Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications

Quansheng Guan, *Member, IEEE*, F. Richard Yu, *Senior Member, IEEE*, Shengming Jiang, *Senior Member, IEEE*, and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*—Security is the main concern and bottleneck for widely deployed wireless applications due to the fact that wireless channels are vulnerable to attacks and that wireless bandwidth is a constrained resource. In this sense, it is desirable to adaptively achieve security according to the available resource. In particular, mobile ad hoc networks (MANETs) based on cooperative communication (CC) present significant challenges to security issues, as well as issues of network performance and management. In this paper, we focus on authentication and topology control issues. Although authentication and topology control are separately studied in most existing works, they are, in fact, closely correlated in MANETs. For example, both authentication and topology control schemes have significant impacts on throughput. In this paper, we jointly consider authentication and topology control. Specifically, we analyze the effective throughput with upper layer authentication schemes and physical-layer schemes related to channel conditions and relay selections for CCs. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. JATC is formulated as a discrete stochastic optimization problem, which does not require prior perfect channel status but only channel estimate. We also mathematically prove the tracking convergence property and the convergence rate of the discrete stochastic optimization approach in this paper. Simulation results show that our scheme can substantially improve throughput in MANETs with CC.**

***Index Terms*—Cooperative communication (CC), mobile ad hoc networks (MANETs), security, topology control.**

I. Introduction

RECENTLY, cooperative communication (CC) has been considered as a promising technique to improve transmission reliability over the ever-challenging wireless medium [1], [2]. CC exploits user diversity to emulate multiple-antenna systems, making use of the broadcast nature of the wireless medium by relaying the overheard messages from the source to the destination. Although CC brings significant benefits, it also raises serious security issues. For example, it is possible for malicious nodes to join the network and relay unsolicited information to the destination, thereby compromising the network. As the front line of defense, authentication is crucial for the security design [3]–[5]. Since multiple-hop communications are used in mobile ad hoc networks with CC (CC-MANETs), not only end-to-end (e2e) but also hop-by-hop (HBH) authentication and message integrity are required to protect the network from tampering with and forging of packets by malicious nodes.

Security has become the main concern and bottleneck for widely deployed wireless applications [6]. This issue can be seen in two aspects: First, the open shared access medium is vulnerable to attacks. Second, the wireless resources are stringently constrained. In particular, CC-MANETs present more challenges to secure routing, key exchange, and management, as well as intrusion detection and protection [7]–[9]. These challenges are attributed to the peculiarities of MANETs, such as multihop routing and packet forwarding, lack of infrastructure, dynamic topology, and node cooperation.

Security always comes with a price in terms of performance (e.g., network throughput) degradation [10]. It is desirable to adaptively achieve security according to the available resource without much performance degradation in the network. Topology control is a scheme that optimizes network performance in a network-wide perspective. Since the major activities involved in self-organization are neighbor discovery and topology organization, topology control is an important issue in MANETs, where topologies are changing over time as nodes are moving and adjusting their transceiver parameters all the time. The dynamic topology in MANETs has significant impact on the quality of service (QoS), particularly for the e2e throughput in MANETs. Topology control is referred to as selecting a set of neighbors to establish logical links and dynamically adjust the transceiver parameters [11]. Most existing topology control

Manuscript received June 26, 2011; revised November 13, 2011 and February 26, 2012; accepted April 5, 2012. Date of publication April 26, 2012; date of current version July 10, 2012. This work was supported in part by the National Fundamental Research and Development Programs of China (i.e., 973 Program, Grant 2011CB707003), by the National Natural Science Foundation of China (Grant 61101083), and by the Fundamental Research Funds for the Central Universities of China (Grant 2012ZM0021 and Grant 2012ZZ0031), South China University of Technology. The review of this paper was coordinated by Prof./Dr. Y. Zhang.

Q. Guan and S. Jiang are with South China University of Technology, Guangzhou 510640, China (e-mail: eeqshguan@scut.edu.cn; shmjiang@scut.edu.cn).

F. R. Yu is with Carleton School of Information Technology and the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: richard_yu@carleton.ca).

V. C. M. Leung is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: vleung@ece.ubc.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2012.2196061

schemes are focused on adjusting the physical (PHY)-layer or medium-access control (MAC)-layer parameters, such as transmission power and interference, to improve the overall network performance, such as energy consumption [12], interference [13], [14], and network capacity [15] for MANETs. Recently, some security-aware topology control schemes have been studied in [16] and [17]. They try to exclude malicious nodes in the network topology while maintaining connectivity, thus minimizing the harm to the network. Indeed, topology control has been exploited to form a trusted network for key distribution, routing, and network coding [18]–[20]. However, security is not a single-layer issue. It should be considered spanning over the entire protocol stack for the overall network performance improvement.

Although security, topology control, and CC are separately studied in most existing works, they are, in fact, closely correlated in MANETs, e.g., security schemes such as authentications consume significant network resources (e.g., wireless bandwidth) and consequently decrease network throughput in MANETs [10]. In this sense, security and throughput are conflicting aspects to some degrees. This problem will be more severe with the introduction of CC in MANETs.

Since topology control can be used to improve network throughput performance [11], we jointly consider security and topology control for CC-MANETs in this paper. To jointly design topology and authentication, a closed-form equation for the effective link throughput under an authentication protocol is derived, which depends on 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 CC-MANETs. In addition, most existing topology control schemes assume that the wireless channel is perfectly known. However, in practice, it is difficult to have perfect knowledge of a dynamic channel [21], [22]. 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 [23]–[26]. Simulation results are presented to show that JATC can substantially improve the throughput with authentication and integrity protection in CC-MANETs.

The remainder of this paper is structured as follows: Section II describes the system model and the authentication protocol. With the throughput analysis in Section III, JATC is presented in Section IV. This problem is then solved by a discrete stochastic approximation approach in Section V. Simulation results are presented and discussed in Section VI. Finally, Section VII concludes this study.

II. System Model for Topology Control and the Authentication Protocol

To jointly consider security and topology control, in this section, we first present the system model for topology control and then introduce an authentication protocol that can be used in CC-MANETs.

A. System Model for Topology Control

In general, a network topology can be described 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). Since it is difficult to collect the entire network information in MANETs, topology control in such networks should be resolved by distributed schemes, which are executed by each individual node to optimize all the neighboring connections. Usually, a general distributed topology control problem is modeled as

$$\mathcal{G}_N^* = \arg\max f(\mathcal{G}_N) \text{ or } \mathcal{G}_N^* = \arg\min f(\mathcal{G}_N) \quad \text{s.t. connectivity to all the neighbors} \quad (1)$$

where $\mathcal{G}_N(\mathcal{V}_N, \mathcal{E}_N)$ denotes the neighborhood graph obtained by each node. The aforementioned topology control problem contains three elements, which are denoted by a triple $\langle \mathbb{M}, \mathbb{P}, \mathbb{O} \rangle$ [27]. $\mathbb{M}$ presents the network model; $\mathbb{P}$ represents the desired network property, which is often the network connectivity constraint; 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 $\mathcal{G}_N^*$ is constructed from the original topology $\mathcal{G}_N$. How good the output topology is strongly related to the optimization objective in (1).

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. Considering that CC may improve communication reliability and efficiency [1], transmissions in a MANET may be one of the following: direct transmissions (DTs), multihop transmissions (MTs), and CCs. In CCs, the destination node decodes a combined signal from the source node and the relayed signals of interest from assistant relays. In this paper, a decode-and-forward (DF) scheme is used. The other two types of transmissions can be regarded as special cooperative transmissions. A DT utilizes no relays, whereas an MT does not combine signals at the destination. Therefore, the selection of the transmission manner and the selection of the relay node comprise a wireless link and thus determine the network topology in MANETs. A link refers to a logical connection for two neighboring nodes working possibly in one of the three transmission modes. The best type of transmissions and the best relay node can be determined according to the current channel conditions. In this paper, we consider only dual-hop transmissions since dividing a neighboring link into too many hops may introduce more duplicates of packets in the network and thus decrease network capacity according to [28].

In distributed topology control, every node independently executes the algorithm to determine the neighboring connections, which are the main element in a network topology. The entire network connectivity is preserved in an HBH manner. Suppose that the original topology $G(V, E)$ is connected (e.g., the

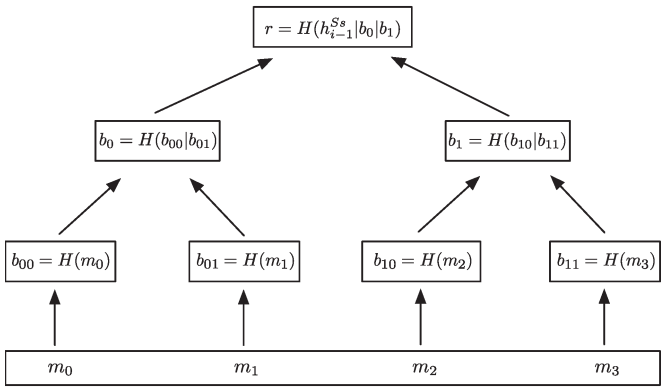


Fig. 1. Merkle tree.

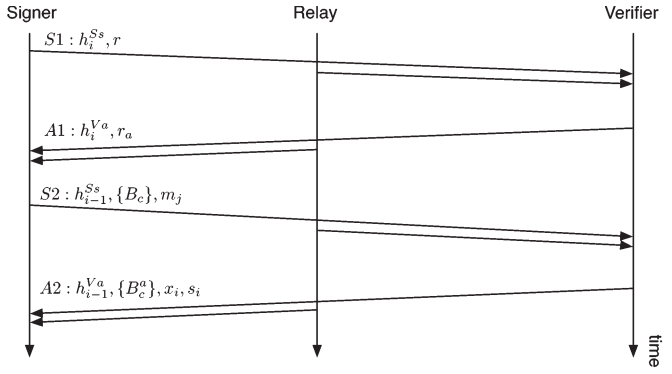


Fig. 2. Authentication protocol for cooperative transmissions. Each packet is attached with a signature hash chain to identify the sender. The first handshake exchanges the root r of the Merkle Tree in S1/A1 packets. Messages and the corresponding complementary $\{B_c\}$ are contained in S2 packets, whereas they are acknowledged by A2 packets. x_i and s_i are used to identify the message.

transmission range is set to be sufficiently large). By preserving all the neighboring connections in E (i.e., the connection can be configured to use DT, MT, or cooperative transmission), the entire network connectivity is maintained.

B. Authentication Protocol

A computationally efficient protocol for e2e and HBH integrity verification and authentication based on hash chains has been proposed [5]. It combines concepts of interactive signatures and Merkle Trees [29] to design a lightweight mechanism that is adaptive and flexible to the limited resources of mobile devices.

A hash chain [30] is a successive application of any cryptographic hash function $H(x)$ by hashing a random seed variable x. It is recursively and sequentially calculated by $h_i = H(h_{i-1})$, where $h_1 = H(x)$. Thus, $h_i = H^i(x)$ in a hash chain of length i. The hash chain is usually applied in an opposite sequence since h_i will not be revealed without h_{i-1}. In the authentication protocol, the last element of the hash chain, i.e., the *anchor* h_i, is initially provided by the owner to the verifier. The verifier can confirm the authenticity of the owner with h_{i-1} by subsequently hashing h_{i-1}.

A Merkle Tree is a binary tree of hashes with the leaves as hashes of data messages and nodes as the hashes of the concatenation of their respective children. The root of the Merkle Tree, which is calculated by its leaves and nodes, is used as presignature information. To independently authenticate each message, the message m_j, the root r of the Merkle Tree, and a set of complementary branches $\{B_c\}$ are required. Take the Merkle Tree in Fig. 1 as an example. To authenticate m_2, the sibling node of the nodes on the path from m_2 to r should be included in $\{B_c\}$. In this case, $\{B_c\} = \{b_{00}\}$. The verifier recalculates r with $\{B_c\}$ and m_j. Message m_j is authentic if and only if the recalculated value matches the root r.

The operation process of the protocol begins with an initial handshake to exchange the anchors of hash chains. As shown in Fig. 2, the protocol consists of a four-way packet exchange for each signed data message m_j. The signer establishes a signature Merkle Tree before the four-way exchange. Let S1, A1, S2, and A2 denote the packets in the four-way exchange, respectively. In Fig. 2, the S1/A1 packet consists of the root of the signature/acknowledgment Merkle Tree r and a fresh hash-chain element of the signer/verifier. The signer and verifier maintain their own signature and acknowledgment hash chains to identify themselves. Message m_j is disclosed in S2, along with a set of complementary branches $\{B_c\}$. On receiving S2, the verifier obtains messages m_j and $\{B_c\}$ and uses them to regenerate the Merkle Tree root. Comparing this root with the received r in S1, message m_j is authenticated, and its integrity is verified. An index x_i and a secret s_i are contained in A2 to identify message m_j. Herein, the set of complementary branches $\{B_c\}$, which logarithmically increases with the number of the signed data messages in a Merkle Tree, enables the verifier to independently authenticate each message. Thus, throughput, buffer memory, hash calculations, and latency are subject to the size of signed data blocks. Note that CCs occupy two time slots in the transmissions. The packets in the protocol, including S1, A1, S2, and A2, are broadcast to the relay and the verifier in the first time slot. The relay forwards them to the verifier in the second time slot. The signals are combined to decode the information at the verifier.

Moreover, the susceptible and fluctuating wireless channel necessitates the adoption of techniques such as automatic repeat request (ARQ) for reliable transmissions. The transmissions of A2 packets enable some ARQ retransmission schemes [31] to be adaptive to dynamic channel conditions, which is discussed in the next section.

III. Throughput Analysis

The authentication protocol provides throughput adaptation in its configuration. As the study in [5], the total amount of payload transmitted with a single presignature (i.e., S1/A1 exchange as shown in Fig. 2) is expressed by

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

where s_{packet} is the packet size, s_h is the hash size, and n is the size of the Merkle Tree. A tradeoff between the signed payload of S2 packets in a Merkle Tree and the additional signature data accompanied with S2 packets is necessarily considered, as the size of the set $\{B_c\}$ of complementary branches logarithmically grows with the number of data chunks (S2 packets) in Merkle Tree. When this set approaches packet size s_{packet}, s_{payload} drops to zero.

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 the average rate of successfully message delivery over a communication channel.

The average number of transmissions needed for one packet to be successfully accepted by the destination is

$$\sum_{i=1}^{\infty} i p_c (1-p_c)^{i-1} = \frac{1}{p_c} \tag{3}$$

where

$$p_c = (1-\epsilon)^{s_{\text{packet}}} \tag{4}$$

and ϵ is the bit error rate (BER). According to [31], we can then calculate the throughput of the authentication protocol with SR-ARQ by

$$\eta = \frac{s_{\text{payload}}}{T_1 + T_2} \cdot p_c \tag{5}$$

where T_1 and T_2 are the transmission time needed for an S1/A1 and S2/A2 exchanges for s_{payload}, respectively. As shown in Fig. 2, multiple S2 packets are transmitted, following an S1/A1 exchange. The S1/A1 initial presignature 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 to with an A1 packet by the destination. Time T_2 is taken by message transmissions in the SR-ARQ mode.

The throughput expressions are different for the three types of transmissions, as previously mentioned in Section II-A.

1) DTs: In DTs, two nodes are involved in the transmissions and packets directly go from the source to the destination. Accordingly, we derive T_1 and T_2, respectively, as follows:

$$T_1 = t_{S1} + \text{IFS} + t_{A1} + \text{IFS} \tag{6}$$
$$T_2 = n \cdot (t_{S2} + \text{IFS}) \tag{7}$$

where IFS denotes interframe space between two consecutive packets [32], and t is the frame transmission time.

The BER for the calculation of the probability p_c in (3) is

$$\epsilon = \frac{1}{2}\left(1 - \sqrt{\frac{\gamma}{1+\gamma}}\right) \tag{8}$$

where γ is the receive signal-to-noise ratio (SNR). Let S, R, and D be the source, relay, and destination. Given γ_{SD}, γ_{SR}, and γ_{RD} for the links among them, we get ϵ_{SD}, ϵ_{SR}, and ϵ_{RD}, respectively. Then, we obtain the throughput of DTs

$$\begin{aligned}\eta_{dt} &= \frac{s_{\text{payload}}}{T_1 + T_2} \cdot p_c^{dt} \\ &= \frac{n\left(s_{\text{packet}} - s_h\left(\lceil \log_2 n \rceil + 1\right)\right)}{t_{S1} + t_{A1} + t_{S2} + (n+2)\cdot \text{IFS}} \cdot p_c^{dt}.\end{aligned} \tag{9}$$

2) MTs: MTs require another node to act as forwarder, and packets are transmitted via two hops. Then, we obtain the throughput for MTs

$$\begin{aligned}\eta_{mt} &= \frac{s_{\text{payload}}}{T_1 + T_2} \cdot \frac{1}{\frac{1}{p_c^{\text{SR}}} + \frac{1}{p_c^{\text{RD}}}} \\ &= \frac{n\left(s_{\text{packet}} - s_h\left(\lceil \log_2 n \rceil + 1\right)\right)}{t_{S1} + t_{A1} + t_{S2} + (n+2)\cdot IFS} \cdot \frac{1}{\frac{1}{p_c^{\text{SR}}} + \frac{1}{p_c^{\text{RD}}}}.\end{aligned} \tag{10}$$

3) Cooperative Transmissions: The destination requires both the signals from the source and the relay to decode the information in CCs. Usually, these two signals are transmitted in a separate consecutive time slots [2]. Consequently, we get the throughput of cooperative transmissions in DF mode as follows:

$$\begin{aligned}\eta_{ct} &= \frac{s_{\text{payload}}}{2(T_1 + T_2)} \cdot p_c^{\text{SRD}} \\ &= \frac{n\left(s_{\text{packet}} - s_h\left(\lceil \log_2 n \rceil + 1\right)\right)}{2\left(t_{S1+A1+S2} + (n+2)\cdot \text{IFS}\right)} \cdot p_c^{\text{SRD}}\end{aligned} \tag{11}$$

where p_c^{SRD} is the combined signal decoding correct rate at the destination [33]. The BER for p_c^{SRD} calculation in (4) is

$$\epsilon_{\text{SRD}} = P_{\text{out}}^{\text{SR}} \cdot \epsilon_{\text{SD}} + \left(1 - P_{\text{out}}^{\text{SR}}\right) \cdot \epsilon_{\text{div}} \tag{12}$$

where $P_{\text{out}}^{\text{SR}}$ is the outage probability for the link from source S to relay R and given by

$$P_{\text{out}}^{\text{SR}} = 1 - \exp\left\{-\frac{2^{2r}-1}{\gamma_{\text{SR}}}\right\} \tag{13}$$

and the BER for the combined signal decoding at D is

$$\epsilon_{\text{div}} = \frac{1}{2}\left(1 - \frac{1}{\gamma_{\text{RD}} - \gamma_{\text{SD}}}\left(\frac{\gamma_{\text{RD}}}{\sqrt{1+\frac{1}{\gamma_{\text{RD}}}}} - \frac{\gamma_{\text{SD}}}{\sqrt{1+\frac{1}{\gamma_{\text{SD}}}}}\right)\right). \tag{14}$$

We usually use the outage capacity [34], which supports a data rate in a related small outage probability ε, to present data rate r in (13), with an outage probability given by

$$P_{ct}^{\text{out}} = 1 + \frac{\frac{\gamma_{\text{SD}}}{\gamma_{\text{RD}}} u^{\frac{1}{\gamma_{\text{SD}}} + \frac{1}{\gamma_{\text{SR}}}} - u^{\frac{1}{\gamma_{\text{SR}}} + \frac{1}{\gamma_{\text{RD}}}}}{1 - \frac{\gamma_{\text{SD}}}{\gamma_{\text{RD}}}} \tag{15}$$

where $u = e^{-(2^{2r}-1)}$. Let $P_{ct}^{\text{out}} = \varepsilon$; we get u_ε from (15). Then

$$r = \frac{1}{2}\log_2\left(1 + \ln\frac{1}{u_\varepsilon}\right). \tag{16}$$

IV. Joint Authentication and Topology Control

In the sense that an authentication protocol is used to secure communications, the aforementioned throughput is the effective throughput with message integrity protection. In this section, we further discuss the JATC scheme, which is formulated as a stochastic optimization problem to maximize the effective throughput.

A. JATC Configuration

As discussed in the preceding section, the effect throughput depends on some coupled configurations. First, the three types of transmissions have distinct throughput. Even for MTs and cooperative transmissions, the selection of relays has significant impact on throughput since each relay has its own PHY-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 improving 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 but also increases packet error rate and decreases p_c in the throughput formulas. In this sense, we should have a considerate design on the packet size as well.

In addition, the Merkle Tree size n, i.e., the number of signed data blocks in a Merkle Tree is the vital parameter for the authentication protocol. We focus on its impact on throughput in this study. The increase of n also increases the overhead of transmissions. 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 increase 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. From the aforementioned discussion, the throughput is determined by a cross-layer configuration, which jointly considers topology control and authentication setting.

To integrate the relay selection and the choice of transmission manners, we use $\theta = (n, s_{\text{packet}}, k)$ as a configuration for a link. Given node 0 and one of its neighbors j, $\theta_j = (n_j, s_{\text{packet},j}, k_j)$ is the configuration for this neighbor link, and k_j denotes the selected relays, where $k_j \in K_j = \{0, 1, \ldots, |\mathcal{V}_N|, |\mathcal{V}_N|+1, 2|\mathcal{V}_N|\} - \{j, |\mathcal{V}_N|+j\}$. Case $k_j = 0$ corresponds to DTs. Otherwise, k_j is selected for the intermediate node for two-hop transmission if $j \le |\mathcal{V}_N|$, and $k_{j-|\mathcal{V}_N|}$ is selected as the relay node for CC if $j > |\mathcal{V}_N|$. The configuration of θ is actually a JATC setting, which combines the selections of the transmission manners and relays in notation k. When k is determined, it also determines the type of transmissions and the relays, i.e., the link is determined. Accordingly, we rewrite the throughput equations in the preceding section together in one equation as

$$\eta(\theta_j) = \begin{cases} \eta_{dt}, & k_j = 0 \\ \eta_{mt}, & 0 < k_j \le |\mathcal{V}_N| \\ \eta_{ct}, & |\mathcal{V}_N| < k_j \le 2|\mathcal{V}_N| \end{cases}. \tag{17}$$

It is expected to find out the optimal configuration θ_j^* for each neighbor link to maximize its throughput.

Interference also affects the network throughput from a network-wide perspective. Minimizing the interference is usually the objective of topology control [13]. According to the protocol interference model [35], the interference of a link can be 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 omni-antenna, we specify the link interference as the union of neighbor set of nodes involved in the transmissions. Given any node u, let $Cov(u)$ denote its neighbors in its radio coverage. The interference of link (u, v) is then $Cov(u) \cup Cov(v)$. A decreasing of interference will result in higher network capacity. The interference for different types of transmissions is separately obtained as follows:

$$I_{dt} = Cov(0) \cup Cov(j) \tag{18}$$

for DTs, and

$$I_{mt} = \max\{I_{0\to k_j}, I_{k_j \to j}\} \tag{19}$$

$$I_{ct} = Cov(0) \cup Cov(k_j) \cup Cov(j) \tag{20}$$

for MTs and cooperative transmissions, respectively. We rewrite them in one equation as follows:

$$I(\theta_j) = \begin{cases} I_{dt}(\theta_j), & \theta_j = 0 \\ I_{mt}(\theta_j), & 0 < \theta_j \le |\mathcal{V}_N| \\ I_{ct}(\theta_j), & n < \theta_j \le 2|\mathcal{V}_N|. \end{cases} \tag{21}$$

Under the protocol interference model, higher interference will result in lower throughput performance since the wireless channel is shared by neighboring nodes. Throughput $\eta(\theta_j)$ is decreased by its link interference. On the other hand, minimizing the interference solely is not sufficient for network throughput improvement [28]. To take the interference into account, the link throughput is rewritten as

$$f(\theta_j) = \frac{\eta(\theta_j)}{|I(\theta_j)|}. \tag{22}$$

Then, the optimal configuration for a link is obtained by

$$\theta_j^* = \arg\max_{\theta_j \in \Theta_j} f(\theta_j). \tag{23}$$

B. JATC Scheme

In general, distributed topology control schemes are desired to handle all the neighbor links, rather than a single link. As a result, we use another metric named aggregate throughput per node, which is also the network throughput capacity per node in [35], as the objective of link configurations. Then, JATC is formulated as

$$\theta^* = \arg\max \sum f(\theta_j). \tag{24}$$

The objective functions of both optimization problems of (23) and (24) require the knowledge of channel states (i.e., SNR). In practice, perfect knowledge of a dynamic channel is unavailable. We can only use the estimated version of the channel state [22]. In this sense, we only have the estimate of the objective function including some noise in practice. Therefore, the problems of (23) and (24) become discrete stochastic optimization problems.

MAC is usually designed to avoid concurrent transmissions in the vicinity of each other. The relay selection for each link

can be individually and independently conducted since it is the MAC function to avoid interference among different adjacent links. This fact follows the protocol interference model in [35]. In this sense, we get

$$\max \sum f(\theta_j) = \sum \max f(\theta_j). \tag{25}$$

Then, the problem (24) can be divided into several independent subproblems (23), which results in significant reduction of feasible solution space from $|\Theta_j|^{|\mathcal{V}_N|}$ to $|\Theta_j| \cdot |\mathcal{V}_N|$, where $|\Theta_j| = |\{n_j\}| \cdot |\{s_{\text{packet}}\}| \cdot |K_j|$. 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 e2e network connectivity is preserved via an HBH manner in (24) since it preserves all the neighbor links.

V. Discrete Stochastic Approximation Approach for Joint Authentication and Topology Control

JATC is of interest to determine the configuration of the topology that optimizes the expected aggregate throughput. Because the exact values of the objective function $f(\theta)$ are not analytically available due to the inclusion of some noise by the random variables (i.e., SNRs), its expected value under a given configuration has to be estimated via simulations, where the objective function f often takes the form

$$f(\theta) = E\left[f(i, \theta)\right]. \tag{26}$$

Intuitively, a brute-force approach can be used to solve the discrete stochastic problems (23) and (24). 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, i.e.,

$$\hat{f}_N(\theta_j) = \frac{1}{N} \sum_{i=1}^{N} f(i, \theta_j). \tag{27}$$

With (27), the global maximizer of the objective function is exhaustively searched by $\theta_j^* = \arg\max \hat{f}_N(\theta_j)$. Obviously, this heuristic approach requires a large number of objective evaluations and thus takes long optimization time and consumes a large amount of computation. The fact exists in that much optimization time is wasted in estimating the nonoptimal configuration points. In fact, what we are concerned is only the estimates of the optimal configuration.

A. Basic Algorithm for JATC

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 [23], [24], [26].

Let $\theta_j[i]$ denote the configuration at the ith iteration and $\boldsymbol{e}_{\theta_j[i]}$ be a unit $|\Theta_j| \times 1$ vector with a one for element $\theta_j[i]$ and zeros for other elements in the solution space Θ_j. Notation $\boldsymbol{\pi}[i] = [\pi[i,1], \ldots, \pi[i, |\Theta_j|]]$ 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 in each iteration. In fact, these empirical occupation probabilities stand for the visiting frequencies of the possible solutions. At the ith iteration, suppose that there have been $W[i, \theta_j[i]]$ iterations that $\theta_j[i]$ has visited so far, the decreasing step size $\mu[i] = 1/i$ updates the state probabilities as

$$\pi\left[i, \theta_j[i]\right] = \frac{W\left[i, \theta_j[i]\right]}{i}. \tag{28}$$

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 $i = 0$, randomly select an initial state of the algorithm $\theta_j[0] \in \Theta_j$, and set $\boldsymbol{\pi}[0] = \boldsymbol{e}_{\theta_j[0]}$. Initialize the 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.

Uniformly generate an alternative $\tilde{\theta}_j[i] \in \mathcal{N}_{\theta_j[i]}$, and evaluate $g(\tilde{\theta}_j[i])$.

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)

$$\boldsymbol{\pi}[i+1] = \boldsymbol{\pi}[i] + \mu[i+1]\left(\boldsymbol{e}_{\theta_j[i+1]} - \boldsymbol{\pi}[i]\right) \tag{29}$$

with a decreasing step $\mu[i] = 1/i$.

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 Θ_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 θ_j^* in the next section. Accordingly, after sufficient iterations, $\{\hat{\theta}_j[i]\}$ is selected as the output of the algorithm. The tracking feature of Algorithm 1 to

capture the dynamic topology changes will also be discussed in Section V-C.

B. Convergence Discussions

Although the discrete stochastic approximation approach is efficient, the convergence prerequisite needs to be proven when applying it to JATC. In this section, we will discuss the convergence property of JATC, as well as its convergence rate.

Theorem 1 (Global Convergence): JATC asymptotically converges to the global maximizer as the number of iterations goes to infinity.

Proof: Suppose that $s, t, w \in \Theta_j$ and $Y^{s\to t} = f(i,t) - f(i,s)$. Thus, $\Pr\{Y^{s\to t} > 0\}$ denotes the probability that the state of JATC moves from s to t. Let $E\{f(i,s)\} = \mu_s$ and $Var\{f(i,s)\} = \sigma_s^2$ for all $s \in \Theta_j$, and $\mu_s > \mu_t > 0$. Therefore, $E\{Y^{s\to t}\} = \mu_t - \mu_s$, and $Var\{Y^{s\to t}\} = \sigma_s^2 + \sigma_t^2$. According to [36], if the following conditions are satisfied, the algorithm suffices to converge, i.e.,

$$\Pr\{Y^{t\to s} > 0\} > \Pr\{Y^{s\to t} > 0\} \tag{30}$$

$$\Pr\{Y^{w\to s} > 0\} > \Pr\{Y^{w\to t} > 0\}. \tag{31}$$

As $\mu_s > \mu_t$, we know $E[Y^{s\to t}]/Var\{Y^{s\to t}\} > E[Y^{t\to s}]/Var\{Y^{t\to s}\}$. Then, condition (30) is satisfied. The same spirit can be applied to condition (31).

Commonly, we can have independent observations of the objective function value at a given point θ_j. In this sense, the estimate of (27) is unbiased. The algorithm always outputs the most visited state $\hat{\theta}_j$. This state also has a maximial evaluated value since only the larger estimated objective is accepted in Step 2. For unbiased estimates, we have $\hat{\theta}_j = \arg\max \sum f(\theta_j)/W[\theta_j]$, which converges to the optimum θ_j^*. ■

The assumption of independent estimates of objective values facilitates the rigorous proof of convergence and efficiency of the algorithm. However, this assumption can be relaxed to use correlated observations of the objective function [24].

Conditions (30) and (31) make $\{\theta_j[i]\}$ a homogeneous irreducible and aperiodic Markov chain. Given any $s, t \in \Theta_j$, let $\boldsymbol{P} = \{p_{s,t}\}$ be the transition probability matrix, where

$$\begin{aligned} p_{s,t} &= \Pr\{\theta_j[i+1] = t | \theta_j[i] = s\} \\ &= \frac{1}{|\Theta_j| - 1} \Pr\{Y^{s\to t} > 0\} \end{aligned} \tag{32}$$

for $s \neq t$, and

$$p_{s,s} = 1 - \sum_{t \in \mathcal{N}_s} p_{s,t}. \tag{33}$$

Let $s = \theta_j^*$, we obtain $p_{t,s} > p_{s,t}$ from (30). It means that the iterative states prefer going the optimal maximizer rather than moving out of the maximizer. Again, let $w = \hat{\theta}_j \neq \theta_j^*$ and $t \neq \theta_j^*$; condition (31) obtains $p_{w,s} > p_{w,t}$, which means that, if the current state does not stand in the optimal state, it will probably be attracted to that state rather than the nonoptimal states. In this sense, the optimal point θ_j^* will be visited more times than the other points on the probability. Consequently, the algorithm also converges from this point of view.

Regarding the convergence rate, we are interested in finding out at what speed the estimated objective value at the optimal solution converges to the optimal objective value.

Theorem 2 (Rate of Convergence): The convergence rate of JATC is $i^{-1/2}$, i.e., the variance of the estimated objective function asymptotically converges to a constant at a rate of $i^{-1/2}$ iteratively.

Proof: Let $N(\mu, \sigma^2)$ denote the normal distribution with mean μ and variance σ^2. In the communications system, it usually satisfies $-\infty < f(\theta) < \infty$ and $-\infty < \sigma^2(\theta) < \infty$. According to Theorem 4.1 and Remark 4.5 in [23], if Θ_j is finite, we have

$$\sqrt{i}\left(\frac{\sum f(\theta_j)}{W[\theta_j]} - \max_{\theta_j \in \Theta_j} f(\theta_j)\right) \Rightarrow \min Z(\theta_j) \text{ as } i \to \infty \tag{34}$$

where $Z(\theta_j) \sim N(0, \sigma^2(\theta_j)/c(\theta_j))$, $c(\theta_j)$ is a constant, and symbol $\Rightarrow$ denotes weak convergence. Thus, the estimated objective function $\sum f(\theta_j)/W[\theta_j] - \max_{\theta_j \in \Theta_j} f(\theta_j)$ almost surely converges to zero. As we know, $\hat{\theta}_j = \arg\max(\sum f(\theta_j)/W[\theta_j])$ for unbiased estimates. From the law of large numbers, $\hat{\theta}_j$ almost surely converges to θ_j^*, which also confirms Theory 1. The asymptotic variance constant in $Z(\theta_j)$ indicates that the algorithm converges at a rate with respect to iteration times i, i.e., $i^{-1/2}$. ■

The superlinear convergence rate makes the algorithm approach the optimal point in a short time.

C. Adaptive Reconfiguration for Dynamic Topology

The step size μ in (29) is the parameter that controls the speed of convergence, the stable state, and the tracking behavior of Algorithm 1. The algorithm with a small μ opts to stay in one state, so that it ensures low misadjustments 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, although a large μ makes fast convergence and good tracking capability, it may not track the optimal state due to the high misadjustments. 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 [37]. We employ a gradient descent least-mean-square-like algorithm to reduce the squared estimation error in each iteration.

The error is defined as

$$\boldsymbol{\epsilon}^{\mu}[i] = \boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i]. \tag{35}$$

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

$$\mu[i+1] = \mu[i] - \frac{\rho}{2}\frac{\partial \phi(\boldsymbol{\epsilon}[i])}{\partial \mu[i]} \tag{36}$$

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

$$\frac{\partial \phi(\boldsymbol{\epsilon}[i])}{\partial \mu[i]} = -2(\boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i])^T \boldsymbol{J}^{\mu}[i] \tag{37}$$

where $\boldsymbol{J}^{\mu}[i] = (\partial/\partial\mu[i])\boldsymbol{\pi}^{\mu}[i]$. Differentiating (29) with respect to μ, we obtain

$$\boldsymbol{J}^{\mu}[i+1] = \boldsymbol{J}^{\mu}[i] - \mu \boldsymbol{J}^{\mu}[i] + (\boldsymbol{e}[i+1] - \boldsymbol{\pi}^{\mu}[i])\,. \tag{38}$$

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

Substitute Step 3 of Algorithm 1 by

Step 3' (Update empirical state occupation probability)

$$\boldsymbol{\epsilon}[i] = \boldsymbol{e}[i+1] - \boldsymbol{\pi}[i]$$

$$\boldsymbol{\pi}[i+1] = \boldsymbol{\pi}[i] + \mu[i]\boldsymbol{\epsilon}[i]$$

$$\mu[i+1] = \mu[i] + \rho\boldsymbol{\epsilon}[i]^T \boldsymbol{J}^{\mu}[i]$$

$$\boldsymbol{J}[i+1] = (1-\mu[i])\boldsymbol{J}[i] + \boldsymbol{\epsilon}[i], \quad \boldsymbol{J}[0] = 0$$

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.

VI. Simulation Results and Discussions

In the simulations, we set up a scenario with 30 nodes randomly deployed in an area of 800×800 m^2, as shown in Fig. 3. The maximum transmission range of a mobile node is 300 m, and the wireless channel follows a slow flat-fading Raleigh distribution, which can be estimated by the training preamble in practice. A 20-B hash is used for the authentication protocol. The following packet sizes are considered, i.e., $s_{\text{packet}} = \{128, 256, 512, 1024\}$ B. The resultant topology is plotted in Fig. 4. As shown in the resultant topology, some links are working in cooperative transmission manner (in dash lines), other than DTs and MTs (both in solid lines). Examples of cooperative transmissions and MTs are also shown in the figure. We consider the performance of JATC, which configures the size of the Merkle Tree, packet size, appropriate single-relay node, and the selection of the transmission mode, maximizing the system aggregate throughput using (24) as the objective function.

The intrinsic possibility of JATC exists in that the effective throughput discussed in Section III has a convex relationship with the configuration θ. A study is carried out to verify the effective throughput model of JATC. It is shown in Fig. 5 that the effective throughput changes with the number of the signed packets per S1/A1 exchange and the packet sizes. The throughput increases as the packet size increases. The reason is that

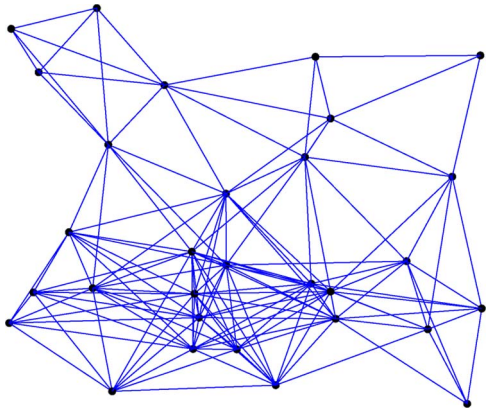


Fig. 3. Original topology.

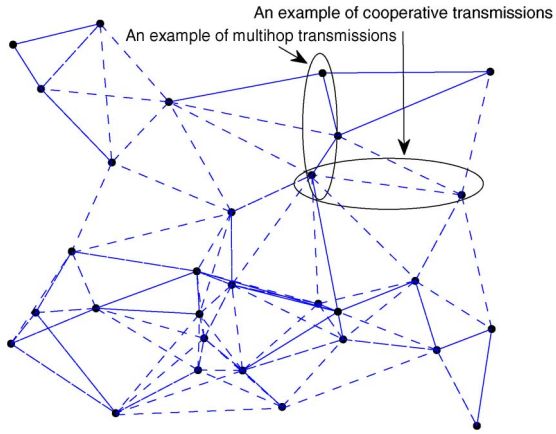


Fig. 4. Resultant topology generated by JATC. (Solid line) Traditional DTs and MTs. (Dashed line) Links involved in CCs.

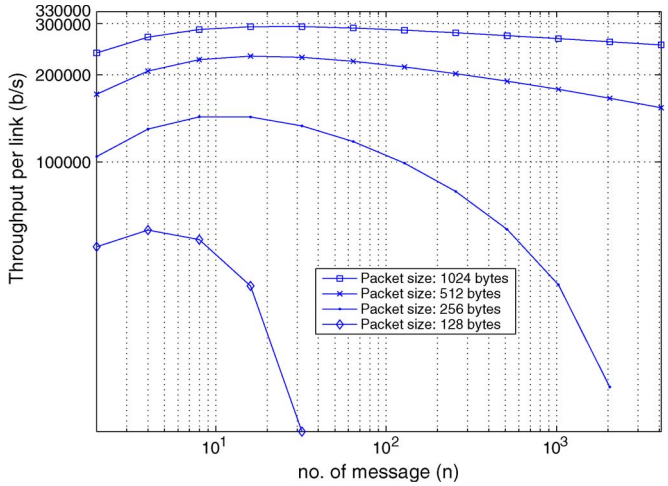


Fig. 5. Throughput changes with signed packets per S1 and the packet sizes. This convex relationship necessitates the joint optimization by JATC.

the proportion of authentication information carried in a packet is decreased due to the increase in the packet size, whereas the amount of authentication information depends on the size of the Merkle Tree, i.e., n. Note that the augmentation in throughput gradually shrinks as the increase in the packet size. We cannot use an arbitrarily large packet size since a large packet may experience packet error or packet loss. Normally, there should

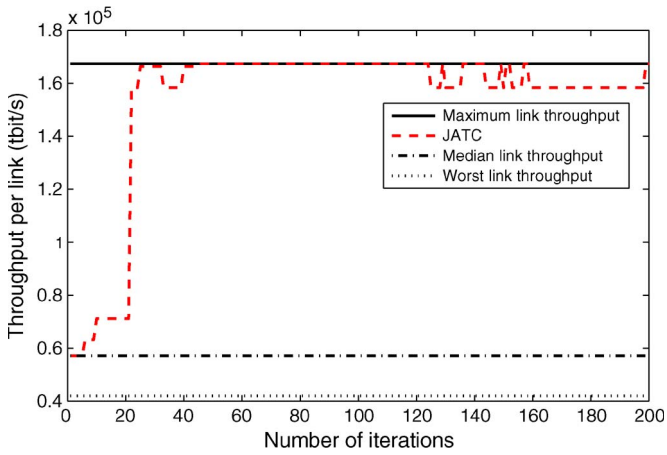


Fig. 6. Single run to optimize link configuration and the link throughput of the chosen configuration by Algorithm 1 versus iteration number n.

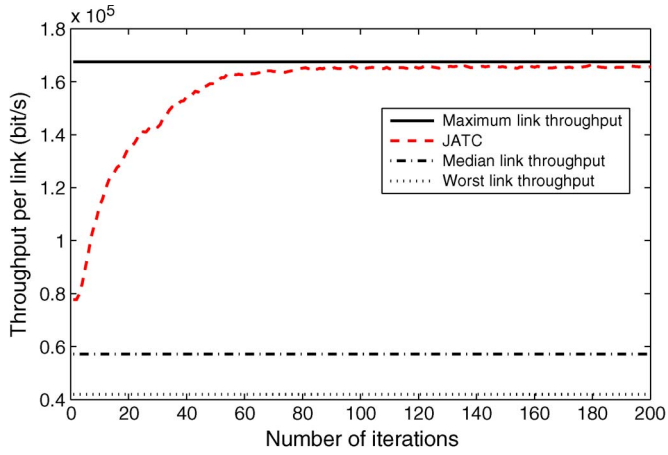


Fig. 7. Average of 200 runs to optimize link configuration and average link throughput of the chosen configuration by Algorithm 1 versus iteration number n.

be a tradeoff between packet size and packet error rate (PER). With an appropriate transmission mode (e.g., CCs), Fig. 5 shows that the overhead of the authentication protocol has more impact on throughput performance than PER. Again, a packet with a large size consumes more time in the transmission, and it will probably interfere with other transmissions, thus contrarily reducing the throughput. This kind of interference has been considered in JATC when constructing network topology. It is also clearly shown that there exists an optimal n value to maximize the throughput. The result in Fig. 5 necessitates the joint consideration in a link configuration $\theta = (n, s_{\text{packet}}, k)$.

A major component in the link configuration is the relay node selection, which takes the interference into account, whereas the interference affects the feasible link throughput in practice. Another simulation is conducted to study the performance of JATC for a link configuration. The initial link configuration for JATC is randomly selected. Fig. 6 shows the result of a single run of JATC, and Fig. 7 shows the average of 200 runs. They demonstrate the tracking feature and the convergence of JATC when the channel state cannot be known in advance. For comparison, the maximum, median, and worst throughput, which are computed according to the known channel state, are shown in the same figure. As shown in Fig. 6, JATC captures the optimum in a short time (around 30 iteration steps) due to the adoption of the discrete stochastic approximation approach. In this sense, it gives JATC a significant property of online computing. The convergence property and the convergence rate of the algorithm are also confirmed in Fig. 7 to support the mathematical proofs of Theorem 1 and Theorem 2.

The ultimate objective of JATC is to optimize the joint authentication and topology configuration to maximize the per-node aggregate throughput capacity, i.e., the sum of all the throughput of links associated with the node. Fig. 8 shows that the aggregate throughput in each iteration iteratively approaches the global optimum. The average result of 200 runs in Fig. 9 indicates that the algorithm asymptotically converges to the global optimum after sufficient iteration times. These simulation results make it sense to apply the discrete stochastic approximation approach to JATC. Comparing Figs. 7 and 9, we find that the algorithm has almost the same convergence rate

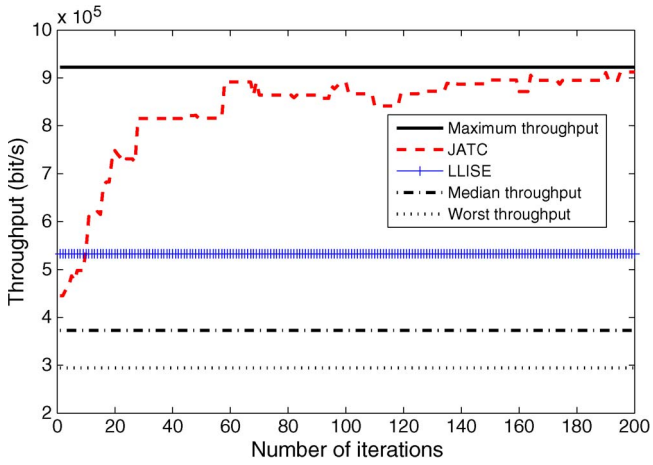


Fig. 8. Single run to optimize the joint authentication and topology configuration for aggregate throughput improvement and system aggregate throughput of the chosen configuration by Algorithm 1 versus iteration number n.

for the link configuration and the topology configuration. This result is attributed to the decomposition of (24) into several (23). We also compare JATC with the LLISE topology control scheme [13]. Similar to JATC, LLISE is executed for each link in a distributed way. It computes the minimum interference path for each link and preserves all the edges on that path in the resulting topology. LLISE can improve network capacity if the interference is minimized. Evidently, JATC has an advantage over LLISE in achieving the aggregate throughput. This is because only the MT mode without relay assistant is considered in LLISE. Each transmission mode discussed in Section III has its own advantage, which depends on the channel states of links among the source, relay, and destination. JATC adaptively chooses the best transmission mode according to the estimated channel states and tunes the configuration of the authentication protocol (i.e., the packet size and the Merkle Tree size) to reach a higher throughput. Note that the throughput with LLISE is fixed once the relay nodes are selected since it assumes a known channel state.

We also investigate the aggregate throughput and the setting of Merkle Tree size in the authentication protocol with different

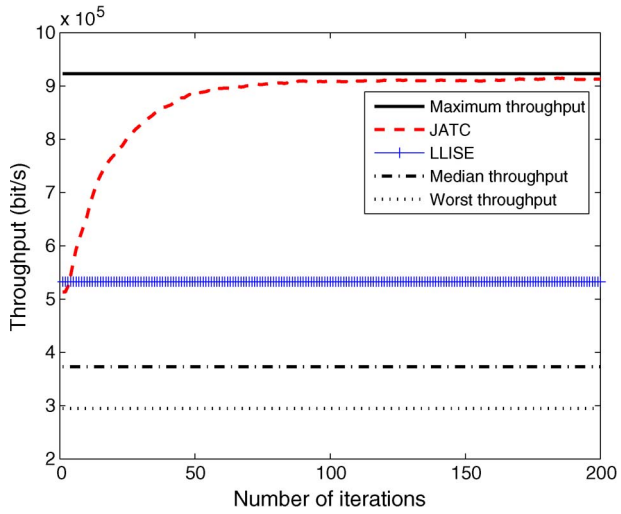


Fig. 9. Average of 200 runs to optimize the joint authentication and topology configuration and average system aggregate throughput of the chosen configuration by Algorithm 1 versus iteration number n.

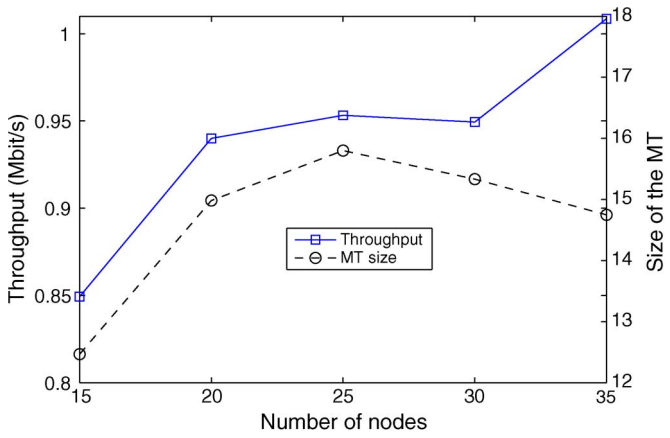


Fig. 10. Aggregate throughput and the size of Merkle tree in the authentication protocol versus different numbers of nodes.

numbers of nodes in the network, which stand for the network throughput and security intensity, respectively. The result in Fig. 10 shows the aggregate throughput is increased in the dense network. This is attributed to the fact that there exist more opportunities for CCs in a dense network. Meanwhile, the size of Merkle Tree is adjusted according to the network environment and the available resources to achieve higher throughput.

A beneficial merit of JATC is that it can track the dynamic topology where nodes are moving. To investigate the dynamic tracking ability of JATC, we set nodes to move under a random-walk-based mobility model, where nodes uniformly move at a direction in [0, 360] degree and a speed in [2, 100] m/s. The mobile node moves to its destination by randomly choosing a speed and a direction. New velocity is randomly generated on arriving the destination. If the node reaches the simulation topology boundary, it bounces off with an opposite direction. It is shown in Fig. 11 that, although the position changes of nodes lead to a degradation of aggregate throughput, JATC with an adaptive step size can reconfigure the joint authentication and topology configuration to track the changes within a short delay. In a mobile environment, constant reconfigurations are

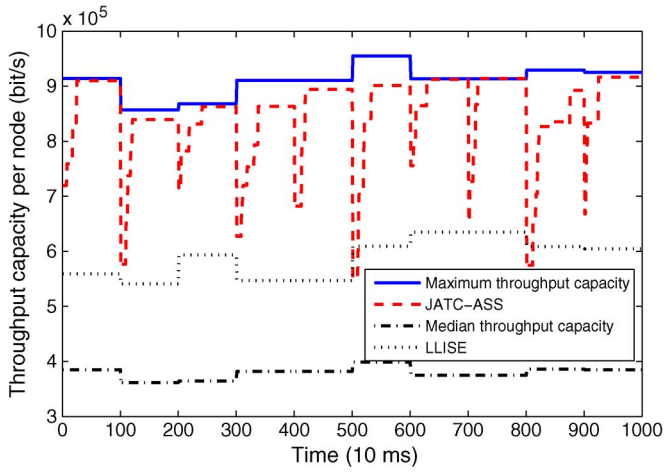


Fig. 11. Performance of JATC to track the dynamic changing topology. Algorithm 2 can capture the dynamic changing in a mobile environment.

desired since the states of the channel and interference will dramatically change from time to time. The dynamic tracking feature of JATC is in accordance with the self-configuration of MANETs.

VII. Conclusion and Future Work

Since security and throughput are two major concerns of MANETs, we have considered them together in this paper for CC-MANETs. With the analysis under an authentication protocol, we have developed a JATC scheme, which tunes the parameters of up-layer authentication protocol and PHY-layer transmission settings to increase resource utilization and throughput capacity of the network. In addition, a discrete stochastic approximation approach has been employed in JATC to deal with the imperfect channel knowledge and the dynamically changing topology. Simulation results have been presented to show that JATC works well in MANETs.

Acknowledgment

The authors would like to thank the editor and the reviewers for their detailed reviews and constructive comments, which have helped to improve the quality of this paper.

References

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

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

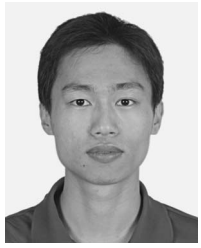
[3] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.

[4] M. Gouda, E. Elnozahy, C. Huang, and T. McGuire, "Hop integrity in computer networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 3, pp. 308–319, Jun. 2002.

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

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

[7] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, Jul. 2002.
[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38–47, Feb. 2004.
[9] N. Garg and R. Mahapatra, "MANET security issues," *Int. J. Comput. Sci. Netw. Security*, vol. 9, no. 8, p. 241, Aug. 2009.
[10] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of security in large-scale wireless ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 319–332, Apr. 2011.
[11] L. Hu, "A novel topology control for multihop packet radio networks," in *Proc. IEEE INFOCOM*, Bal Harbour, FL, 1991, pp. 1084–1093.
[12] Q. Guan, Q. Ding, and S. Jiang, "A minimum energy path topology control algorithm for wireless multihop networks," in *Proc. IWCMC*, Leipzig, Germany, Jun. 2009, pp. 557–561.
[13] M. Burkhart, P. von Rickenbach, R. Wattenhofer, and A. Zollinger, "Does topology control reduce interference?" in *Proc. 5th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Tokyo, Japan, May 2004, pp. 9–19.
[14] P. Von Rickenbach, R. Wattenhofer, and A. Zollinger, "Algorithmic models of interference in wireless ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 172–185, Feb. 2009.
[15] Y. Gao, J. Hou, and H. Nguyen, "Topology control for maintaining network connectivity and maximizing network capacity under the physical model," in *Proc. IEEE INFOCOM*, Phoenix, AZ, 2008, pp. 1013–1021.
[16] M. Ismail and M. Sanavullah, "Security topology in wireless sensor networks with routing optimisation," in *Proc. 4th Int. Conf. Wireless Commun. Sensor Netw.*, Allahabad, India, 2008, pp. 7–15.
[17] P. Galiotos, "Security-Aware topology control for wireless Ad-Hoc networks," in *Proc. IEEE GLOBECOM*, New Orleans, LA, 2008, pp. 1–6.
[18] C. Hsueh, Y. Li, C. Wen, and Y. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," *Sensors*, vol. 10, no. 2, pp. 1251–1278, Feb. 2010.
[19] B. Kannhavong, H. Nakayama, and A. Jamalipour, "SA-OLSR: Security aware optimized link state routing for mobile ad hoc networks," in *Proc. IEEE ICC*, Beijing, China, May 2008, pp. 1464–1468.
[20] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 68–71, Feb. 2004.
[21] H. Meyr, M. Moeneclaey, and S. Fechtel, *Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing*. New York: Wiley, 1997.
[22] L. Tong, B. Sadler, and M. Dong, "Pilot-assisted wireless transmissions: General model, design criteria, and signal processing," *IEEE Signal Process. Mag.*, vol. 21, no. 6, pp. 12–25, Nov. 2004.
[23] S. Andradottir, "Accelerating the convergence of random search methods for discrete stochastic optimization," *ACM Trans. Model. Comput. Simul.*, vol. 9, no. 4, pp. 349–380, Oct. 1999.
[24] I. Berenguer, X. Wang, and V. Krishnamurthy, "Adaptive MIMO antenna selection via discrete stochastic optimization," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4315–4329, Nov. 2005.
[25] V. Krishnamurthy and S. Chung, "Large-scale dynamical models and estimation for permeation in biological membrane ion channels," *Proc. IEEE*, vol. 95, no. 5, pp. 853–880, May 2007.
[26] H. Kushner, "Stochastic approximation: A survey," *Wiley Interdiscip. Rev., Comput. Statist.*, vol. 2, no. 1, pp. 87–96, 2010.
[27] E. Lloyd, R. Liu, M. Marathe, R. Ramanathan, and S. Ravi, "Algorithmic aspects of topology control problems for ad hoc networks," *Mobile Netw. Appl.*, vol. 10, no. 1/2, pp. 19–34, Feb. 2005.
[28] Q. Guan, S. Jiang, Q.-L. Ding, and G. Wei, "Impact of topology control on capacity of wireless ad hoc networks," in *Proc. IEEE ICCS*, Guangzhou, China, Nov. 2008, pp. 588–592.
[29] R. Merkle, "A certified digital signature," in *Proc. CRYPTO*, 1989, pp. 218–238.
[30] L. Lamport, "Password authentication with insecure communication," *ACM Commun.*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[31] 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, Dec. 1984.
[32] P. Liu, Z. Tao, S. Marauamam, T. Korakis, and S. Panwar, "CoopMAC: A cooperative MAC for wireless LANs," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 340–354, Feb. 2007.
[33] P. Herhold, E. Zimmermann, and G. Fettweis, "A simple cooperative extension to wireless relaying," in *Proc. Int. Zurich Semin. Commun.*, Zurich, Switzerland, Aug. 2004.
[34] K. Woradit, T. Quek, W. Suwansantisuk, M. Win, L. Wuttisittikulkij, and H. Wymeersch, "Outage behavior of selective relaying schemes," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3890–3895, Aug. 2009.
[35] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.
[36] S. Andradottir, "A global search method for discrete stochastic optimization," *SIAM J. Optim.*, vol. 6, no. 2, pp. 513–530, May 1996.
[37] V. Mathews and Z. Xie, "A stochastic gradient adaptive filter with gradient adaptive step size," *IEEE Trans. Signal Process.*, vol. 41, no. 6, pp. 2075–2087, Jun. 1993.



Quansheng Guan (S'09–M'11) received the B. Eng. degree in electronic engineering from Nanjing University of Post and Telecommunications, Jiangsu, China, in 2006 and the Ph.D. degree from South China University of Technology, Guangzhou, China, in 2011.

From September 2009 to September 2010, he was a visiting Ph.D. student with the University of British Columbia, Vancouver, BC, Canada, and Carleton University, Ottawa, ON, Canada, where he was supported by the China Scholarship Council. He is currently a faculty member with the School of Electronic and Information Engineering, South China University of Technology. His research areas include topology control, routing and cooperative communications for mobile ad hoc networks, and cognitive networks.

Dr. Guan has served on the Technical Program Committees of several international conferences, including the IEEE Vehicular Technology Conference 2012 (Spring and Fall), Globecom 2011, INFOCOM-GCN 2011, etc. He has served on the organization committees of the IEEE ICCS 2008 and IEEE INFOCOM-CWCN 2010.

F. Richard Yu (S'00–M'04–SM'08) received the Ph.D. degree in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 2003.

From 2002 to 2004, he was with Ericsson (Lund, Sweden), where he worked on research and development of Third-Generation cellular networks. From 2005 to 2006, he was with a start-up company in California, where he worked on research and development in the areas of advanced wireless communication technologies and new standards. In 2007, he joined Carleton School of Information Technology and the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where he is currently an Assistant Professor. He serves on the Editorial Boards of several journals, including *ACM/Springer Wireless Networks*, *EURASIP Journal on Wireless Communications Networking*, *Ad Hoc & Sensor Wireless Networks*, the *Wiley Journal on Security and Communication Networks*, and the *International Journal of Wireless Communications and Networking*. His research interests include cross-layer design, security, and quality-of-service provisioning in wireless networks.

Dr. Yu serves on the Editorial Board of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He has served on the Technical Program Committee (TPC) of numerous conferences, as a TPC Co-Chair of IEEE VTC2012S, Globecom11, INFOCOM-GCN2011, INFOCOM-CWCN'2010, IEEE IWCMC'2009, VTC'2008F, and WiN-ITS'2007; Publication Chair of ICST QShine 2010; and a Co-Chair of ICUMT-CWCN'2009. He received the Ontario Early Researcher Award in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at the IEEE/IFIP TrustCom 2009 and the International Conference on Networking in 2005.

Shengming Jiang (A'96–M'00–SM'07) received the B.Eng. degree from Shanghai Maritime Institute, Shanghai, China, in 1988, the DEA degree from the University of Paris VI, Paris, France, in 1992, and the Dr. degrees from the University of Versailles Saint-Quentin-En-Yvelines, Versailles, France, in 1995.

From 1988 to1990, he was with Nanjing Petrol Transportation Company, Nanjing, China. From February 1995 to August 1997, he was a Research Associate with the Department of Electrical and Electronic Engineering and the Department of Computer Science, The Hong Kong University of Science and Technology, Kowloon, Hong Kong. He was a Member of Technical Staff with the Centre for Wireless Communications, National University of Singapore, from September 1997 to July 2000 and a Senior Member of Technical Staff and the leader of the network strategic group from July 2001 to March 2003. From October 2003 to September 2004, he was an Associate Lead Scientist and the leader of End-to-End Quality-of-Service Laboratory, Institute for Infocomm Research, Singapore. From July 2007 to August 2009, he was a Principal Lecturer with the Faculty of Advanced Technology, University of Glamorgan, Pontypridd, U.K. He is currently a Professor with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. His research interests include communication networks.

Victor C. M. Leung (S'75–M'89–SM'97–F'03) received the B.A.Sc. (Hons.) and the Ph.D. degrees in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 1977 and 1981, respectively.

From 1981 to 1987, he was a Senior Member of Technical Staff with MPR Teltech Ltd., Burnaby, BC, where he contributed to the design and analysis of satellite communication networks. In 1988, he was a Lecturer with the Department of Electronics, Chinese University of Hong Kong, Shatin, Hong Kong. In 1989, he returned to UBC as a faculty member, where he is currently a Professor and the inaugural holder of the TELUS Mobility Research Chair in Advanced Telecommunications Engineering, Department of Electrical and Computer Engineering. He is a member of the Institute for Computing, Information, and Cognitive Systems, UBC. He also holds Guest/Adjunct Professor appointments at Jilin University, Beijing Jiaotong University, South China University of Technology, Hong Kong Polytechnic University, and Beijing University of Posts and Telecommunications in China. He has made substantial contributions to the design and evaluations of wireless networks and mobile systems over the past 30 years and has authored/coauthored more than 500 technical papers in international journals and conference proceedings. He has served on the Editorial Boards of *Computer Communications*, the *International Journal of Sensor Networks*, the *Journal of Communications and Networks*, and the *International Journal of Communication Networks and Distributed Systems*.

Dr. Leung is a Fellow of the Canadian Academy of Engineering and the Engineering Institute of Canada and a voting member of the Association for Computing Machinery. He is a registered member of the Association of Professional Engineers and Geoscientists of British Columbia (APEGBC). He has served on the Editorial Boards of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE TRANSACTIONS ON COMPUTERS. He has guest-edited several special journal issues and served on the technical program committee of numerous international conferences. He is a Distinguished Lecturer of the IEEE Communications Society. He was the Technical Program Committee (TPC) Chair of the wireless networks and cognitive radio track of IEEE VTC-Fall 2008 and the TPC Vice-Chair of IEEE WCNC in 2005. He was the General Chair of QShine 2007 and AdhocNets 2010, as well as a General Co-Chair of ACM MSWiM 2005, IEEE EUC 2009, IEEE MobiWorld 2010, IEEE CWCN 2010, IEEE ASIT 2010, and BodyNets 2010. He is a General Co-Chair of IEEE Mobiworld 2011, IEEE GCN 2011, CSA 2011, and ChinaCom 2011. During his studies, he received the APEGBC Gold Medal as the head of the graduating class in the Faculty of Applied Science and a Natural Sciences and Engineering Research Council Postgraduate Scholarship. He and his coauthors have received several Best Paper Awards.