demerits resulting in expulsion”. Selfish or malicious nodes performing intentional packet drops basically deny the “fellowship of the network” and hence we call the packet drop attacks performed by them as “fellowship denial attack”.

3.4. Choice of Threshold for Fellowship

For simplicity in this paper, we consider only the energy level of participants as the potential and show how the threshold (on which the fellowship rests) is designed. Prior to network operation, the initial energy ‘E_A’ in a node A is in two parts (Equation 1). One part is for self-operations such as receiving packets, transmitting self-generated packets and mobility, which is bounded by the weight ‘C_{SELF}’. The second part, ‘C_{CON}’ decides on the proportion of energy contributed for the network service. The contribution is equivalent to the summation of pre-defined assignment of energy for ‘x’ known nodes and ‘y’ unknown nodes in a network of ‘n’ nodes. This contribution is represented as $E_{A, \text{FORWD}}(T)$ in Equation (2).

For example, if only one packet is forwarded by node A for node B since the time ‘t’, then the fraction of energy remaining at node A in favor of node B is governed by the factor ‘$\delta$’, given in Equation (3). ‘$\delta$’ denotes the fraction of energy committed in forwarding the packet. Conversely from Equation (4), if node B performs fellowship denial attack to node A, then B collects demerit points at A given by the factor ‘$\lambda$’.

A packet is forwarded, only if the requesting node meets the threshold at the forwarding node. The threshold is different depending upon whether the requesting node is already known or unknown. In any case, the threshold ‘$E_{A,B}(t)$’ at node A for node B, is given as the ratio of fraction of energy ‘$e_{AB}(t)$’ committed for node B, to overall energy $E_{A, \text{FORWD}}(t)$ contributed towards the network.
In Equation (5), 'p' is the total number of packets forwarded by node A for node B, 'q' is the total number of node A’s packets dropped at node B and 'r' is the total number of packets forwarded by node A for rest of nodes in the network, inclusive of node B. From Equation (7), we could infer that forwarding node’s threshold (on which the “fellowship of the network” rests) for any requesting node is influenced by the total number of (forwarding node’s) packets dropped at requesting node to the total number of (requesting node’s) packets transmitted at forwarding node. We recommend $\lambda > \delta$ for a strict fellowship.

### 3.4. System Operation

Whenever a node X receives a packet for re-transmission from a node Y, node X ascertains node Y’s familiarity. If node Y is unknown, node X should exhibit fellowship based on the assigned threshold for strangers. Alternatively, node X may drop the packet as a result of faults such as packet error and buffer overflow, which cannot be trapped by node Y’s monitoring. Hence, we explicitly configured node X to broadcast a one-hop restricted route reply as a STATUS_MSG to eliminate the uncertainty. The commitment of resources to broadcast STATUS_MSG infers that node X did not perform fellowship denial attack; otherwise, it could have forwarded the requested packet for the same commitment. However, if node X performs “fellowship denial attack” it collects double demerit points: losing credentials equivalent to $\lambda$ at node Y and additionally missing an opportunity to derive service equivalent to $\delta$ from node Y.

In contrast, if node Y is known then its past actions are taken into account. If node Y is blacklisted, then node X drops the requested packet and never generates a STATUS_MSG because losing merit points at the malicious end do not affect the node X anyway. However, if node Y is above the threshold and provided node X is free from buffer overflow, then the packet is forwarded.

### 4. Concluding Remarks

Though our proposal addresses packet drop attacks performed by selfish and malicious nodes, it falls short when selfish and malicious nodes occupy the channel. Coupled with rate-limiting techniques and inclusion of more parameters for a node’s potential, we anticipate the fellowship model to be robust against the attacks that exploit the availability of mobile ad hoc networks.

In this paper, we have shown the vulnerabilities and seriousness of the packet drop attacks. We have proposed an obligation based enforcement mechanism called fellowship to defend the packet drop attacks in mobile ad hoc networks.

### 5. References


