Title:

Crypto-Aided MAP Detection and Mitigation of False Data in Wireless Relay Data Collection Networks

Abstract:

Relays are widely used in various types of networks to extend the coverage and increase the

communication reliability. The underlying assumption is that relay nodes will faithfully forward

the received data to the next node. However, a relay node in practice may misbehave by acting uncooperatively: such as refuse signal relaying, garbling the transmitting signal or performing

intended malicious attack. Among all of types of misbehaviors, previous studies has shown that

relay malicious attack can cause significant degradation of communication, this intended malicious

attack are usually known as false data injection or Byzantine attack. By altering the transmitting

bits or injecting false data in transmission packets, relay nodes in the routing path could pretend

to forward the correct message, but in fact, change the information so that he can deceive the

destination to process his intended message, which may result in severe consequence.

In the research of this thesis, we first develop the Bayesian test based on sufficient statistic for

detecting the relay misbehavior at the packet level in lossy one-way wireless relay networks. The

Bayesian test is optimal in the sense of minimizing the probability of detection error. This novel

approach works in the physical-layer and does not require any cryptographic keys, tracing symbols,

or third party authentication. Instead, the overheard packet from the source is exploited, which

is available for free due to the broadcast nature of wireless medium. The enabling factor in our

approach is that the overheard packet, although erroneous due to channel impairments, contains

the true information of source packet, hence can serve as a reference in verifying the correctness

of relayed packet. By deriving the probability of false alarm and missed detection as a function

of the overhearing bit error rate (BER), the number of bits modified in a packet with the packet

length. We found that the probability of false alarm and missed detection decrease as the packet

length increases and converge to zero, regardless of the overhearing BER, if the packet length is

sufficiently long. The Bayesian test accuracy, essentially, depends on bit error rates (BERs) in

overhearing channel, sometimes BERs may not be good enough. To address this issue, a cross-layer

detection mechanism where the cryptographic detection outcomes are used to estimate the false

injection rate is proposed. To reduce the computational cost and bandwidth overhead associated

with the cryptographic detection, only a fraction of packets are attached with keyed hash and the

remaining packets are checked using physical-layer technique. The thesis will show that the detection performance that can be provided with the perfect knowledge of the false injection rate can be

achieved by having only 15% of the packets checked using cryptography and the remaining packets

checked at the physical-layer.

In order to make proposed Bayesian detection scheme adapted to the emerging high-speed wire-

less relay networks, where massive short packets are collected from multiple sources through a relay.

A new detection scheme named as maximum a posteriori probability (MAP) test, is developed for

detecting false data in wireless relay networks composed of multiple sources. The MAP test can

minimize the probability of detection error, meanwhile does not incur any overhead. The fundamental challenge is that the reference information provided by the overheard packet is erroneous

(noisy) due to the channel impairment between the source and the destination. We seek to mitigate

the effects of unreliable reference information on the accuracy of the MAP test by leveraging the

multiplicity of source nodes. It can be shown that the average probability of detection error decreases exponentially as the number of source nodes increases, regardless of the reliability of the reference

information. Hence, a powerful integrity check mechanism can be constructed at the physical layer

if the number of source nodes is large enough. Then, we discuss a packet recovery mechanism

after the MAP test to repair false alarmed packets, i.e. unmodified packets that are mistakenly

declared as modified. The proposed recovery mechanism relies on the likelihood ratio test (LRT)

that conveys the confidence that a particular packet is modified or not. It allows the destination

to determine, with no additional feedback or information from the source nodes, which packets are

likely to be correct and to recover the remaining packets, thereby improving the throughput.

To enhance the performance of MAP test, another cross-layer detection mechanism, named as

crypto-aided MAP test is proposed, in which the MAP test is able to extract prior information of

x

relay attack probability by collecting the detection outcomes of cryptographic hash check results.

The proposed scheme seeks to apply a lightweight hash tag on each packet such that latency and

overhead for integrity check can be made insignificant. Also to overcome the drawbacks caused

by the short hash, the physical layer detection outcomes and cryptographic hash check results are

combined using maximum a posteriori probability (MAP) detection rule to assure low missed detection rate.

Above all, the proposed scheme in this thesis can provide a high accuracy efficient detection

efficiency to guarantee data integrity for those high-density wireless networks while operating under

resource constraints. Also our results show that crypto-aided MAP test has significant improvement

over conventional cryptographic and it doesn’t requires any training set or pre-embedded tracing

bits to help make the decision, like other exist detection method does. In addition, the detection

error of crypto-aided MAP test can be reduced to zero if the number of collected packets is sufficiently large, even if the bit error rate in overhearing channel is very high. This novel technique

will benefit a wide variety of limited resources wireless applications where the traffic type are tend

to be short and massive, meanwhile the information needs to be communicated in trustworthy and

timely manner.