# A Joint Design for Topology and Security in MANETs with Cooperative Communications

Quansheng Guan*†, F. Richard Yu†, Shengming Jiang‡ and Victor C.M. Leung†

*School of Electronic and Information Engineering, South China University of Technology, P.R. China
†Department of Electronic and Computer Engineering, University of British Columbia, Canada
‡Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada

***Abstract*—Security is an important issue in mobile ad hoc networks (MANETs). However, security schemes have significant impacts on throughput. That is because 1) they need some overhead and consume some network resources, thus decrease throughput consequently, 2) most previous works consider security and throughput separately in designing a MANET, which can not achieve an overall optimization of network performance. In this paper, we propose a topology control scheme to improve throughput by jointly designing upper layer security schemes and physical layer schemes related to channel conditions and relay selections for cooperative communications. Simulation results show that our scheme can substantially improve throughput in MANETs.**

***Index Terms*—Security, throughput, topology control, cooperative communications**

## I. Introduction

Security is the main concern and bottleneck for widely deployed wireless applications due to the vulnerable open shared access medium and the stringent resource constraints [1]. Particularly, mobile ad hoc networks (MANETs) present more challenges to secure routing, key exchange, key distribution and management, as well as intrusion detection and protection [2], [3]. These challenges are attributed to the peculiarities of MANETs, i.e., multi-hop routing and packet forwarding, lack of infrastructure, dynamic topology, node cooperation, etc.

Recently, cooperative communication has been considered as a promising technique to improve transmission reliability [4], [5]. However, it brings extra challenges to security issues in MANETs. Cooperative communications make use of the broadcast nature of the wireless medium by the assistant of relay nodes. Although cooperative communication brings in significant benefits, it also raises serious security issues, e.g., it is possible for malicious nodes to join the network and relay unsolicited information to the destination thereby to compromise the network.

As the front line of defense, authentication is crucial for the security design [6], [7]. Since multiple-hop communications are used in MANETs with cooperative communications, not only end-to-end but also hop-by-hop authentication and message integrity are required to protect the network from tampering with and forging of packets by malicious nodes.

Another important issue in MANETs is topology control. Topologies in MANETs are changing over time as nodes are moving and adjusting their transmission and reception parameters all the time. The dynamic topology in MANETs has significant impact on the quality of service (QoS), especially for the end-to-end throughput in MANETs. Most existing topology control schemes are focused on adjusting the PHY or MAC layer parameters, such as transmission power and interference, to improve the overall network performance such as energy consumption, interference and network capacity for MANETs [8], [9].

Although security, topology control and cooperative communications are studied separately in most existing works, they are in fact closely correlated in MANETs. For example, security schemes such as authentications consume significant network resources (e.g., wireless bandwidth) and consequently decrease network throughput in MANETs. This problem will be more severe with the introduction of cooperative communications in MANETs, where high-volume data need not only end-to-end but also hop-by-hop authentication and message integrity. In this paper, we consider security and topology control jointly with cooperative communications in MANETs.

In order to jointly design throughput and security, a closed-form equation for the effective throughput under an authentication protocol is derived, which depends on some cross-layer network configurations. Then, we propose a joint authentication and topology control (JATC) scheme to adaptively tune the network configurations to optimize the effective throughput and the efficiency of authentication protocols for MANETs with cooperative communications. In addition, most existing topology control schemes assume that the wireless channel is well known. However, in practice, it is difficult to have the perfect knowledge of a dynamic channel [10]. Therefore, we only use the channel estimate in our scheme. The system is formulated as a discrete stochastic optimization problem, which can be solved using a stochastic approximation approach [11]–[13]. Simulation results are presented to show that JATC can substantially improve the throughput in MANETs with cooperative communications.

The rest of the paper is structured as follows. Section II

This work was supported in part by the Guangdong Provincial Key Lab. of Short-Range Wireless Detections and Communications, China and the National Fundamental Research and Development Programs of China (i.e., 973 Program, no. 2011CB707003).

978-1-61284-233-2/11/$26.00 ©2011 IEEE

describes the system model and the authentication protocol. JATC is presented in Section III. This problem is then solved by a discrete stochastic approximation approach in Section IV. Simulation results are presented and discussed in Section V. Finally, Section VI concludes this study.

## II. System Model for Topology Control and the Authentication Protocol

In this section, we first present the system model for topology control and then introduce an authentication protocol that can be used in MANETs with cooperative communications.

### A. System Model for Topology Control

In general, a network topology can be modeled as a graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, including all its nodes $\mathcal{V}$ and link connections $\mathcal{E}$ among them. Network topology control is essentially to determine where to deploy links and how links work to form a good topology, which can optimize some global network performance while preserving some global graph property (i.e., connectivity). Usually, a general distributed topology control problem is modeled as

$$\mathcal{G}_N^* = \arg\max f(\mathcal{G}_N) \text{ or } \mathcal{G}_N^* = \arg\min f(\mathcal{G}_N) \tag{1}$$

$$\textit{s.t. connectivity to all the neighbors},$$

where $\mathcal{G}_N(\mathcal{V}_N, \mathcal{E}_N)$ denotes the neighborhood graph. The above topology control problem contains three elements, denoted by a triple $\langle \mathbb{M}, \mathbb{P}, \mathbb{O} \rangle$. $\mathbb{M}$ presents the network model, $\mathbb{P}$ represents the desired network property, which often refers to network connectivity constraints, and $\mathbb{O}$ represents the optimization objective, which is determined by $f$ in (1). Each topology control has its own set of rules to connect the network. A good topology $\mathcal{G}_N^*(\mathcal{V}_N, \mathcal{E}_N^*)$ is constructed from the original topology $\mathcal{G}_N(\mathcal{V}_N, \mathcal{E}_N)$. How good the output topology is strongly related to the optimization objective.

The objective of topology control is achieved by adjusting some controllable parameters that affect link status such as transmission power, antenna direction, channel assignment, cooperative level and transmission manners. In general, multi-hop routing is performed to find a route for any two distant nodes. In each hop, considering that cooperative communications may improve communication reliability and efficiency [4], transmissions may be one of the following: direct transmissions, multi-hop transmissions and cooperative communications. In cooperative communications, the destination node decodes a combined signal from the source node and the relayed signals of interest from assistant relays. The other two types of transmissions can be regarded as special cooperative transmissions. A direct transmission utilizes no relays while a multi-hop transmission does not combine signals at the destination. The best type of transmissions and the best relay node can be determined according to the current channel conditions. Therefore, selections of the transmission manner and the relay node comprise a wireless link in MANETs.

On the other hand, we need to consider security and the above parameters jointly due to the reasons described in Section I. In this paper, we consider a modified authentication protocol, which leverages Merkle Trees (MTs) [14] and interactive hash chains [15] to generate pre-signatures and pre-acks and enable end-to-end as well as hop-by-hop integrity protection. The protocol is introduced in the following subsection.

### B. Authentication Protocol

A computationally efficient protocol for on-path end-to-end and hop-by-hop integrity protection and authentication based on hash chains has been proposed [7]. It combines concepts of interactive signatures and MTs to design a lightweight mechanism that is adaptive and flexible to the limited resources of mobile devices. In the following, we will describe how it works in MANETs 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 $r$ and the data block $m_j$, a verifier requires a set of complementary branches $\{B_c\}$, which increases logarithmically as the number of data blocks signed, to authenticate each data block independently. Thus, throughput, buffer memory, hash calculations and latency are subject to the size of signed data blocks. The operation process of the protocol begins with an initial handshake to exchange the anchors of hash chains. As depicted in Fig. 1, the protocol consists of a four-way packet exchange for each signed data message $m_j$. The first packet S1 consists of the root of the MT $r$ and a fresh hash-chain element of the signer. The A2 packet is attached with a signature chain to identify the verifier and with the root of the acknowledgment MT. The message $m_j$ is disclosed in S2 along with the set $\{B_c\}$ in order to be authenticated independently of other messages. An index $x_i$ and a secret $s_i$ are contained in A2 to identify the message $m_j$. In cooperative transmissions, the destination node in each link capture both signals from the source and the relay.

Moreover, the transmissions of A2 packets enable some automatic repeat request (ARQ) retransmission schemes [16] to be adaptive to dynamic channel conditions, which is discussed in the next subsection.

## III. A Joint Design for Authentication and Topology Control

### A. Throughput Analysis

The authentication protocol provides throughput adaptation in its configuration. As the study in [7], the total amount of payload transmitted with a single pre-signature (an S1/A1 exchange) is expressed by

$$s_{payload} = n \cdot (s_{packet} - s_h(\lceil \log_2 n \rceil + 1)). \tag{2}$$

A tradeoff between the signed payload of S2 packets in aNn MT and the additional signature data accompanied with S2 packets is necessarily considered, as the size of the set $\{B_c\}$ of complementary branches grows logarithmically with the increasing data chunks (S2 packets) in an MT.

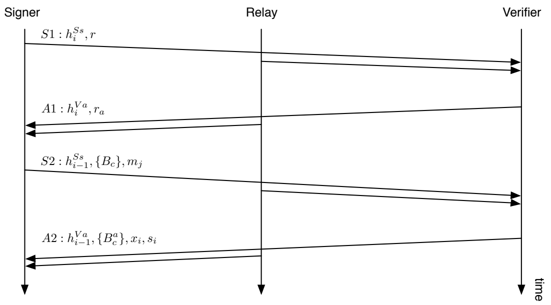
Signer
Relay
Verifier
$S1 : h_i^{Ss}, r$
$A1 : h_i^{Va}, r_a$
$S2 : h_{i-1}^{Ss}, \{B_c\}, m_j$
$A2 : h_{i-1}^{Va}, \{B_c^a\}, x_i, s_i$
time

Fig. 1. An authentication protocol for cooperative transmissions.

We are interested in the throughput performance of the protocol. To improve its reliability, an ARQ scheme is needed. As selective-repeat (SR)-ARQ has been proven to outperform other forms of ARQ schemes, we use SR-ARQ in the study. Detailed studies of ARQ schemes are beyond this paper. The throughput is defined as average rate of successfully message delivery over a communication channel.

Considering persistent ARQ, the average number of transmissions needed for one packet to be successfully accepted by the destination is

$$1 \cdot p_c + 2 \cdot p_c(1-p_c) + \cdots + \ell \cdot p_c(1-p_c)^{\ell} + \cdots = \frac{1}{p_c}, \quad (3)$$

where

$$p_c = (1-\epsilon)^{s_{packet}}. \quad (4)$$

and $\epsilon$ is the bit error rate (BER). According to [16], we can then calculate the throughput of the authentication protocol with SR-ARQ by

$$\eta = \frac{s_{payload}}{T_1+T_2} \cdot p_c, \quad (5)$$

where $T_1$ and $T_2$ are the transmission time needed for S1/A1 and S2/A2 exchanges for $s_{payload}$ respectively. As shown in Fig. 1, multiple S2 packets are transmitted following an S1/A1 exchange. The S1/A1 initial pre-signature process can be regarded to work in a basic stop-and-wait ARQ mode, where an S1 packet is transmitted by the source, processed and replied with an A1 packet by the destination. The time $T_2$ is taken by message transmissions in SR-ARQ mode. For two point-to-point communicating nodes, $T_1$ and $T_2$ are derived respectively as follows,

$$T_1 = t_{S1} + IFS + t_{A1} + IFS, \quad (6)$$

$$T_2 = n(t_{S2} + IFS), \quad (7)$$

where IFS denotes inter frame space between two consecutive packets and $t$ is the frame transmission time.

To integrate the relay selection and the choice of transmission manners, we use $\theta = (n, s_{packet}, k)$ as a configuration for a node. Given a node 0 and one of its neighbors $j$, $\theta_j = (n, s_{packet}, k)_j$ is the configuration for this neighbor link and $k_j$ denotes the selected relays, where $k_j \in K_j = \{0, 1, \cdots, |\mathcal{V}_N|, |\mathcal{V}_N|+1, 2|\mathcal{V}_N|\} - \{j, |\mathcal{V}_N|+j\}$. The case $k_j = 0$ corresponds to direct transmissions. Otherwise, $k_j$ is selected for multi-hop transmissions and $k_j + |\mathcal{V}_N|$ is the same relay but for cooperative transmissions. We combine the selections of the transmission manners and relays in the notation $k$. When $k$ is determined, it also determines the type of transmissions and the relays. The throughput expressions are different for the three types of transmissions as aforementioned in Subsection II-A. They are summarized as

$$\eta(\theta_j) = \begin{cases} \frac{s_{payload}}{T_1+T_2} \cdot p_c^{SD}, & k_j = 0 \\ \frac{s_{payload}}{T_1+T_2} \cdot (\frac{1}{p_c^{SR}} + \frac{1}{p_c^{RD}})^{-1}, & 0 < k_j \leq |\mathcal{V}_N| \\ \frac{s_{payload}}{2(T_1+T_2)} \cdot p_c^{SRD}, & |\mathcal{V}_N| < k_j \leq 2|\mathcal{V}_N|, \end{cases} \quad (8)$$

where $p_c^{SD}$, $p_c^{SR}$ and $p_c^{RD}$ are calculated by (4). The BERs therein are $\epsilon(\gamma_{SD})$, $\epsilon(\gamma_{SR})$ and $\epsilon(\gamma_{RD})$ respectively, where

$$\epsilon(x) = \frac{1}{2}\left(1 - \sqrt{\frac{x}{1+x}}\right). \quad (9)$$

$p_c^{SRD}$ is the combined signal decoding correct rate at the destination [17]. The BER for $p_c^{SRD}$ in (4) is

$$\epsilon_{SRD} = P_{out}^{SR} \cdot \epsilon_{SD} + (1 - P_{out}^{SR}) \cdot \epsilon_{div}, \quad (10)$$

where $P_{out}^{SR}$ is the outage probability for the link from the source R to the destination D,

$$P_{out}^{SR} = 1 - exp\{-\frac{2^{2r}-1}{\gamma_{SR}}\}, \quad (11)$$

and the BER for the combined signal decoding is

$$\epsilon_{div} = \frac{1}{2}\left(1 + \frac{1}{\gamma_{RD} - \gamma_{SR}}\left(\frac{\gamma_{SR}}{\sqrt{1+\frac{1}{\gamma_{SR}}}} - \frac{\gamma_{RD}}{\sqrt{1+\frac{1}{\gamma_{RD}}}}\right)\right).$$

### B. The JATC Scheme

As discussed in the preceding section, the throughput depends on some coupled configurations. First of all, the three types of transmissions have distinct throughput. Even for multi-hop transmissions and cooperative transmissions, the selection of relays has significant impact on throughput since each relay has its own physical layer parameters. A better SNR in the wireless channel results in a smaller outage probability and a higher outage capacity as well as a better BER. The relay with the best BER for the cooperative link is preferred for the throughput. Again, the packet size, which is managed by segmentation techniques, also has impact on throughput efficiency. Larger packet size increases the amount of payload in that packet, however also increases packet error rate and decreases $p_c$ in the throughput formulas. In addition, the MT size $n$, i.e., the number of signed data blocks in an MT, is the vital parameter for the authentication protocol. We focus on its impact on throughput in this study. The increasing of $n$ also increases the overhead of transmissions and the overhead has to be less than the packet size, or the payload will drop to zero according to (2). Regarding the security respect, the increasing of $n$ improves the authentication strength of a packet due to the increased sizes of complementary branches required. However, it may decrease the transmission throughput.

Topology control schemes usually consider the network-wide configuration. In order to extend the local configuration to a network-wide profile for traffic load balance, network capacity improvement, etc, we need to take some network environment such as interference into consideration [8]. The interference of a link is defined as the number of its influenced nodes during transmissions. Since all the neighbors of the transmitter and the receiver have to be silent during the transmission with onmi-antenna, we specify the link interference as the union coverage neighbors of nodes involved in the transmissions. A decreasing of interference will result in higher network capacity. Let $Cov(j)$ denote the neighbor set of $j$ and $I_{i\rightarrow j} = Cov(i) \cup Cov(j)$. The interference for different types of transmissions is obtained as follows,

$$I(\theta_j)=\begin{cases} I_{0\rightarrow j}, & \theta_j = 0 \\ \max\{I_{0\rightarrow k_j}, I_{k_j\rightarrow j}\}(\theta_j), & 0<\theta_j \leq |\mathcal{V}_N| \\ Cov(0)\cup Cov(k_j)\cup Cov(j), & n<\theta_j\leq 2|\mathcal{V}_N|. \end{cases} \quad (12)$$

Then, the optimal configuration for a link is obtained by

$$\theta_j^* = \arg\max_{\theta_j\in\Theta_j} f(\theta_j) = \frac{\eta(\theta_j)}{|I(\theta_j)|}. \quad (13)$$

In general, distributed topology control schemes are desired to handle all the neighbor links, rather than a single link. As a result, we use throughput per node as the objective of all the link configurations. Then JATC is formulated as

$$\theta^* = \arg\max \sum f(\theta_j). \quad (14)$$

The objective functions of both optimization problems of (13) and (14) require the knowledge of channel states (i.e., SNR). In practice, the perfect knowledge of a dynamic channel is unavailable. We can only use the estimated version of the channel [10]. In this sense, we only have the estimate of the objective function including some noise in practice. Therefore, the problems of (13) and (14) become discrete stochastic optimization problems. The complexity of the topology control problem (14) can be reduced by (13) since the relay selection for each link can be conducted individually and independently since it is the MAC function to avoid interference among different adjacent links. In this sense, we get $\max\sum f(\theta_j) = \sum \max f(\theta_j)$. Then the problem (14) can be divided to several independent subproblems (13), which results in significant reduction of feasible solution space from $|\Theta_j|^{|V_N|}$ to $|\Theta_j|\cdot|V_N|$, where $|\Theta_j| = |\{n_j\}|\cdot|\{s_{packet}\}|\cdot|K_j|$. The computations to find the optimal configuration for topology control are consequently dramatically mitigated.

As described in the formulation (1) and in the topology control triple $\langle \mathbb{M}, \mathbb{P}, \mathbb{O}\rangle$, JATC should guarantee network connectivity. In fact, the network end-to-end network connectivity is preserved via a hop-by-hop manner in (14) since it preserves all the neighbor links [9].

## IV. Discrete Stochastic Approximation Approach

Intuitively, a brute force approach can be used to solve the discrete stochastic problems (13) and (14). For each possible link configuration $\theta_j \in \Theta_j$, the expected objective function is approximated by empirically averaging $N$ estimates of its observations as $N$ grows to infinity.

Based on the estimations, the global maximizer of the objective function is exhaustively searched. Obviously, this heuristic approach requires a large number of objective evaluations, thus takes long optimization times and consumes a large amount of computations. The fact exists in that many optimization times are wasted in estimating the non-optimal configuration points. In fact, what we are concernd is only the estimates of the optimal configuration.

Since the brute force approach is inefficient, we turn to other more efficient methods. Discrete stochastic optimization problems have been extensively analyzed and discrete stochastic approximation approaches are developed to solve these problems [11]–[13].

Let $\theta_j[i]$ denote the configuration at $i$th iteration and $\boldsymbol{e}_{\theta_j[i]}$ be a unit $|\Theta_j| \times 1$ vector with a one for the configuration $\theta_j[i]$ and zeros for other configurations in $\Theta_j$. The notation $\boldsymbol{\pi}[i] = [\pi[i,1],\cdots,\pi[i,|\Theta_j|]]$ presents the state probability vector. A basic discrete stochastic approximation approach for JATC is described in Algorithm 1. It consists of four steps in each iteration. Algorithm 1 randomly selects an initial configuration $\theta_j[0]$ from the solution space. In the iteration, an alternative configuration $\tilde{\theta}_j[i]$ is uniformly generated from the neighborhood space $\mathcal{N}_{\theta_j[i]}$, which is defined as $\mathcal{N}_{\theta_j[i]} = \Theta_j - \{\theta_j[i]\}$. The configuration with larger evaluated throughput is chosen as the current visiting state. The state probability vector is updated at each iteration. In fact, this empirical occupation probabilities stand for the visiting frequencies of the possible solutions. At the $i$th iteration, suppose there have been $W[i,\theta_j[i]]$ iteration times that visited $\theta_j[i]$ so far, the decreasing step size $\mu[i] = \frac{1}{i}$ updates the state probabilities as

$$\pi[i,\theta_j[i]] = \frac{W[i,\theta_j[i]]}{i}. \quad (15)$$

This decreasing step size makes the algorithm increasingly conservative to stay in the current promising state. $\hat{\theta}_j[i]$ is the most frequently visited state in the state probability vector $\pi[i]$.

**Algorithm 1.** *Basic algorithm for JATC*

```
Step 0 (Initialization)
  At iteration $i = 0$, select an initial state of the algorithm
  $\theta_j[0] \in \Theta_j$ randomly and set $\boldsymbol{\pi}[0] = \boldsymbol{e}_{\theta_j[0]}$. Initialize
  estimate of optimal relay selection as $\hat{\theta}_j[0] = \theta_j[0]$.
Step 1 (Sampling and evaluation)
  Evaluate $g(\theta_j[i])$ given $\theta_j[i]$ at iteration $i$.
  Generate an alternative $\tilde{\theta}_j[i] \in \mathcal{N}_{\theta_j[i]}$ uniformly and eval-
  uate $g(\tilde{\theta}_j[i])$.
Step 2 (Acceptance)
  IF $g(\tilde{\theta}_j[i]) > g(\theta_j[i])$
        $\theta_j[i+1] = \tilde{\theta}_j[i]$
  ELSE
        $\theta_j[i+1] = \theta_j[i]$
  END IF
```

```
Step 3 (Update empirical state occupation probability)
    $\boldsymbol{\pi}[i+1] = \boldsymbol{\pi}[i] + \mu[i+1](\boldsymbol{e}_{\theta_j[i+1]} - \boldsymbol{\pi}[i])$    (16)
  with a decreasing step $\mu[i] = \frac{1}{i}$.
Step 4 (Update estimate of optimal maximizer)
  IF $\pi[i+1, \theta_j^{(i+1)}] > \pi[i+1, \hat{\theta}_j^{(i)}]$
      $\hat{\theta}_j[i+1] = \theta_j[i+1]$
  ELSE
      $\hat{\theta}_j[i+1] = \hat{\theta}_j[i]$
  END IF
  Go back to Step 1.
```

The visited state sequence $\{\theta_j[i]\}$ is a Markov chain on $\Theta_j$ since it is determined by the current sample and the previous state. It is not necessarily guaranteed to converge. However, the sequence $\{\hat{\theta}_j[i]\}$ will be proven to almost surely converge to the global maximizer $\theta_j^*$ in the next subsection. Accordingly, after sufficient iterations, $\{\hat{\theta}_j[i]\}$ is selected as the output of the algorithm.

The step size $\mu$ in (16) is the parameter that controls the speed of convergence, the stable state and the tracking behavior of Algorithm 1. The algorithm with a small $\mu$ opts to stay in one state so that it ensures low mis-adjustments of optimal state in stationary networks. However, it will result in slow convergence and may not track the dynamic changing topologies in MANETs. On the other hand, though a large $\mu$ makes fast convergence and good tracking capability, it may not track the optimal state due to the high mis-adjustments. Take an extreme case for an instant. When $\mu = 1$, the previous states are totally forgotten in the algorithm, and no statistical knowledge of the environment is available.

Apparently, the decreasing step-size in Algorithm 1 is not suitable for dynamic MANETs. The algorithm is expected to converge fast and has an output state close to the optimal point in the mean-squared-error. Many approaches are available to design the adaptive step-size sequence [18]. We employ a gradient descent least-mean-square-like algorithm to reduce the squared estimation error at each iteration.

The error is defined as

$$\boldsymbol{\epsilon}^{\mu}[i] = \boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i]. \tag{17}$$

The step size is updated using a gradient-based procedure,

$$\mu[i+1] = \mu[i] - \frac{\rho}{2}\frac{\partial \phi(\boldsymbol{\epsilon}[i])}{\partial \mu[i]}, \tag{18}$$

where the error cost function $\phi(\boldsymbol{\epsilon}[i])$ is usually the squared estimation error, i.e., $\phi(\boldsymbol{\epsilon}[i]) = \boldsymbol{\epsilon}[i]\boldsymbol{\epsilon}[i]^T$. Then,

$$\frac{\partial \phi(\boldsymbol{\epsilon}[i])}{\partial \mu[i]} = -2(\boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i])^T \boldsymbol{J}^{\mu}[i], \tag{19}$$

where $\boldsymbol{J}^{\mu}[i] = \frac{\partial}{\partial \mu[i]}\boldsymbol{\pi}^{\mu}[i]$. Differentiating equation (16) with respect to $\mu$, we obtain

$$\boldsymbol{J}^{\mu}[i+1] = \boldsymbol{J}^{\mu}[i] - \mu \boldsymbol{J}^{\mu}[i] + (\boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i]). \tag{20}$$

**Algorithm 2.** *Adaptive step-size algorithm for JATC (JATC-ASS).*

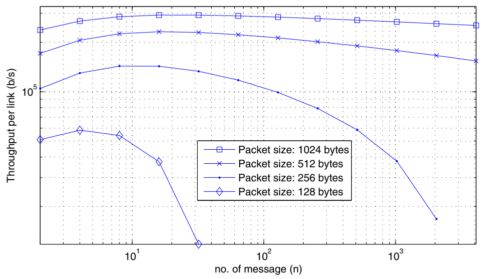

Fig. 2. Throughput changes with signed packets per S1 and the packet sizes.

*Substitute Step 3 of Algorithm 1 by*

*Step 3´ (Update empirical state occupation probability)*

$$\boldsymbol{\epsilon}[i] = \boldsymbol{e}[i+1] - \boldsymbol{\pi}[i]$$
$$\boldsymbol{\pi}[i+1] = \boldsymbol{\pi}[i] + \mu[i]\boldsymbol{\epsilon}[i]$$
$$\mu[i+1] = \mu[i] + \rho\boldsymbol{\epsilon}[i]^T \boldsymbol{J}^{\mu}[i]$$
$$\boldsymbol{J}[i+1] = (1-\mu[i])\boldsymbol{J}[i] + \boldsymbol{\epsilon}[i], \boldsymbol{J}[0] = 0$$

Algorithm 2 consists of two cross-coupled adaptive algorithms: a discrete algorithm to select the optimal link configurations and a continuous algorithm to adapt the step-size. Our results later will show that it tracks the dynamic changes well.

## V. Simulation Results and Discussions

In the simulations, we set up a scenario with 30 nodes randomly deployed in an area of 800 × 800 square meters. The maximum transmission range of mobile nodes is 300 meters and the wireless channel follows a slow flat fading Raleigh distribution, which can be estimated by the training preamble in practice. A 20-byte hash is used for the authentication protocol. The following packet sizes are considered, $s_{packet} = \{128, 256, 512, 1024\}$ bytes.

A study is carried out to verify the throughput model of JATC. It is shown in Fig. 2 that the throughput changes with the number of the signed packets per S1/A1 exchange and the packet sizes. There exists an optimal $n$ value and an optimal packet size to maximize the throughput. The result in Fig. 2 necessitates the joint consideration in a link configuration $\theta = (n, s_{packet}, k)$.

The ultimate objective of JATC is to optimize the network topology configuration to maximum throughput of the network. We compare JATC with the LLISE topology control scheme in [8]. Fig. 3 shows that the aggregate throughput in each iteration approaches to the optimum iteratively. The average result of 200 runs in Fig. 4 indicates that the algorithm converges.

## VI. Conclusions and Future Work

Since security and network throughput are two major concerns of MANETs, we have developed a joint design for authentication and topology control (JATC) scheme in this paper for MANETs with cooperative communications. With the throughput closed-form equation in this paper, JATC tunes the parameters of up-layer authentication protocol and

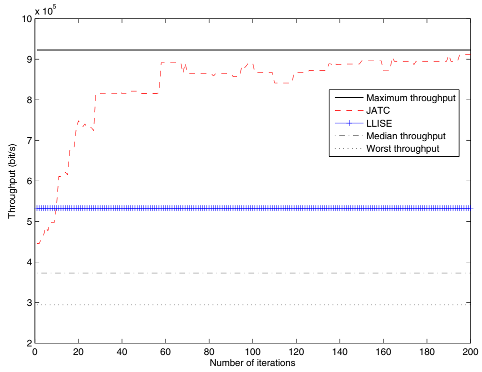

Fig. 3. Single run to optimize topology configuration.

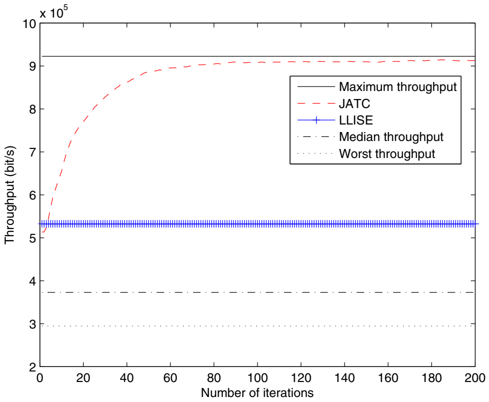

Fig. 4. Average of 200 runs to optimize topology configuration.

physical layer transmission settings to maximize the throughput. In addition, a discrete stochastic approximation approach was employed in JATC to deal with the imperfect channel knowledge and the dynamically changing topology. Simulation results were presented to show that JATC works well in MANETs. Future work is to further study the cooperative routing performance on the resultant topology.

## References

[1] H. Yang, F. Ricciato, S. Lu, and L. Zhang, "Securing a wireless world," *Proc. the IEEE*, vol. 94, no. 2, pp. 442–454, 2006.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[3] N. Garg and R. Mahapatra, "MANET Security Issues," *International Journal of Computer Science and Network Security*, vol. 9, no. 8, p. 241, 2009.

[4] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Comm. Mag.*, vol. 42, no. 10, pp. 74–80, 2004.

[5] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[6] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.

[7] T. Heer, S. Gtz, O. G. Morchon, and K. Wehrle, "ALPHA: an adaptive and lightweight protocol for hop-by-hop authentication," in *Proc. ACM CoNEXT*, (Madrid, Spain), pp. 1–12, ACM, 2008.

[8] M. Burkhart, P. von Rickenbach, R. Wattenhofer, and A. Zollinger, "Does topology control reduce interference?," in *Proc. 5th ACM Int. Symposium on Mobile Ad Hoc Networking and Computing*, (Roppongi Hills, Tokyo, Japan), May 2004.

[9] Q. Guan, Q. Ding, and S. Jiang, "A minimum energy path topology control algorithm for wireless multihop networks," in *Proc. IWCMC*, (Leipzig, Germany), June 2009.

[10] L. Tong, B. Sadler, and M. Dong, "Pilot-assisted wireless transmissions: general model, design criteria, and signal processing," *IEEE Signal Proc. Mag.*, vol. 21, no. 6, pp. 12–25, 2004.

[11] H. Kushner, "Stochastic approximation: a survey," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, no. 1, pp. 87–96, 2010.

[12] S. Andradóttir, "Accelerating the convergence of random search methods for discrete stochastic optimization," *ACM Trans. Model. Comput. Simul.*, vol. 9, no. 4, pp. 349–380, 1999.

[13] I. Berenguer, X. Wang, and V. Krishnamurthy, "Adaptive MIMO antenna selection via discrete stochastic optimization," *IEEE Trans. Signal Proc.*, vol. 53, no. 11, pp. 4315–4329, 2005.

[14] R. Merkle, "A certified digital signature," in *Proc. Advances in Cryptology CRYPTO89*, pp. 218–238, 1989.

[15] L. Lamport, "Password authentication with insecure communication," *ACM Commun.*, vol. 24, no. 11, pp. 770–772, 1981.

[16] S. Lin, D. J. Costello, and M. J. Miller, "Automatic-repeat-request error control schemes," *IEEE Commun. Mag.*, vol. 22, no. 12, pp. 5–17, 1984.

[17] P. Herhold, E. Zimmermann, and G. Fettweis, "A simple cooperative extension to wireless relaying," in *Proc. 2004 International Zurich Seminar on Communications*, (Zurich, Switzerland), Aug. 2004.

[18] V. Mathews and Z. Xie, "A stochastic gradient adaptive filter with gradient adaptive step size," *IEEE Trans. Signal Processing*, vol. 41, no. 6, pp. 2075–2087, 1993.