Ad Hoc Networks 9 (2011) 418–429

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

# LEAPER: A lightweight reliable and faithful data packet relaying framework for VANETs ☆

Zhengming Li, Chunxiao Chigan *

*ECE Department, Michigan Tech University, United States*

ARTICLE INFO

*Article history:*
Received 18 June 2009
Received in revised form 12 March 2010
Accepted 30 July 2010
Available online 24 August 2010

*Keywords:*
Packet relaying
Faithfulness
Reliability
VANETs

ABSTRACT

In vehicular ad hoc networks (VANETs), it is vital to ensure reliable and faithful data packet relaying over multiple hops, which is critical to many VANET applications. In this paper, a novel Adaptive Role Playing (ARP) strategy is proposed to enable VANET nodes in each hop to countermeasure the malfunctions and misbehaviors of individual nodes. A lightweight reliable faithful data packet relaying framework (LEAPER) is proposed to implement the ARP strategy in each hop, so that each hop can reliably relay the authentic data packet to the next hop. Hop by hop, LEAPER ensures reliable and faithful data packet relaying from the source to the destination. In each hop the required security strength is configurable, making LEAPER flexible and adaptive to various application scenarios. Theoretical analysis and simulation studies show that LEAPER outperforms existing schemes in ensuring reliable and faithful data packet relaying.



## 1. Introduction

Vehicular ad hoc networks (VANETs) promise numerous applications to enhance driving safety and convenience [1–3], such as Collision Avoidance, Accident Warning, Event Reporting and Car-to-Home Synchronization, among which many rely on trustworthy multi-hop data packet relaying. However, in VANETs multi-hop packet relaying often suffers from various node misbehaviors and malfunctions, such as packet tampering and packet dropping. The resulting packet loss and tampered packet are seriously harmful to most VANET applications. For instance, the loss or tampering of a warning message about an accident may render the vehicles approaching the accident site unprepared for the potential dangers. Besides being harmful, tampered packets, once propagated throughout VANETs, are also a waste of the network resource.

Thus, *reliable* and *faithful* data packet relaying is vital to VANETs. Here, reliable relaying of a data packet means that this packet will certainly be relayed by each intermediate relaying node; faithful relaying requires that the data packet will not be tampered in each hop. Both requirements are necessary to ensure that the destination can receive the authentic data packets sent by the source. However, to our best knowledge, existing schemes for multi-hop communications in VANETs fail to meet both requirements. Briefly speaking (see Section 2.2 for details), general routing protocols [7,8] are mainly concerned with routing, ignoring the node misbehaviors and malfunctions. The contention-based forwarding protocols [9–14] pay no attention to data tampering, while the existing schemes for faithful packet relaying [5,6,15–17] generally ignore the reliability issue.

In this paper, a novel Adaptive Role Playing (ARP) strategy is proposed to allow the nodes in each hop to adaptively play the roles of a *relaying node* or *watchdogs* monitoring the relaying node, based on their capabilities for such roles and their neighbors' behaviors. Thus, if its current role is not played honestly by a misbehaving or

☆ This paper is partially supported by NSF CAREER Award (CNS-0644056).

* Corresponding author. Address: 712 EERC, 1400 Townsend Dr, Houghton, MI 49931-1295, United States. Tel.: +1 906 487 2494; fax: +1 906 487 2949.

*E-mail addresses:* zli1@mtu.edu (Z. Li), cchigan@mtu.edu (C. Chigan).

1570-8705/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2010.07.019

malfunctioning node, it will be taken over by the other honest nodes, so that as long as enough honest nodes exist in any hop, the data packet will be faithfully relayed eventually. As such, in principle, ARP can prevent the malfunctioning and misbehaving nodes from directly affecting the packet relaying in any hop, which is its major advantage over the existing schemes. A Lightweight Reliable and Faithful Packet Relaying Framework (LEAPER) is proposed to securely implement the ARP strategy, organizing the nodes in each hop into a trust group where each node's behaviors are monitored by its neighbors. Thus, reliable and faithful data packet relaying can be ensured in each trust group, based on which the end-to-end reliable and faithful packet relaying can be achieved.

Meanwhile, a configurable *security threshold k* determines the number of required watchdogs in each hop, tuning the tradeoff between the security strength and performance requirements of LEAPER and making LEAPER flexible and adaptive to various application scenarios. Theoretic analysis and simulation studies prove LEAPER's salient merits compared to the existing schemes in face of misbehaving and malfunctioning VANET nodes.

The rest of this paper is organized as follows. In Section 2, the background and related work are introduced. The overview and detailed procedures of LEAPER are presented in Section 3, with the enabling techniques presented in Section 4. In Section 5, the security strength and performance of LEAPER are analyzed and evaluated. Section 6 concludes this paper with brief discussions of the future work.

## 2. Background and related work

### 2.1. Background

Here the problem of ensuring reliable and faithful packet relaying is considered in the multi-hop communication scenarios where simplistic flooding [4] is not feasible due to the overhead involved. In this scenario, if any hop needs to determine whether the received data packet is authentic or not, it has to depend on the information from its previous hop. Such a scenario is common in either urban areas or highways, so in this paper the traffic models are not differentiated for specific VANET scenarios. Indeed, as we will show later, the procedures of LEAPER in each hop will end within 100 ms so that the network topology can be considered as fixed during the concerned period. Thus, the merges and departures in the urban traffic model have no direct impact on the procedures of LEAPER and do not need to be considered.

For brevity, following the conventions of [5,6], in each hop the relaying node is called a *Relayer*. Due to the properties of wireless communications, the nodes within the communication range of the Relayer in each hop can overhear the data packet sent by this Relayer. Thus, as shown in Fig. 1, the nodes within the communication ranges of both Relayers in hop $i$ and hop $(i+1)$ can verify whether the data packet sent by hop $(i+1)$ is the same as that sent by hop $i$, functioning as *watchdogs* for hop $(i+1)$. These watchdogs can in turn inform the next hop of hop $(i+1)$, namely hop $(i+2)$, of their opinion about the data packet, so that hop $(i+2)$ is able to know whether the data packet it receives from hop $(i+1)$ is authentic or not.

As such, four *basic functions* critical to reliable and faithful data packet relaying can be abstracted in each hop: *data reception*, *data verification*, *data transmission* and *proof presenting*, as shown in Fig. 2. In data reception, the nodes in this hop (say hop $i$) receive or overhear the data packet ($D_{i-1}$) from the previous hop. These nodes need to verify the authenticity of $D_{i-1}$ based on the proof presented by the previous hop with the data verification function. $D_{i-1}$, if regarded as authentic, will be transmitted to hop $(i+1)$ in the form of $D_i$ by the Relayer in hop $i$. Similarly, in proof presenting the nodes in hop $i$ need to present the proof of the authenticity of $D_i$, usually constructed and vouched for by the watchdogs of hop $i$, to hop $(i+1)$. As such, these four basic functions can establish the trust of the data packet's

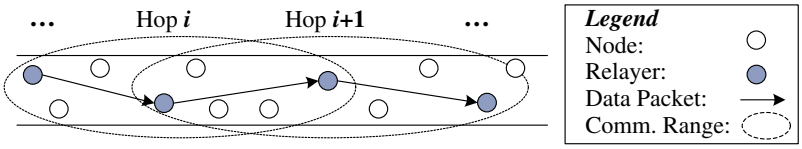


**Fig. 1.** Relayers and watchdogs.

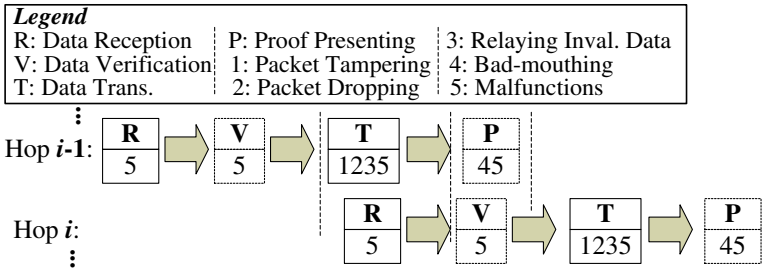


**Fig. 2.** Basic functions, failures and potential attacks in data packet relaying.