Impact of Trust-based Security Association and Mobility on the Delay Metric in MANET

Dang Quan Nguyen, Mylène Toulgoat, and Louise Lamont

Abstract: **Trust models in the literature of MANETs commonly assume that packets have different security requirements. Before a node forwards a packet, if the recipient's trust level does not meet the packet's requirement level, then the recipient must perform certain security association procedures, such as re-authentication. We present in this paper an analysis of the epidemic broadcast delay in such context. The network, mobility and trust models presented in this paper are quite generic and allow us to obtain the delay component induced only by the security associations along a path. Numerical results obtained by simulations also confirm the accuracy of the analysis. In particular, we can observe from both simulation's and analysis results that, for large and sparsely connected networks, the delay caused by security associations is very small compared to the total delay of a packet. This also means that parameters like network density and nodes' velocity, rather than any trust model parameter, have more impact on the overall delay.**

Index Terms: **Delay analysis, depoissonization, mobility, security association, trust.**

I. INTRODUCTION

In recent years, the success of research in mobile ad hoc networks (MANETs) has led to the development of new applications in military and civilian domains such as wireless sensor networks and mobile device comfort. For examples, cheap devices can be deployed in a hostile environment to monitor and report on enemy's activities, or authentication-capable controllers can be embedded in the equipment of each deployed unit to restrict their use to the authorized owner.

The device confort is studied in [1]. When operating in a distributed environment, the proper working order of these devices can only be guaranteed if there is a system to monitor the *trustworthiness* of each device. One can imagine a sensor being captured and modified to ignore intrusion, or a weapon being stolen and its authentication controller replaced. Therefore, besides the fact that these devices must be authenticated at the network's deployment phase, it could be considered suspicious if at anytime during an operation, a device is reported by its peers to be missing, turned off, or simply disconnected from them.

Proximity-based trust has been designed to address this situation in distributed environments such as MANETs. Basically, each node monitors the connectivity with its neighbours and assigns a trust value to them. If two nodes lose connection with each other, then the trust value between them will start decaying at a rate proportional to the time they are disconnected. The purpose of trust decay is merely preventive since no evidence of an actual intrusion or attack is collected when nodes are out of each other's sight. A trust management system could also implement an authentication procedure, forcing nodes with a low level of trust to re-authenticate. This procedure is known as *security association* (SA) or *security handshake*.

It is worth mentioning that our intention is not to cover the security issues that arise in the Internet with machines being infected by malware or spyware. Indeed, in such scenarios, the malicious nodes would try to stay connected as long as possible in order to infect as many other nodes as they can. Also, such systems cannot be thought as MANETs since they usually have a fixed and centralized infrastructure with strong authentication mechanisms.

When studying such systems, communicating nodes are assumed to be disconnected from each other during most of the time. A packet travelling on a path is usually buffered at each intermediate node, then forwarded to the next hop, after the two nodes meet and perform the security handshake whenever required. This is a variant of the delay tolerant networks, with consideration for proximity-based trust relationship. The forwarding process is often called *store-carry-forward*.

Objective and contributions:

We analyze in this paper the delay of epidemic broadcast for MANETs enhanced with the trust-based security association. While the delay of epidemic broadcast in MANETs has been extensively researched, the novelty of this paper consists in taking into consideration the extra delay induced by SA procedures, if the nodes along the path need to perform a security handshake. The contributions of our work are:

1. A mathematical model that allows for analyzing the delay of epidemic broadcast in a MANET where packets have different levels of security requirement.
2. An expression for the asymptotic delay of epidemic broadcast in such context. In particular, we obtain the delay component that is induced only by the security handshakes along a path.

Related work:

In [2], the authors present an architecture for managing SAs in MANETs. Each node has a state-machine to monitor the trustworthiness of the other nodes according to a customizable security policy (e.g., based on their identity, connection time, past behavior). Trust values decay with time and a security association is triggered if the trust level is low.

Delay of epidemic broadcast has been extensively studied in

Manuscript received October 3, 2013; approved for publication by Tae-Kyoung (Ted) Kwon, Division III Editor, December 1, 2014.

This work has been supported by the Defence Research & Development Canada (DRDC).

The authors are with the Communications Research Centre, Industry Canada, Ottawa, Canada, email: {dang.nguyen, mylene.toulgoat, louise.lamont}@crc.gc.ca.

Digital object identifier 10.1109/JCN.2016.000013