EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A joint design of security and quality-of-service (QoS) provisioning in vehicular ad hoc networks with cooperative communications

Li Zhu[2], F Richard Yu[1*], Bin Ning[2] and Tao Tang[2]

Abstract

In vehicular ad hoc networks (VANETs), some distinct characteristics, such as high node mobility, introduce new non-trivial challenges to quality-of-service (QoS) provisioning. Although some excellent works have been done on QoS issues in VANETs, security issues are largely ignored in these works. However, it is know that security always comes at a price in terms of QoS performance degradation. In this article, we consider security and QoS issues jointly for VANETs with cooperative communications. We take an integrated approach of optimizing both security and QoS parameters, and study the tradeoffs between them in VANETs. Specifically, we use recent advances in cooperative communication to enhance the QoS performance of VANETs. In addition, we present a prevention-based security technique that provides both hop-by-hop and end-to-end authentication and integrity protection. We derive the closed-form effective secure throughput considering both security and QoS provisioning in VANETs with cooperative communications. The system is formulated as a partially observable Markov decision process. Simulation results are presented to show that security schemes have significant impacts on the throughput QoS of VANETs, and our proposed scheme can substantially improve the effective secure throughput of VANETs with cooperative communications.

Keywords: VANETs, Cooperative communications, Quality-of-service, Security

1 Introduction

Recently, there is a strong interest in vehicular ad hoc networks (VANETs), where vehicles can dynamically establish an ad hoc network without necessarily using a fixed infrastructure. VANETs can offer various applications and tremendous benefits to Intelligent Transportation Systems [1]. For example, safety information exchange using VANETs enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging. Value-added services using VANETs can enhance drivers' traveling experience by providing convenient Internet access, navigation, toll payment services, etc. [2].

Certainly, quality-of-service (QoS) issues in traditional mobile ad hoc networks in general are still of interest in VANETs. However, some distinct characteristics of VANETs, such as high node mobility, introduce new non-trivial challenges to QoS provisioning in VANETs [3,4]. Particularly, in vehicle-to-vehicle (V2V) communications, due to high vehicle mobility and relatively low elevation of the antennas on the communicating vehicles, other vehicles will act as obstacles to the signal, often affecting propagation even more than static obstacles (e.g., buildings or hills), especially in the case of an open road [5]. Indeed, non-line-of-sight safety-critical conditions require careful attention in order to provide safety benefits in VANETs [6].

There are some studies on QoS issues in VANETs. Rawat et al. [7] propose a scheme to adapt transmission power at the physical layer and contention window size at the medium access control (MAC) layer based on the estimated local vehicle density to enhance VANET performance. Rate control, MAC, and routing problems in cooperative VANETs are studied in [8], where a cross-layer solution is developed. In [9], a contextual cooperative congestion control policy is proposed to exploit the traffic

*Correspondence: richard_yu@carleton.ca
[1] State Key Lab. of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
Full list of author information is available at the end of the article

context information of each vehicle to reduce the channel load, while satisfying the vehicular applications requirements. Cross-layer routing is studied in [10] by applying cooperative transmission and a new strategy of path selection to achieve a better tradeoff between the transmission power consumption and end-to-end reliability.

While some excellent studies have been done on QoS issues in VANETs, *security* issues are largely ignored in these works. This is not surprising, as these two important areas have traditionally been addressed separately in the literature. However, security is one of the main challenges for VANETs [11], and it is known that security always comes with a price in terms of QoS performance degradation, since securing communications against the adversary typically consumes network resources in terms of bandwidth and/or hardware capacities [12]. This price may be tolerable in wireline networks, but it may dominate the consumption of scarce network resources in VANETs. This situation makes the study of tradeoffs between QoS and security in VANETs an important open challenge [13].

In this article, we consider security and QoS issues jointly for VANETs with cooperative communications. We take an integrated approach of optimizing both security and QoS parameters, and study the tradeoffs between them in VANETs. To the best of the authors' knowledge, combining security and QoS issues for VANETs with cooperative communications has not been considered in existing works. Some distinct features of this study are as follows.

- We use recent advances in cooperative communication to enhance the QoS performance of VANETs. Cooperative communication in wireless networks takes advantage of the broadcast nature of the wireless medium to have nodes adjacent to the source transmit the message to the destination. As a result, nodes in the network act not only as end users but also as relays for others to create a spatial diversity that allows for increased throughput and reliability [14,15]. Cooperative communication has been considered as a promising technique, and has been involved in the standards of WiMAX [16] and 3GPP-LTE [17].
- Prevention-based techniques, such as authentication, are crucial as the front line of defence for the integrity, confidentiality, and non-repudiation of communications [18]. In this article, we propose a prevention-based security scheme for VANETs with cooperative communications. Specifically, we make use of an authentication protocol referred as adaptive and lightweight protocol for both hop-by-hop and end-to-end authentications (ALPHA) [19], which is based on hash chains and Merkle trees (MT), i.e., a tree of hashes [20].
- Based on the proposed prevention-based security scheme for VANETs with cooperative communications, we study the relay selection problem in VANETs. In previous works on relay selection (e.g., [14]), it is generally assumed that the channel conditions are perfectly known and remain in the same state from the current frame to the next. However, these assumptions may not be realistic in VANETs due to high node mobility. Therefore, in this article, we consider channel estimation errors and Markov channel models to improve the performance in VANETs.
- We formulate the system as a partially observable Markov decision process (POMDP) [21], which has successfully been used to solve the security scheduling problem [18] among others. The obtained policy for security and QoS parameters has an indexability property that dramatically reduces the computation and implementation complexity. Effective secure throughput is considered as the optimization objective in our formulation.
- Simulation results are presented to show that security schemes have significant impacts on the throughput QoS of VANETs, and our proposed scheme can substantially improve the effective secure throughput of VANETs with cooperative communications.

The remainder of the article is structured as follows. Section 2 presents the system model. We derive the secure throughput in Section 3. Stochastic formulation of the joint design of security and QoS provisioning is presented in Section 4. Simulation results are presented and discussed in Section 5. Finally, we conclude this study in Section 6 with future work.

2 System model

In this section, we first describe a simple vehicle ad hoc network model. Then, the Markov channel model is introduced next. Finally, we describe the authentication model.

2.1 Network model

We consider a simple VANET with cooperative communications, where each vehicle has the ability to relay data packets to each other. When viewed from the multihop routing diversity point of view, the first hop is more important than all subsequent hop(s) [22]. Therefore, in this study, we only consider two-hop relays, comprising of a source (S), destination (D), and K relay nodes, $R_1, R_2, \ldots, R_k, \ldots, R_K$, as shown in Figure 1. The source node can send information to the destination directly or through a relay. As the relay cannot transmit and receive simultaneously, on account of the half-duplex constraint, the transmission time is divided into two time slots with transmission by the source in the first time slot,

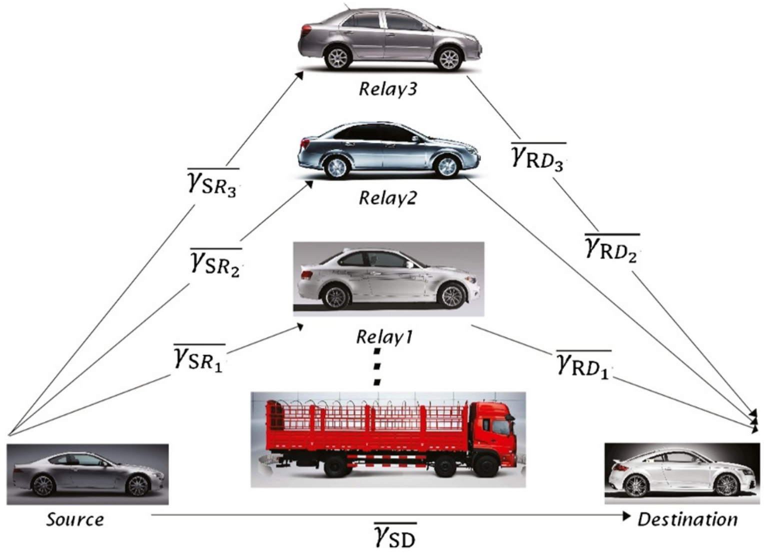

Relay3
Relay2
Relay1
Source
Destination
$\overline{\gamma_{SR_3}}$
$\overline{\gamma_{SR_2}}$
$\overline{\gamma_{SR_1}}$
$\overline{\gamma_{RD_3}}$
$\overline{\gamma_{RD_2}}$
$\overline{\gamma_{RD_1}}$
$\overline{\gamma_{SD}}$

Figure 1 A simple vehicle ad hoc network with cooperative communications.

transmission by the relay in the second time slot, and the destination finally combining the two received signals.

In our network model, all vehicles are considered to be transmitting with the same average transmit signal power. We denote the average transmitted signal-to-noise ratio (SNR) between any nodes as γ, which is given by

$$\gamma = \frac{P_w}{N_0 W}, \tag{1}$$

where P_w is the average transmit signal power, W is the transmission bandwidth, and N_0 is the noise.

We denote the channel gain between two nodes, x and y, as h_{xy}. Therefore, the channel gain between the source vehicle and the destination vehicle is denoted as h_{SD}. The channel gain between the source vehicle and a relay vehicle R_k is denoted as h_{SR_k}, and the channel gain between a relay vehicle and the destination vehicle is denoted as h_{R_kD}. We further denote the average received SNR between the source vehicle and the destination vehicle as γ_{SD}, the average received SNR between the source and the relay as γ_{SR_k}, and the average received SNR between the relay vehicle and the destination vehicle as γ_{R_kD}. Accordingly, we can get $\gamma_{SD} = \frac{\gamma}{h_{SD}}$, $\gamma_{SR_k} = \frac{\gamma}{h_{SR_k}}$, and $\gamma_{R_kD} = \frac{\gamma}{h_{R_kD}}$.

In this article, since our main focus is on the joint design of security and QoS issues, we assume that the problem of fighting for channel access among multiple nodes is handled by MAC layer, which will be responsible for resource sharing and contention resolution among multiple nodes. There are many articles studying MAC issues in cooperative communications in the literature (e.g., [4,23]). The proposed design in this article can be used with these MAC schemes.

2.2 Channel model

In this article, we use finite-sate Markov channel (FSMC) models. FSMC models have widely been accepted in the literature as an effective approach to characterize the correlation structure of wireless channels. These include the following channels: satellite channels [24], indoor channels [25], Rayleigh fading channels [26], Ricean fading channels [27], and Nakagami fading channels [28]. Considering FSMC models can enable substantial performance improvement over the schemes with memoryless channel models [29,30].

In the FSMC, the range of the channel gain is partitioned (quantized) into L levels, and each level is associated with a state of a Markov chain. The channel varies over these states at each time slot according to a set of Markov transition probabilities. In VANETs, the different channel gains between source and relay (S2R) h_{SR_k}, relay and destination (R2D) h_{R_kD}, as well as source and destination (S2D) h_{SD} can be modeled as a random variable according to an FSMC, which is characterized by a set of states $\Gamma = \gamma_0, \gamma_1, \ldots, \gamma_{L-1}$. Due to high node mobility and channel estimation errors, the channel states may not be perfectly known.

Let $\psi_k(i,j))$ denote the probability that h_{SR_k} moves from state i to state j, where $i,j \in \{\gamma_0, \gamma_1, \ldots, \gamma_{L-1}\}$. The $L \times L$ channel state transition probability matrix of relay k for source to relay channel is defined as

$$\Phi_k = [\,\phi_k(i,j)]_{L \times L}\,. \tag{2}$$

Similarly, we can get the channel state transition probability matrix of relay k for relay to destination channel as

$\Psi_k = [\,\psi_k(i,j)]_{L\times L}$, and the channel state transition probability matrix for source to destination channel as $\Xi_k = [\,\xi_k(i,j)]_{L\times L}$.

2.3 Authentication model

There are several ways to perform authentication in communication networks. Traditional public key infrastructure (PKI) approaches are gaining popularity in wireless networks. PKI scheme uses a public key validated by a trusted third party to encrypt a message that can only be decrypted by the corresponding private key. In general, PKI-based authentication mechanisms are relatively expensive in terms of generating and verifying digital signatures. Symmetric cryptography, where the communicating nodes share a secret, is more efficient due to its reduced computational complexity. However, when used in cooperative communication networks, distributing the shared keys in the first place becomes a problem.

Hash chains are a simple and computationally efficient means of authenticating nodes in a network when tied to identities. A hash chain is generated by hashing a random seed variable ϑ using any cryptographic hash function. The resulting value serves as the input for the next hashing, and continues on until the desired length i is reached. A hash chain of length i is generated as

$$\begin{aligned}[\vartheta, Ha(\vartheta) = ha_1, Ha(ha_1) = Ha(Ha(\vartheta)) = ha_2, Ha(ha_2)\\ = Ha(Ha(Ha(\vartheta))) = ha_3, \ldots, ha_{i-1}, ha_i]\,,\end{aligned} \tag{3}$$

where ha_i is the *anchor* of the hash chain corresponding to the last hashed value for that hash chain.

Although hash chains are uncomplicated to calculate and easy to use, they are not sufficient to prevent insider attacks by relay nodes. However, the ALPHA can prevent insider attacks through integrity protection and also perform authentication making use of MT and interaction-based hash chains, which is based on delayed message disclosure [19]. When hash chains are combined in an MT in ALPHA [19], they allow for the authentication of identities while the MT provides integrity protection for individual messages, which is especially useful for on-path verification with the high-volume data in cooperative communication networks. We now begin to describe how the ALPHA-MT scheme works in VANETs with cooperative communications.

An MT is a binary tree of hashes with the leaves as hashes of data blocks and nodes as the hashes of the concatenation of their respective children. In addition to the root of the MT and the data block m_j, a verifier requires a set of complementary branches $\{B_c\}$, which increases logarithmical as the number of data blocks signed, to authenticate each data block independently. As shown in Figure 2, the source and destination maintain their own separate hash chains and initially exchange their respective hash chain anchors (h_{Si} and h_{Di}, respectively) through an initial handshaking process. In the case of communication passing through a relay, the anchor information is also passed on to the relay. There are four packet types exchanged between the source and the destination, with the source transmitting S_1 packet containing the pre-signature and S_2 packets containing the actual messages, and the destination transmitting A_1 packet containing the pre-signature and A_2 packets containing the acknowledgments. The source constructs the MT with hashes of data blocks, m_j, and sends the pre-signature, which is obtained by hashing the root with the next element of the hash chain (i.e., key of the pre-signature), in an initial S_1 packet along with a fresh element of the hash chain. The destination builds an acknowledgment MT and sends the acknowledgment A_1 packet with its own pre-signature. The actual message transfer process is then initiated with the source sending S_2 packets corresponding to the number of messages/data blocks in the MT along with the respective set $\{B_c\}$ and key of the pre-signature. Following receipt of this information, the destination can rebuild the MT corresponding to the message block and verify the integrity of the pre-signature, from which we can conclude that the message block has not been tampered with. As a consequence, the destination sends a positive or negative acknowledgment (ack/nack) through the A_2 packets. The authenticity of the source or the destination can be confirmed by the recipient nodes by hashing the key of the pre-signature received in the S_2 or A_2 packets to arrive at the respective hash chain anchor values.

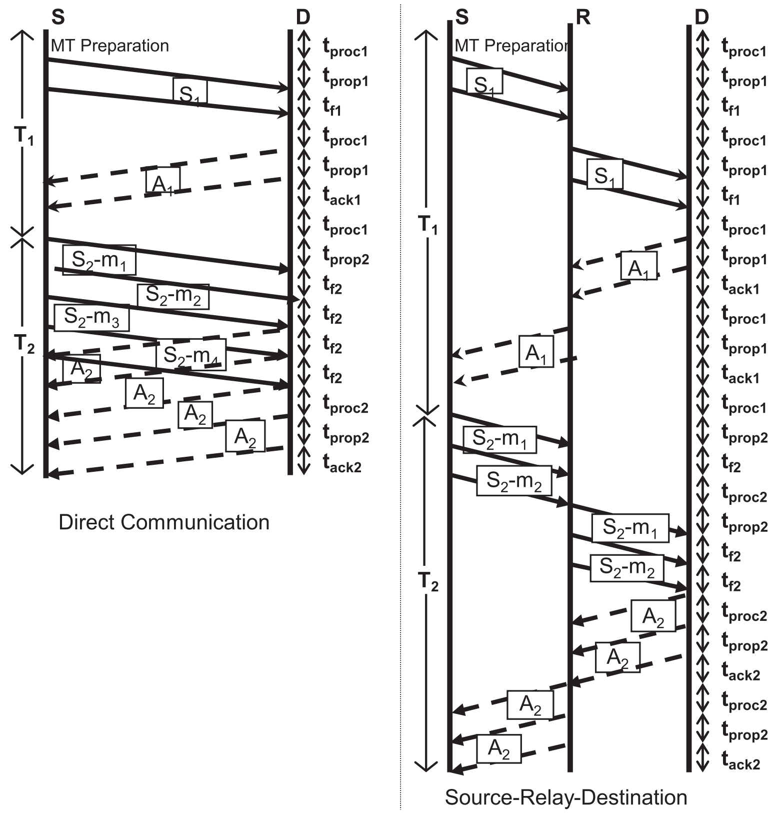
3 Secure throughput in VANETs with cooperative communications

As we mentioned in Section 1, security always comes with a price in terms of QoS performance degradation. Throughput is one of the main QoS measures in VANETs. In this section, we derive the effective secure throughput in VANETs with cooperative communications, which will be used as the objective function in our optimization formulation in Section 4. We first derive the outage capacity. Then, bit error rate is derived. Finally, we obtain effective secure throughput considering both the authentication protocol and cooperative communications.

3.1 Outage capacity

The mutual information equations for non-cooperative and cooperative diversity schemes can be described as follows. In the non-cooperative mode, the source node transmits the signal directly to the destination node. The mutual information between the source and the destination in the non-cooperative mode is simply

$$I_{\text{non-coop}} = \log_2\left(1 + \mid h_{SD}\mid^2 \gamma\right), \tag{4}$$



Direct Communication

Source-Relay-Destination

Figure 2 Message sequence charts in VANETs.

where $|\ h_{SD}\ |$ is the channel between the source and the destination. To be sustainable, the data rate over this channel r should be less than the mutual information $I_{\text{non-coop}}$.

In the cooperative decode-and-forward (DF) relaying mode, the transmission between the source and the destination makes use of the intermediate relay node. As stated, the relays operate in half duplex and cannot receive and transmit simultaneously. The relay that maximizes the mutual information between the source and destination is selected as the best relay. As indicated earlier, the transmission is divided into two time slots. In the first time slot, the source transmits the signal to both the selected relay and the destination. In the second time slot, the selected relay decodes the received signal, re-encodes it, and forwards it to the destination node. The destination combines the received signal from the relay and source nodes using maximal ratio combining (MRC).

The mutual information between the source and each of the kth relay nodes is given by

$$I_{SR_k} = \frac{1}{2}\log_2\left(1+\mid h_{SR_k}\mid^2\gamma\right). \tag{5}$$

Given the half-duplex constraint, the factor $\frac{1}{2}$ reflects the two time slots for relaying.

The mutual information between source–destination and destination- each of the kth relay nodes is given by

$$I_{\mathrm{MRC}} = \frac{1}{2}\log_2\left(1+\left(\mid h_{SR_k}\mid^2+\mid h_{SR_k}\mid^2\right)\gamma\right). \tag{6}$$

Thus, the maximum end-to-end mutual information in the cooperative DF mode is given by

$$I_{\text{coop}} = \max_{k\in K}\min\{I_{SR_k}, I_{\mathrm{MRC}}\}. \tag{7}$$

In the DF opportunistic relay, the relay is selected from the entire set of available relays. The relay transmits only if both source–relay and relay–destination mutual information are above the required rate r. Thus, the source selects the relay that maximizes the minimum mutual information between the source–relay and the relay–destination channels.

We consider a smart cooperative (SC) system that uses cooperation only if it is beneficial in terms of mutual information. In this scheme, the source uses the relay only if it increases the achievable rate. We define the deciding criteria of the SC relaying system as the maximum end-to-end mutual information between the cooperative and non-cooperative mutual information, and is expressed as

$$I_{\mathrm{SC}} = \max\{I_{\text{coop}}, I_{\text{non-coop}}\}. \tag{8}$$

When the mutual information between the source, relay, and the destination fall below the data rate (r), it indicates an unsuccessful data transmission causing an outage. Therefore, outage probability (P_{out}) is defined as the probability that the mutual information (I) between the source and the destination, including relay falls below the required rate r, i.e.,

$$P_{\text{out}} = P[\,I < r\,]\,. \tag{9}$$

This indicates that the channel cannot support the transmission rate and consequently the data transmission is unsuccessful. It is an important analytical metric that characterizes the probability of data loss providing a bound on the symbol error rate or equivalently of deep fading.

In the case of the SC relaying system, the outage probability is expressed as

$$P_{\text{out}}^{\text{SC},k} = P[\,I_{\text{SC}} < r\,]\,, \tag{10}$$

i.e.,

$$P_{\text{out}}^{\text{SC},k} = P\left\{\max\left\{I_{SD}, \max_{k\in K}\min\{I_{SR_k}, I_{\text{MRC}}\} < r\right\}\right\}, \tag{11}$$

from which we arrive at [13],

$$P_{\text{out}}^{\text{SC},k} = 1 - \upsilon + \left(\frac{\omega^{\left(h_{SR_k}+h_{R_kD}\right)}\left(\upsilon^{\left(1-h_{R_kD}\right)}-1\right)}{1-h_{R_kD}}\right), \tag{12}$$

where υ and ω are given by

$$\upsilon = \exp\left(-\left(\frac{2^r-1}{\gamma}\right)\right), \tag{13}$$

$$\omega = \exp\left(2\ln\upsilon - (\ln\upsilon)^2\gamma\right). \tag{14}$$

We consider the outage capacity $C_{\varepsilon}^{SC,k}$ as the largest rate of transmission (r) that can be supported if the outages are allowed to occur at a certain outage probability ε, which corresponds to the probability that the transmission cannot be decoded with negligible error probability. Solving $P_{\text{out}}^{\text{SC},k} = \varepsilon$, yields υ_ε. Then, we obtain the outage capacity as

$$C_{\epsilon}^{\text{SC},k} = r = \log_2\left(1+\gamma\ln\left(\frac{1}{\upsilon_\varepsilon,\gamma}\right)\right). \tag{15}$$

3.2 Bit error rate

According to [31], the end-to-end BER of SC transmission, $P_e^{\text{SC},k}$, is given by

$$P_e^{\text{SC},k} = P_{\text{out}}^{SR_k}\cdot P_e^{SD} + \left(1-P_{\text{out}}^{SR_k}\right)\cdot P_e^{div,k}, \tag{16}$$

where $P_{\text{out}}^{SR_k}$ is the outage probability of the link from source to relay.

If an outage occurs between source and relay, the relay will not decode, and falls back to direct transmission, i.e.,

$$P_{\text{out}}^{SR_k} = 1 - \exp\left(-\left(\frac{2^{2r}-1}{\overline{\gamma_{SR_k}}}\right)\right). \tag{17}$$

P_e^{SD} is the probability of error in direct transmission from source to destination over the Rayleigh channel, i.e.,

$$P_e^{SD} = \frac{1}{2}\left(1-\sqrt{\frac{\overline{\gamma}_{SD}}{1+\overline{\gamma_{SD}}}}\right), \tag{18}$$

and $P_e^{\text{div},k}$ is the probability that an error occurs in combined transmission from source and relay nodes at the destination. This occurs if the relay has decided to DF the signal to the destination. To prevent error propagation, we assume that the relay decodes if it has correctly received the signal from the source. When Rayleigh channel is approximately assumed, it can be expressed as

$$P_e^{\text{div},k} = \frac{1}{2}\left[1+\frac{1}{\overline{\gamma_{R_kD}}-\overline{\gamma_{SD}}}\left(\frac{\overline{\gamma_{SD}}}{\sqrt{1+\frac{1}{\overline{\gamma_{SD}}}}}-\frac{\overline{\gamma_{R_kD}}}{\sqrt{1+\frac{1}{\overline{\gamma_{R_kD}}}}}\right)\right]. \tag{19}$$

3.3 Secure throughput

In this section, we discuss the throughput performance of the authentication protocol by considering the outage capacity and BER of the direct communication (DC, communication without the use of relay) and source–relay–destination communication paths. The error rate is also taken into consideration by applying ARQ retransmission schemes, which involves error detection and retransmission of lost or corrupted packets.

The payload for ALPHA-MT scheme is given as

$$S_{\text{payload}} = n\cdot(S_{\text{packet}} - S_h(\lceil\log_2(n)\rceil + 1)), \tag{20}$$

where S_{payload} is the amount of payload that can be transmitted with a single pre-signature, n is the number of messages/data blocks in the MT, S_{packet} is the size of the packet, and S_h is the hash output.

In general, throughput is defined as the payload size divided by the total time taken to process the payload. In our case, while the payload is evident from the above, the time element is dependent upon time taken for the exchange of S_1 and A_1 packets, as well as S_2 and A_2 packets. We denotes them as T_1 and T_2, respectively. Accordingly,

$$Thr_{\text{general}} = \frac{S_{\text{payload}}}{T_1+T_2}, \tag{21}$$

where T_1 is the time for the initial pre-signature process between the source and the destination. It works like a basic Stop-and-Wait ARQ model (*explained below*) with transmission of S_1 packet by the source, processing at the destination, transmission of acknowledgment A_1 packet by the destination and processing at the source. The message delivery is complete only after the source receives the confirmatory acknowledgment from the destination; T_2 is the time taken for the actual message transmission and delivery, i.e., the actual transfer of messages from the source through the S_2 packets and the transfer of acknowledgments from the destination through A_2 packets.

Both T_1 and T_2 are dependent on the data transmission rate, which is equal to the outrage capacity described in Section 3.1.

Equation (21) shows the generic throughput for the authentication protocol. To improve system reliability, an ARQ scheme is needed. As selective-repeat SR-ARQ has been proven to outperform other forms of basic ARQ schemes (stop-and-wait ARQ, go-back-N ARQ) [32], we use SR-ARQ in this study.

Detailed studies of ARQ schemes are beyond the scope of this article. The throughput of ARQ scheme is defined as average rate of successfully message delivery over a communication channel. We have already explained $P_e^{\mathrm{SC},k}$ in (16) as the end-to-end BER, i.e., the probability that any given bit of received data is in error. We define P_c as the probability that the received packet comprising of S_{packet} bits contains no error [32], which is given by

$$P_c = \left(1 - P_e^{\mathrm{SC},k}\right)^{S_{\mathrm{packet}}}. \tag{22}$$

The throughput equation for the authentication process needs to be modified if selective repeat SR-ARQ is used, as only the error frames are retransmitted. The modified throughput for the authentication process with SR-ARQ is

$$Thr_{\mathrm{SR}} = \frac{S_{\mathrm{payload}}}{(T_1 + T_2)} \left(P_c\right). \tag{23}$$

For each packet size S_{packet}, the optimal value of the number of messages (n) in the MT, which corresponds to the number of S_2 packets, is the value that results in the highest throughput, which is denoted by n^*. There is a trade-off as the throughput increases initially with the number of messages in the MT but then starts to decrease as a consequence of the larger signature size overheads from the increased number of messages in the MT. Therefore, one of the objectives in our research is to find the optimal number of messages in the MT for relay R_k.

4 Stochastic formulation of the joint design of security and QoS provisioning

In this section, we formulate the effective secure throughput optimization problem in the system described above as a POMDP [21], which can determine the optimal policy for the number of messages/data blocks in the MT selection (for security) and relay selection (for QoS) to maximize the system effective secure throughput.

Markov decision process (MDP) provides a mathematical framework for modeling decision making in situations where outcomes are partly random and partly under the control of a decision maker. In VANETs with cooperative communications, the vehicles make decisions at specific time instances according to the current state $s(t)$, and the system moves into a new state based on the current state $s(t)$ as well as the chosen decision $a(t)$.

As described in Section 2, we use FSMC. Given the current channel state $s(t)$, the next channel state is conditionally independent of all previous states and actions. This Markov property of state transition process makes it possible to model the optimization problem as an MDP. Furthermore, in VANETs, due to channel sensing and channel state information errors, the system state cannot directly be observed. As a result, we formulate the optimization problem as a POMDP, in which it is assumed that the system dynamics are determined by an MDP, but the underlying state can only be observed inaccurately, or with some probabilities.

A POMDP can be defined by a hex-tuple $< S, A, P, \Theta, B, R >$, where S stands for a finite set of states with state i denoted by s_i, A stands for a finite set of actions with action i denoted by a_i, P stands for transition probabilities for each action in each state, and p_{ij}^a denotes the probability that system moves from state s_i to state s_j when action a is performed, Θ stands for a finite set of observations, and θ_i denotes the observation of state i, B is the observation model, and $b_{j\theta}^a$ denotes the probability that θ was observed when the system state is s_j and last action taken is a, and R stands for the immediate reward. r_{ij}^a denotes the immediate reward received for performing action a and the system state moves from s_i to state s_j, with an observation θ.

In our POMDP model, the vehicle node has to make a decision whenever a slot has elapsed. These instant times are called *decision epochs*. The optimal optimization policy can be obtained from value iteration algorithms in this formulation. Using the POMDP-derived policy, a channel state is observed according to the information from last slot. Based on the observation, the system jointly considers the number of messages/data blocks selection and relay selection to maximize the system throughput.

In order to obtain the optimal solution, it is necessary to identify the states, actions, state transition probability, observation model, and reward functions in our POMDP model, which is described in the following sections.

4.1 Actions, states, and observations

In VANETs with cooperative communications, the vehicle nodes need to decide the number of messages/data blocks in the MT and which relay to use at every decision epoch. Therefore, the current composite action $a(t) \in A$ is denoted as,

$$a(t) = \{a_n(t), a_R(t)\}, \tag{24}$$

where $a_n(t)$ is the action to decide the number of messages/data blocks in the MT, and $a_n(t) > 0$. $a_R(t)$ is the relay selection action, and $a_R(t) \in \{1, 2, \ldots, K\}$, where K is the number of relays.

The current composite state $s(t) \in S$ is given as

$$s(t) = \left\{h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t)\right\}, k \in \{1, 2, \ldots, K\}, \tag{25}$$

where h_{SR_k} is the channel gain between source and relay R_k, h_{R_kD} is the channel gain between relay R_k and destination, and h_{SD} is the channel gain between source and destination.

The composite observation $\theta(t) \in \Theta$ is defined as

$$\theta(t) = \left\{\widehat{h_{SR_k}}(t), \widehat{h_{R_kD}}(t), \widehat{h_{SD}}(t)\right\}, \tag{26}$$

where $\widehat{h_{SR_k}}(t)$, $\widehat{h_{R_kD}}(t)$, and $\widehat{h_{SD}}(t)$ are the observation of h_{SR_k}, h_{R_kD}, and h_{SD}, respectively, and they have the same space as the state space.

4.2 State transition model and observation model

Given the current state

$$s(t) = \left\{h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t)\right\}, k \in \{1, 2, \ldots, K\}, \tag{27}$$

the current observation $\theta(t) = \{\widehat{h_{SR_k}}(t), \widehat{h_{R_kD}}(t), \widehat{h_{SD}}(t)\}$, and the chosen action $a(t)$, the probability function of the next state $s(t+1) = \{h_{SR_k}(t+1), h_{R_kD}(t+1), h_{SD}(t+1)\}, k \in \{1, 2, \ldots, K\}$ is given by

$$\begin{aligned} &P(s(t+1)|s(t), (\theta(t), a(t))) \\ &\quad = \prod_{k=1}^{K} \phi\left(h_{SR_k}(t), h_{SR_k}(t+1)\right) \psi \\ &\quad \times \left(h_{R_kD}(t), h_{R_kD}(t+1)\right) \xi(h_{SD}(t), h_{SD}(t+1)), \end{aligned} \tag{28}$$

where $\phi(h_{SR_k}(t), h_{SR_k}(t+1))$, $\psi(h_{R_kD}(t), h_{R_kD}(t+1))$, $\xi(h_{SD}(t), h_{SD}(t+1))$ are the channel state transition probabilities for difference channels as described in Section 2.2.

Given the channel estimation errors, the vehicle nodes are not able to have full knowledge of the channel information. Following the work in [33], we assume that the channel estimation error has a Gaussian distribution with zero mean and δ^2 variance. At a particular time epoch, the observed channel gain is

$$\widehat{\varrho} = \varrho_m + \omega, \tag{29}$$

where $\widehat{\varrho}$ is the actual channel gain, and ω is a Gaussian random variable with zero mean and δ^2 variance. The receiver then quantizes the channel gain to the nearest possible value. The probability that $\hat{\varrho}$ is closest to ϱ_n is given by $B_{ch}(m, n) =$

$$\begin{cases} \frac{1}{2}\left[erf\left(\frac{\varrho_n + \varrho_{n+1} - 2\varrho_m}{2\sqrt{2}\delta}\right)\right. \\ \quad \left. -erf\left(\frac{\varrho_n + \varrho_{n-1} - 2\varrho_m}{2\sqrt{2}\delta}\right)\right], & \text{if } n \neq \varrho_1, \varrho_{L-1}, \varrho_L, \\ \frac{1}{2}\left[1 + erf\left(\frac{\varrho_1 + \varrho_2 - 2\varrho_m}{2\sqrt{2}\delta}\right)\right], & \text{if } n = \varrho_{L-1}, \\ \frac{1}{2}\left[1 - erf\left(\frac{\varrho_{L-2} + \varrho_{L-1} - 2\varrho_m}{2\sqrt{2}\delta}\right)\right], & \text{if } n = \varrho_1, \\ 0, & \text{if } n = \varrho_L. \end{cases} \tag{30}$$

In our observation model, channel observation is independent on the composite action $a(t)$, so we can get the observation matrix under action $a(t)$ as

$$\begin{aligned} B^{a(t)} = &B_{SR_1} \otimes B_{SR_2} \ldots \otimes B_{SR_K} \otimes B_{R_1D} \otimes B_{R_2D} \ldots \\ &\otimes B_{R_KD} \otimes B_{SD}, \end{aligned} \tag{31}$$

where B_{SR_k}, B_{R_kD}, and B_{SD} are channel observation probability matrices for S2R channel, R2D channel, and S2D channel, respectively. $\otimes$ denotes Kronecker product which is used here to expand the transition matrices. Note that all the channel observation probability is independent. That is why we can use $\otimes$ to expand it.

4.3 Information state

Information state is an important concept in POMDP. We refer to a probability distribution over states as the information state and the entire probability space (the set of all possible probability distributions) as the information space. Let $\pi^{t+1} = \left\{\pi_0^t, \pi_1^t \ldots, \pi_S^t\right\}$ denote the information space, where π_i^t represents the probability that the current state is i at time t. As will be shown later, the knowledge of the system dynamics and the transition probabilities must be known in order to maintain an information state.

One important property of the information state is that it can be easily updated with Bayes Rule by incorporating one additional observation into the history,

$$\pi_j^t = \frac{\sum_i \pi_i^t p_{ij}^a b_{j\theta}^a}{\sum_{i,j} \pi_i^t p_{ij}^a b_{j\theta}^a}, \tag{32}$$

where p_{ij}^a is the probability when the system state changes from i to j when action a is adopted. $b_{j\theta}^a$ stands for the observation probability that we observe the system state j to θ when action a is adopted. Both p_{ij}^a and $b_{j\theta}^a$ are described in Section 4.2.

The new information state will be a vector of probabilities computed according to the above formula. The information states capture all the history information at time t. Therefore, we can save all the past actions and observations by constantly updating the information state. Also, it is reasonable to make decisions according to the information state.

4.4 Reward function and objective

Our optimization objective is to maximize the network throughput in VANETs. Therefore, a natural definition of the reward is the throughput that can be obtained at each decision epoch. Given the current state $s(t) = \{h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t)\}$, and action $a(t) = \{a_n(t), a_R(t)\}$, the immediate reward can be defined as

$$R(s(t), a(t)) = Thr_{SR}(h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t), a_n(t), a_R(t)), \tag{33}$$

where Thr_{SR} is the throughput for the authentication process with SR-ARQ, and it is derived in Section 3.3.

Although we use effective secure throughput as the optimization objective in our formulation, other QoS parameter can be used in the reward function as well. For example, when we obtain communication delay $De_{SR}(h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t), a_n(t), a_R(t))$ between the source and destination node, the reward function can be rewritten as

$$\begin{aligned} &R(s(t),a(t)) \\ &\quad = \beta * Thr_{SR}(h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t), a_n(t), a_R(t)) \\ &\qquad + (1-\beta) * De_{SR}(h_{SR_k}(t), h_{R_kD}(t), h_{SD}(t), a_n(t), a_R(t)), \end{aligned} \tag{34}$$

where β and $(1-\beta)$ are importance weight factors to indicate the importance of throughput and communication delay. In (34), we combine throughput and delay into a single function. This is a common approach used in the optimization literature, which is called Aggregate Objective Function, to solve an optimization problem with multiple objectives [34,35]. In reality, different VANETs have different throughput and packet delay requirements. By adjusting the parameters in (34), the proposed scheme is generic enough to accommodate different requirements in practical VANETs.

The expected total reward of the POMDP depicts the overall reward over Z time epochs and can be expressed as

$$V_\mu = E_{\mu_n,\mu_R}\left[\sum_{t=t_0}^{t_0+Z} R(s(t), a(t))\right], \tag{35}$$

where μ_h specifies the number of messages/data blocks selection policy, μ_R is the relay selection policy, E_{μ_n,μ_R} is the expectation when the policies μ_h and μ_R are employed, and t_0 is the initial time.

We aim to develop a joint design of an optimal policy for throughput improvement in VANETs. $\{\mu_n^*, \mu_R^*\}$ should be a joint policy that maximizes the expected total reward in Z decision epochs, which is

$$\{\mu_n^*, \mu_R^*\} = \arg\max_{\mu_n,\mu_R} E_{\mu_n,\mu_R}\left[\sum_{t=t_0}^{t_0+Z} R(s(t), a(t))\right]. \tag{36}$$

4.5 Separation principle for optimal policy

In this section, we solve the POMDP model to obtain the optimal policy for the number of messages/data blocks selection and relay selection. Specifically, we establish a separation principle that simplifies the calculation process.

In POMDP models, the underlying states cannot be observed directly, the continuous information state, i.e., the likelihood of being in each state is used instead to make decision. Our task is to compute a policy that obtains, based on the information state, the maximum expected reward for a single action. The POMDP policy can be derived from a value function which is defined over the entire information space. Let $V_t(\pi^t)$ be the value function that represents the maximum expected total reward that can be obtained starting from epoch t, given information state π^t at the beginning of epoch t. The value function of POMDP consists of the immediate reward and the maximum expected future reward, which is given as

$$V_t(\pi^t)^* = \max_{a\in A}\left[\sum_{i\in S}\pi_i^t \sum_{j\in S} p_{j\theta}^a \sum_{\theta\in S} b_{j\theta}^a \left(R(i,a) + V_{t+1}^*\left(\pi^{t+1}\right)\right)\right], \tag{37}$$

where π_{t+1} represents the updated knowledge of system state after incorporating the action $a(t)$ and the observation $\theta(t)$ in the epoch t.

Smallwood and Sondik [36] have showed that the value function with finite horizon is *piecewise*, *linear*, and *convex*, which means that the value function can be represented with a set of linear segments, and it can be written simply as

$$V_t(\pi(t))^* = \max_k \sum_i \pi_i \alpha_i^k(t), \tag{38}$$

for some sets of vectors $\alpha_i^k(t) = \left\{\alpha_i^0(t), \alpha_i^1(t), \ldots\right\}$. The sets of α-vectors represents the coefficients of one of the linear pieces of a piecewise linear function. These piecewise linear functions can represent the value functions for each step in the finite horizon POMDP problem. We only need to find the vector that has the highest dot product with the information state to determine which action to take.

One of the main problem in our POMDP model is the action space. As shown in Section 4.1, the number of messages/data blocks selection action space is $\{a_n(t) : a_n(t) > 0\}$. The infiniteness of the action space makes it hard to solve the model with traditional value iteration algorithms. To this point, we establish a separation principle that leads to closed-form optimal design of the number of messages/data blocks selection and relay selection strategy. The policy calculation is carried out in two steps without losing optimality.

Step 1: Calculate the optimal number of messages/data blocks policy μ_n in the MT to maximize the instantaneous throughput subject to the current relay. Specifically, the optimal number of messages n^* in the MT for relay R_k is determined as follows:

$$n^* = \arg\max_n Thr_{SR}(R_k, n). \tag{39}$$

Step 2: Using the optimal number of messages/data blocks policy μ_n given by (39), we calculate the relay selection policy to maximize the expected total throughput with piecewise linear value functions described above. Specifically, the optimal relay selection policy is given by

$$\mu_R^* = \arg\max_{\mu_R} E_{\pi_R}\left[\sum_{t=1}^{T} R(t)|\pi(1)\right]. \tag{40}$$

5 Simulation results and discussions

In order to evaluate the performance of our proposed scheme, we have carried out a set of simulation experiments using NS-2 simulator. We first illustrate our secure throughput model performance. The performance improvement of our POMDP optimization algorithm is given next. We then discuss the effects of the channel state transition matrix and observation model parameters on the optimal policy.

All simulations were run on a computer equipped with Windows 7, Intel Core 2 Duo P8400 CPU (2.26 GHz) and 4 GB memory. We considered a topology set-up with three relays located arbitrarily between the source and the destination. All the initial locations of nodes are random assigned into the VANET. When the simulation begins, nodes start to move along with their trajectory, which are already defined. The vehicles velocity is a random number. After considering the traffic situation in VANET and driver's behavior, we set the range of velocity from 0 to 60 km/h. We assume that the state of the S2R, R2D, and S2D channels can be *bad* (s_0), *modest* (s_1), or *good* (s_2). The corresponding SNRs to these three states for the S2D channel are 15, 20, and 25 dB, and the corresponding SNRs to these three states for the S2R and R2D channels are 12, 16, and 21 dB, respectively. For simplicity, we assume the S2R channel, R2D channel, and S2D channel have the same channel state transition probability matrix. We set the channel transition probability of staying in the same state as 0.6 and set the probability of transition to the adjacent state to be three times that of transition to a nonadjacent state. Therefore, the channel state transition probability matrix is

$$P_t = \begin{pmatrix} 0.6 & 0.2 & 0.2 \\ 0.2 & 0.6 & 0.2 \\ 0 & 0.2 & 0.6 \end{pmatrix}. \tag{41}$$

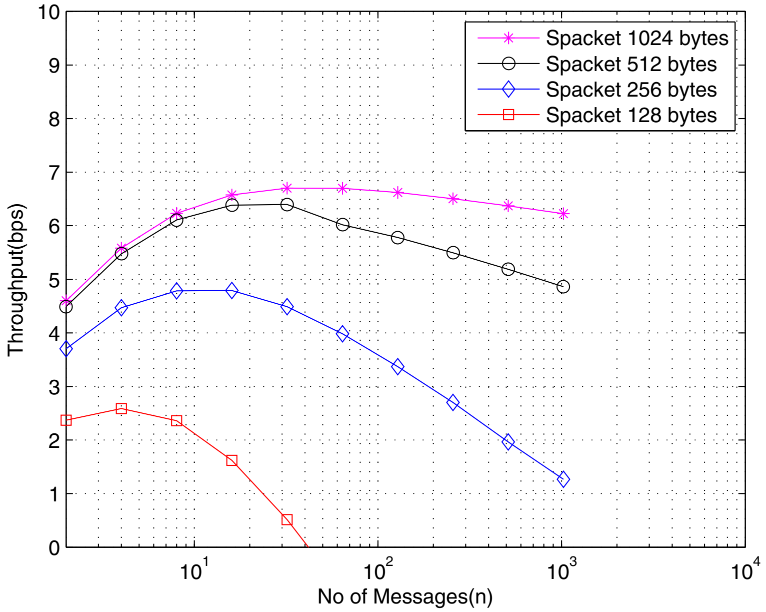


Figure 3 Effects of number of messages (*n*) on system secure throughput.

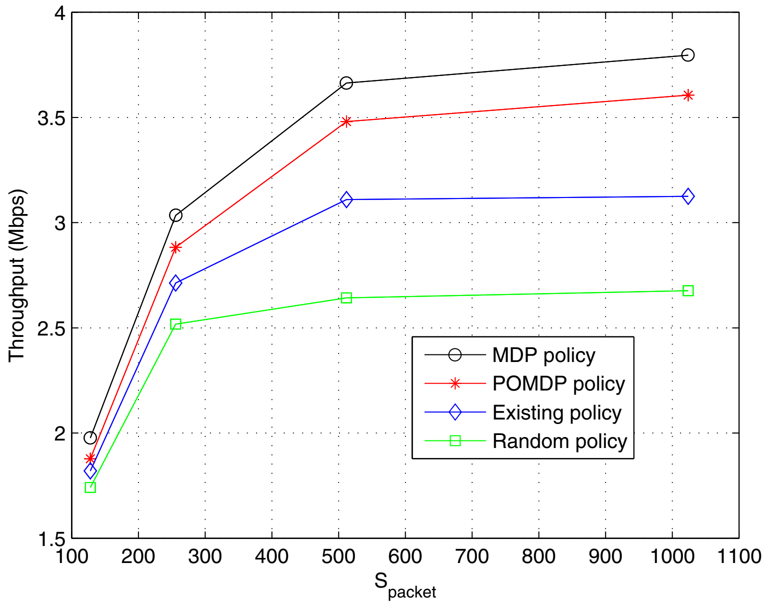


Figure 4 Throughput comparison of different policies under different S_{packet}.

We took the processing time at each node as 10 μs, hash size as 20 bytes, and a fixed outage probability of 0.01. In all figures, the values represent the average results of 20 different runs.

5.1 Throughput improvement

We first carry out a study to verify the secure throughput model when authentication is used in VANETs with cooperative communications. We consider four different packet sizes (S_{packet}) of 128, 256, 512, and 1024 bytes. The number of messages in the MT varies by power of 2 as the MT requires binary representation. Figure 3 shows the throughput versus the number of messages and the optimal n value for each of the four packet sizes. As we can see from this figure, the number of messages in the MT (i.e., the number of S_2 packets) has significant effect on

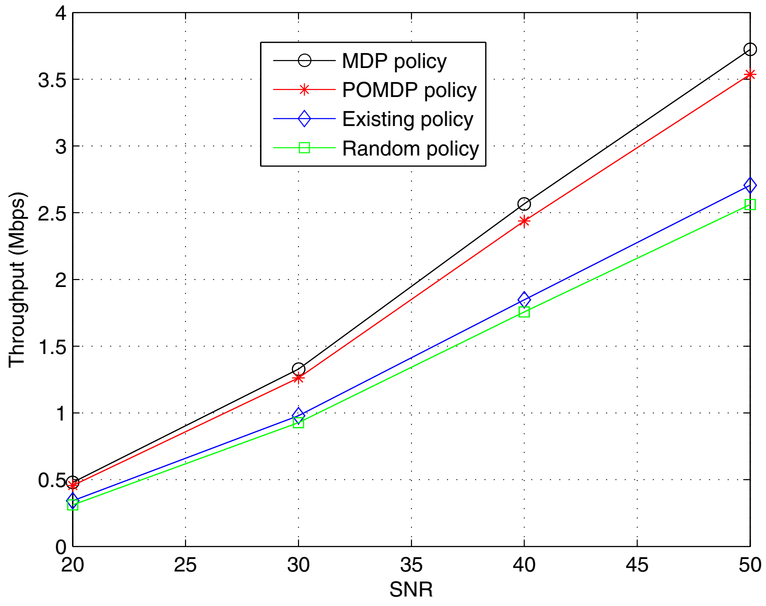


Figure 5 Throughput comparison of different policies under different SNRs.

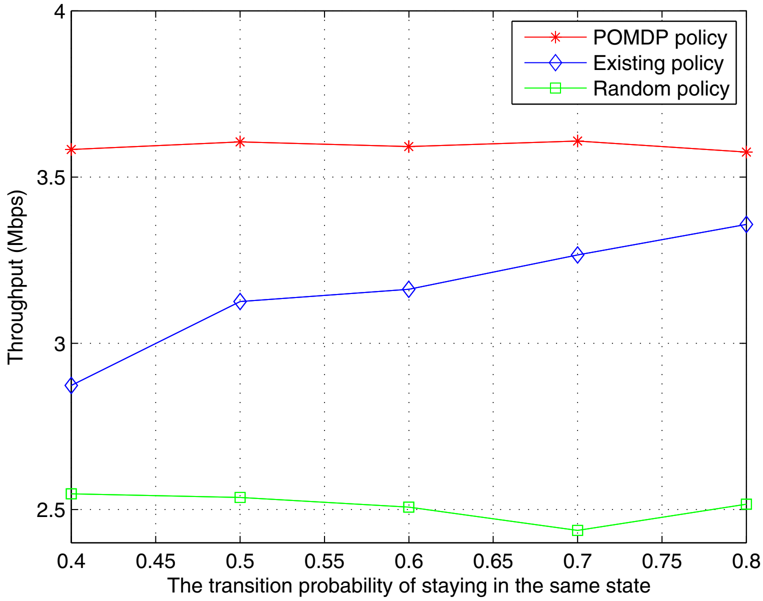


Figure 6 Effects of the channel state transition matrix on throughput.

the system throughput. As indicated in Section 3.3, the throughput starts to increase initially with the increase of the number of messages in the MT, but then decreases on account of large signature size overheads and the payload subsequently drops to zero. Therefore, the number of messages that provides the highest throughput, for a given packet size, is chosen as the optimal *n* value. The optimal number of messages in the MT for packet sizes 128, 256, 512, and 1024 bytes are 4, 8, 16, and 32, respectively.

Next, we start to illustrate the performance improvements of our POMDP policy. We compare the POMDP policy with three other policies. For the first policy, we assume the channel state can be observed accurately. Therefore, the POMDP policy becomes an MDP policy. The second policy is the existing policy, in which the vehicle nodes use the observed inaccurate channel states in the current epoch to make the relay selection decision for the subsequent epoch. The third policy is the random

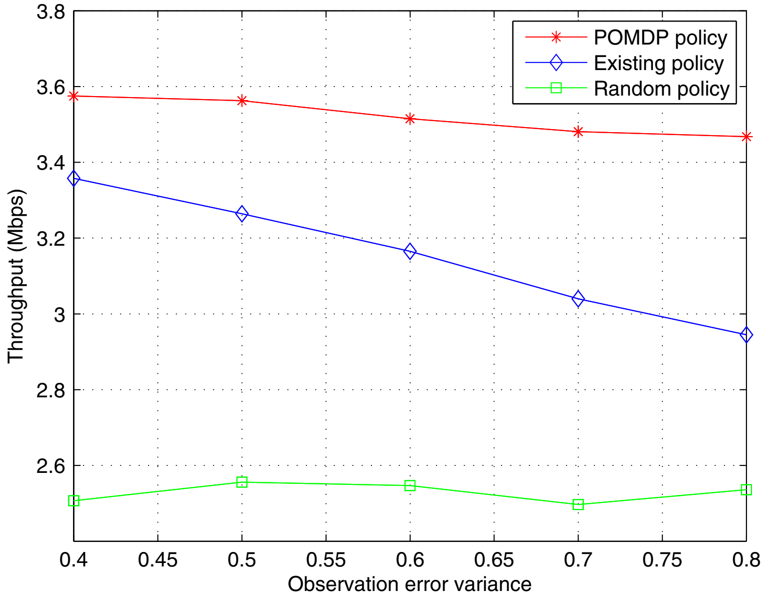


Figure 7 Effects of the channel observation error on throughput.

policy, in which the vehicle nodes randomly choose relays. Figures 4 and 5 show the throughput performance for the four policies given different packet sizes and transmission SNRs. As shown in the figures, the proposed POMDP policy significantly improves the average throughput compared to the existing policy. This is because the existing policy makes relay selection decisions by its current channel information, and it does not consider the dynamic transition of the wireless channel in VANETs, which is very important information to make relay selection decisions. The simulation results also show that our POMDP policy performance is very close to the MDP policy. The channel estimation error cannot be avoided in VANETs, but our POMDP policy can minimize the impact caused by channel estimation error, and achieve a satisfying performance.

5.2 Effects of the state transition matrix

We evaluate how the parameters in the channel state transition matrix affect the average reward. Given the channel state transition matrix P_t, Figure 6 shows the simulation results for the effect of the transition probability of staying in the same state.

We can observe from this figure that the POMDP policy achieves a much greater performance improvement in comparison to the existing and random policies when the transition probability of staying in the same state is very small. The average throughput in the existing policy gradually approaches to the POMDP case with the increase of that probability. This is because when the transition probability of staying in the same state increases, the channel becomes more memoryless, and the advantage of POMDP policy is not obvious given a memoryless channel.

5.3 Effects of the observation model parameters

The observation matrix in (30) is derived from the channel estimation error δ. We evaluate how the channel estimation error affects the average throughput.

Figure 7 shows the average throughput under different channel estimation errors δ for the different policies. All three policies' performance decreases significantly with the increase of channel estimation error. This is because an accurate channel state is difficult to obtain when the channel estimation error increases. A higher channel estimation error increases the probability of observing a wrong channel state and the probability of making a wrong decision. Nevertheless, from these two figures, we observe that the performance of the proposed POMDP policy does not decrease as much as the other two policies. This is because the POMDP policy considers the channel errors in the formulation, and it decreases the observation errors' impacts on the throughput performance.

6 Conclusions and future work

The distinct characteristics of VANETs, such as high node mobility and relatively low elevation of the antennas on vehicles, make the QoS provisioning challenging. In this article, we proposed to use recent advances in cooperative communications to enhance the QoS performance of VANETs. In order to address the security problem caused by cooperative communications, we presented a joint design of security and QoS provisioning in VANETs. We proposed a prevention-based technique for secure relay selection taking into consideration authentication protocol, which is based on hash chains and MT, to provide both end-to-end and hop-by-hop authentication and integrity protection. Particularly, we considered channel estimation errors and the impacts of security on throughput QoS performance in VANETs. The dynamic wireless channel was modeled as a finite-sate Markov process. With channel estimation errors, the channel state cannot accurately be observed. Therefore, we formulated the relay selection and the number of messages/data blocks selection problem as a POMDP. The optimal policy was obtained by a separated principle. Simulation results show that the number of messages/data blocks in the MT has significant impacts on the throughput QoS. The proposed scheme significantly improves the effective secure throughput. In addition, due to considering the channel errors in the formulation, the POMDP policy decreases the observation errors' impacts on the throughput performance.

Future work is in progress to consider network topology control in VANETs using the proposed combined security and QoS provisioning framework.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

We thank the reviewers for their detailed reviews and constructive comments, which have helped to improve the quality of this article. This study was in part supported by Beijing Laboratory For Mass Transit, he Key Projects in State Key Lab. of Rail Traffic control and Safety (RCS2012ZQ002, RCS2012K010), the China Education Ministry Funding Project (2013JBM124,2011JBZ014), the National Science Foundation of China (No. 61132003), the National High Technology Research and Development Program of China (863 Program) (2011AA110502), and by the Natural Sciences and Engineering Research Council (NSERC) of Canada and industrial and government partners, through NSERC-DIVA Strategic Research Network.

Author details

[1]State Key Lab. of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China. [2]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada.

Received: 2 September 2012 Accepted: 15 February 2013
Published: 27 March 2013

References

1. F-Y Wang, C Herget, D Zeng, Guest editorial developing and improving transportation systems: the structure and operation of IEEE intelligent transportation systems society. IEEE Trans. Intell. Transp. Sys. **6**(3), 261–264 (2005)

2. C Casetti, M Cesana, I Filippini, G Dan, I Marsh, in *Proceedings of the 7th EURO-NGI Conference on Next Generation Internet (NGI)*. Context-aware information dissemination in vehicular networks (Kaiserslau, Germany, 2011)
3. Y-T Wu, W Liao, C-L Tsao, T-N Lin, Impact of node mobility on link duration in multihop mobile networks. IEEE Trans. Veh. Technol. **58**, 2435–2442 (2009)
4. Q Wang, S Leng, H Fu, Y Zhang, An IEEE 802.11p-based multichannel MAC scheme with channel coordination for vehicular ad hoc networks. IEEE Trans. Intell. Trans. Syst. **13**, 449–458 (2012)
5. M Boban, T Vinhoza, M Ferreira, J Barros, O Tonguz, Impact of vehicles as obstacles in vehicular ad hoc networks. IEEE J. Sel. Areas Commun. **29**, 15–28 (2011)
6. P Alexander, D Haley, A Grant, Cooperative intelligent transport systems: 5.9-GHz field trials. Proc. IEEE. **99**, 1213–1235 (2011)
7. D Rawat, D Popescu, G Yan, S Olariu, Enhancing VANET performance by joint adaptation of transmission power and contention window size. IEEE Trans. Paral. Dist. Syst. **22**, 1528–1535 (2011)
8. L Zhou, B Zheng, B Geller, A Wei, S Xu, Y Li, Cross-layer rate control, medium access control and routing design in cooperative VANET. Comput. Commun. **31**, 2870–2882 (2008)
9. M Sepulcre, J Gozalvez, J Harri, H Hartenstein, Contextual communications congestion control for cooperative vehicular networks. IEEE Trans. Wirel. Commun. **10**, 385–389 (2011)
10. Z Ding, K Leung, Cross-layer routing using cooperative transmission in vehicular ad-hoc networks. IEEE J. Sel. Areas Commun. **29**, 571–581 (2011)
11. A Hamieh, J Ben-Othman, L Mokdad, in *Proceedings of the IEEE Globecom'09*. Detection of radio interference attacks in VANET (Honolulu, Hawaii, 2009)
12. Q Guan, FR Yu, S Jiang, VCM Leung, Joint topology control and authentication design in mobile ad hoc networks with cooperative communications. IEEE Trans. Veh. Technol. **61**, 2674–2685 (2012)
13. F Dressler, F Kargl, J Ott, O Tonguz, L Wischhof, Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl seminar. IEEE Commun. Mag. **49**, 158–164 (2011)
14. K Woradit, TQS Quek, W Suwansantisuk, H Wymeersch, L Wuttisittikulkij, MZ Win, Outage behavior of selective relaying schemes. IEEE Trans. Wirel. Commun. **8**, 3890–3895 (2009)
15. Q Guan, FR Yu, S Jiang, VCM Leung, Capacity-optimized topology control for MANETs with cooperative communications. IEEE Trans. Wirel. Commun. **10**, 2162–2170 (2011)
16. W Ni, G Shen, S Jin, T Fahldieck, R Muenzner, Cooperative relay in IEEE 802.16j MMR, Technical Report, IEEE C802.16j-06_006r1, Alcatel (2006). [http://www.ieee802.org/16/relay/contrib/C80216j-06_006.pdf]
17. PHJ Chong, F Adachi, S Hamalainen, V Leung, Technologies in multihop cellular network. IEEE Commun. Mag. **45**(9), 64–65 (2007)
18. S Bu, FR Yu, P Liu, P Manson, H Tang, Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE Trans. Veh. Technol. **60**, 1025–1036 (2011)
19. T Heer, S Gotz, OG Morchon, K Wehrle, in *Proceedings of the ACM CoNEXT'08*. ALPHA: an adaptive and lightweight protocol for hop-by-hop authentication (ACM, Madrid, 2008)
20. R Merkle, in *Proceedings of the CRYPTO'89*. A certified digital signature (Springer, Santa Barbara, 1989)
21. M Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. (Wiley, New York, 1994)
22. M Yu, J Li, in *Proceedings of the IEEE ICASSP'05*, vol. 3. Is amplify-and-forward practically better than decode-and-forward or vice versa? (IEEE, location Philadelphia, 2005), pp. 365–368
23. M Khalid, Y Wang, I Ra, R Sankar, Two-relay-based cooperative MAC protocol for wireless ad hoc networks. IEEE Trans. Veh. Technol. **60**, 3361–3373 (2011)
24. F Babich, G Lombardi, E Valentinuzzi, Variable order Markov modeling for LEO mobile satellite channels. Electron Lett. **35**, 621–623 (1999)
25. F Babich, G Lombardi, in *Proceedings of the IEEE VTC'97*. A measurement based Markov model for the indoor propagation channel (Phoenix, AZ, 1997), pp. 77–81
26. HS Wang, P-C Chang, On verifying the first-order Markovian assumption for a rayleigh fading channel model. IEEE Trans. Veh. Technol. **45**(2), 353–357 (1996)
27. C Pimentel, TH Falk, L Lisbôa, Finite-state Markov modeling of correlated Rician-fading channels. IEEE Trans. Veh. Technol. **53**(5), 1491–1501 (2004)
28. CD Iskander, PT Mathiopoulos, Fast simulation of diversity Nakagami fading channels using finite-state Markov models. IEEE Trans. Broadcast. **49**(3), 269–277 (2003)
29. Y Wei, FR Yu, M Song, Distributed optimal relay selection in wireless cooperative networks with finite-state Markov channels. IEEE Trans. Veh. Technol. **59**, 2149–2158 (2010)
30. L Zhu, FR Yu, B Ning, T Tang, Handoff performance improvements in MIMO-enabled communication-based train control systems. IEEE Trans. Intell. Transp. Syst. **13**, 582–593 (2012)
31. P Herhold, E Zimmermann, G Fettweis, in *Proceedings of the International Seminar on Communications*. A simple cooperative extension to wireless relaying (Zurich, Switzerland, 2004)
32. S Lin, D Costello, M Miller, Automatic-repeat-request error-control schemes. IEEE Commun. Mag. **22**(12), 5–17 (1984)
33. AT Hoang, M Motani, in *Proceedings of the IEEE WCNC'04*. Buffer and channel adaptive transmission over fading channels with imperfect channel state information (Atlanta, GA, 2004)
34. A Messac, E Melachrinoudis, CP Sukam, Aggregate objective functions and pareto frontiers: required relationships and practical implications. Optim. Eng. **1**, 171–188 (2000)
35. MB Gadallah, in *Proceedings of the 34th International Conference on Computers and Industrial Engineering*. On muti-objective optimization problem: modeling issues and numerical verification (San Francisco, USA, 2004), pp. 635–640
36. R Smallwood, E Sondik, Optimal control of partially observable Markov processes over a finite horizon. Oper. Res. **21**, 1071–1088 (1973)

doi:10.1186/1687-1499-2013-88
Cite this article as: Zhu *et al.*: A joint design of security and quality-of-service (QoS) provisioning in vehicular ad hoc networks with cooperative communications. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:88.