Adaptive Message Authentication for Vehicular Networks

Nikodin Ristanovic Panos Papadimitratos George Theodorakopoulos
Jean-Pierre Hubaux Jean-Yves Le Boudec
EPFL, School of Computer and Communication Sciences, Lausanne, Switzerland
firstname.lastname@epfl.ch

ABSTRACT

Public key cryptography can introduce significant processing delays in vehicular communication platforms. This can lead to serious performance issues, especially in the case of multi-hop Inter-Vehicle Communication. In this paper we propose Adaptive Message Authentication (AMA), a lightweight filtering scheme that reduces the number of cryptographic operations performed by the nodes. Based only on local observations and with no additional communication channel, our scheme achieves global improvement of network performance. We show through simulation that the scheme successfully adapts the number of cryptographic operations to the locally observed number of adversaries.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection; C.2.1 [**Network Architecture and Design**]: Wireless communication

General Terms

Algorithms, Performance, Security

1. INTRODUCTION

Current prominent efforts to secure inter-vehicle communication (IVC) rely on well-established cryptographic building blocks such as public key cryptography and Certification Authorities (CAs), and mandate that all vehicular communication (VC) messages are digitally signed and carry the certificate of the signing node (vehicle or Road-Side Unit (RSU)). This way, the authenticity of any message can be validated by receiving nodes.

Recent benchmarks [1] show that signature verification on a wide range of platforms takes significant amount of time, even for the fast elliptic curve algorithms. Due to on-board vehicle equipment cost, the currently envisioned VC boxes face the same limitations.

The solution we propose is an adaptive scheme which improves the overall performance of a vehicular network by allowing nodes to perform fewer message verifications. The scheme takes advantage of the fact that nodes in different parts of network face different security conditions at a given point in time (Fig. 1). We verify that the reduction in number of message verifications does not make the network more vulnerable to adversaries.

VANET'09, September 25, 2009, Beijing, China.
ACM 978-1-60558-737-0/09/09.

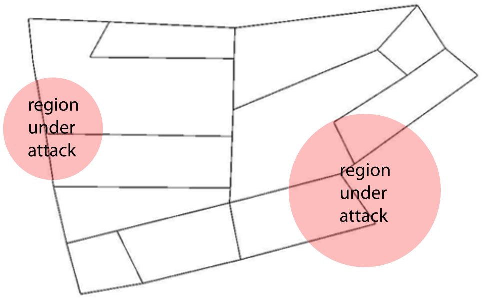

Figure 1: A few regions in the city are under attack; nodes in these regions actively defend. Nodes in other areas can relax their security.

2. SYSTEM AND ADVERSARY MODEL

We define L to be the set of legitimate nodes. During the lifetime T of the network, each legitimate node transmits at a constant rate of r_L messages/s. Let N_i be the total number of legitimate messages received by destination i. Then, we define the *goodput* γ_L as:

$$\gamma_L = \frac{1}{|L|} \sum_{i \in L} \frac{N_i}{T} \quad (1)$$

We consider two representative position-based forwarding algorithms: the Cached Greedy GeoCast (CGGC) [4] from the group of beacon-based unicast routing algorithms and broadcast-based Contention-Based Forwarding (CBF) [3].

Security Assumptions. In accordance with the state-of-the-art on secure VC [2], we assume that all messages are signed with an EC-DSA and that the sender's certificate is attached to enable message validation ("message checking"), i.e. certificate validation and sender's signature validation.

Adversary Model. We consider adversaries that do not have cryptographic keys certified by the CA. This implies that they cannot sign on behalf of legitimate nodes. Their goal is to reduce the goodput γ_L of legitimate nodes, by injecting forged messages and making the legitimate nodes waste their processing time on their verification. All adversarial nodes inject forged messages at a rate r_A messages/s. We define a as the percentage of adversaries in the network. The adversaries are aware of a and choose their sending rate r_A in order to minimize γ_L.

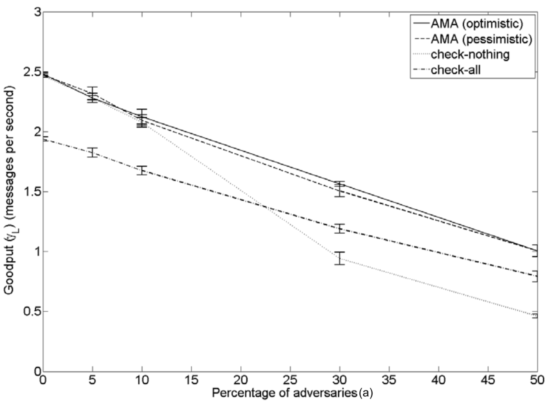

Figure 2: Goodput γ_L obtained under AMA, "check-all", and "check-nothing" for the CBF algorithm.

3. PROBLEM DEFINITION AND AMA

We define "check-all" and "check-nothing" as two extreme approaches that can be applied to messages that need to be relayed by nodes. "Check-all" is the default strategy in the existing proposals. It assumes checking of each relayed message. "Check-nothing" assumes that messages are not checked prior to relaying (only messages received in destination zones are checked). As we can see in Fig. 2 "check-all" is not the best approach for small percentages of adversaries in the network and "check-nothing" becomes very bad as the percentage of adversaries increases.

We propose Adaptive Message Authentication (AMA), an adaptive scheme for authentication and integrity check of messages exchanged between vehicles. Briefly, an AMA node can be in one of two modes: "check-all" and "relaxed." A node starts in "relaxed" mode. In this mode, a node checks with probability 1 the messages destined for itself, but only with probability p the messages destined for other nodes. If it detects a forgery, the node switches to the "check-all" mode. In the "check-all" mode, a node checks all messages with probability 1, and switches to "relaxed" mode only if c consecutive legitimate messages are received.

The rationale is that if a node senses that the current "temperature" of the neighborhood is low, it can relay most of the messages without prior authentication and keep authenticating only a small fraction of messages in order to ensure timely detection of security threats.

4. EVALUATION

Simulation Setup. We use SUMO traffic simulator and SWANS network simulator. A population of 600 vehicles moves in an area of 6 sq. km (Fig. 1). For the "check-all" and "check-nothing" approaches we run 20 simulations for every combination of $a \in \{0, 5, 10, 30, 50\}$ and $r_A \in \{0, 1, 2, 5, 10\}$ messages/s. For AMA we run 20 simulations for every combination of a, r_A, and AMA parameters $p \in \{0.05, 0.1, 0.2, 0.3, 0.5\}$ and $c \in \{20, 40, 60, 80, 100\}$. The legitimate node sending rate r_L is 1 message per second. The CGGC beaconing rate is 1 beacon/300ms.

AMA Parameter Selection. Having calculated γ_L achieved under AMA for all combinations of the parameters (p, c, a, r_A), we now show how to select p and c to maximize γ_L. When doing the selection, we have to keep in mind that the percentage a of adversaries is fixed and that the adversaries will learn the selected values of p and c, and choose r_A to minimize the goodput.

In the first case, which we call *pessimistic*, we do not know a. So, we select p and c that maximize the resulting γ_L against the worst case combination of a and r_A.

$$(p^*, c^*) = \text{argmax}_{(p,c)} \min_{(a,r_A)} \gamma_L (p, c, a, r_A) \qquad (2)$$

In the second, *optimistic* case, we know a but of course not r_A. So, for the given value of a, we will choose p and c that maximizes γ_L against the worst case reply r_A.

$$(p^*, c^*)(a) = \text{argmax}_{(p,c)} \min_{r_A} \gamma_L (p, c, a, r_A) \qquad (3)$$

In either case, the adversaries will choose r_A to minimize γ_L, given the legitimate users' choice of p^* and c^*.

$$r_A^*(a) = \text{argmin}_{r_A} \gamma_L (p^*, c^*, a, r_A) \qquad (4)$$

$$r_A^*(a) = \text{argmin}_{r_A} \gamma_L (p^*(a), c^*(a), a, r_A) \qquad (5)$$

Performance Evaluation. Fig. 2 shows the goodput obtained under the CBF routing algorithm (results for CGGC can be found in [1]), with the average over 20 simulations and error bars corresponding to one standard deviation.

Observe that the knowledge of a, i.e., the difference between the pessimistic and optimistic case, guarantees only a slight performance improvement. In the pessimistic case the goodput of legitimate nodes γ_L improves up to 30% for CBF. The performance gain is due to the reduced number of messages that are being checked by intermediate nodes (it drops up to 46%). For comparison, the performance gain in the case of CGGC is up to 33%, owing mostly to the reduction in the checking of beacon messages.

5. CONCLUSION

In this paper, we demonstrate that a simple, yet adaptive, filtering scheme that allows nodes to judiciously decide when to check the received message that requires further relaying, and when to simply forward it without any delay, brings significant performance gain. Our simulations with the state of the art in vehicular routing algorithms show that, as a result of security overhead reduction, the goodput of legitimate nodes increases up to 33%.

6. REFERENCES

[1] N. Ristanovic, G. Theodorakopoulos, P. Papadimitratos J-P. Hubaux and J-Y. Le Boudec. Adaptive Message Authentication for Vehicular Networks. Technical Report.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communications: Design and architecture. *IEEE Communcations Magazine*, Nov. 2008.

[3] H. Fuessler, J. Widmer, M. Kaesemann, M. Mauve, and H. Hartenstein. Contention-based forwarding for mobile ad-hoc networks. *Ad Hoc Networks*, 1(4):351–369, 2003.

[4] C. Maihöfer, Reinhold Eberhardt, and Elmar Schoch. CGGC: Cached greedy geocast. *2nd Intl. Conference on Wired/Wireless Internet Communication*, Frankfurt/Oder, Germany, February 4-6 2004.