ISSN:0975-9646

Topology Control and Hop-by-hop Authentication in MANETs with Cooperative Communications

Srichandradeep. C[1], Dr. B. Raveendra Babu[2]

[1]*M.Tech Student (SE),*
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

[2]*Professor and Head of the Department (CSE),*
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

Abstract— **Cooperative communications can significantly enhance transmission reliability and bandwidth efficiency in wireless networks. However, the impact of cooperative communications on network-level upper layer issues, such as topology control, routing and network capacity, is largely ignored. At the same time, security is an important issue in MANETs and existing security schemes have significant impact on throughput. In this paper, a security cum topology control scheme, called COCO+ALPHA scheme to improve the network capacity as well as to provide the security in mobile ad hoc networks (MANETs) with cooperative communications is presented. Both upper layer network capacity and physical layer relay selections are considered in the proposed scheme.**

Keywords— **Cooperative communication, security, network capacity, MANETs, topology control.**

I. Introduction

The demand for speed in wireless networks is continuously increasing. Recently, cooperative wireless communication has gained tremendous interest as an untapped means for improving the performance of information transmission operating over the ever-challenging wireless medium. Cooperative communication has emerged as a new dimension of diversity to emulate the strategies designed for multiple antenna systems, since a wireless mobile device may not be able to support multiple transmit antennas due to size, cost, or hardware limitations [1]. By exploiting the broadcast nature of the wireless channel, cooperative communication allows single-antenna radios to share their antennas to form a virtual antenna array, and offers significant performance enhancements. This promising technique has been considered in the IEEE 802.16j standard, and is expected to be integrated into Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) multi-hop cellular networks [2].

Although extensive research has been done on cooperative communications, most existing works are focused on physical layer issues, such as decreasing outage probability and increasing outage capacity [3], which are only link-wide metrics. However, from the network point of view, it may not be sufficient for the overall network performance, such as the whole network capacity. Therefore, many upper layer aspects of cooperative communication merit further research, e.g., the impacts on network structure and topology control, especially in mobile ad hoc networks (MANETs). Indeed, most current studies on MANETs attempt to create, adapt, and manage a complex network based on traditional simple point-to-point non-cooperative wireless links.

Security is the other concern and bottleneck for widely deployed wireless applications due to the vulnerable open shared access medium and the stringent resource constraints [4]. 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 [5], [6]. 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.

In wireless multi-hop networks, a communication between end-hosts may involve a large number of forwarding nodes, which may lead to resource exhaustion attacks (e.g. targeting energy, bandwidth, and CPU resources) on any element of a communication path. To limit the impact of this attack, it is vital to efficiently verify the authenticity of a message and its sender’s identity to detect and drop forged or unauthorized messages early. Such a facility also allows on-path entities to authenticate data, e.g., for control and signalling data between end-hosts and forwarding nodes such as location updates from mobile devices. Together, forgery detection and data extraction form the basis for more complex services, such as rate and resource allocation within the network controlled by end-host but enforced by intermediate nodes.

Conventionally, light-weight end-to-end integrity protection and encryption are based on shared secrets and symmetric ciphers. However, these mechanisms cannot enable integrity checking on a hop-by-hop basis because forwarding nodes typically have no access to the shared secrets. Therefore, they cannot use these mechanisms to verify the authenticity of data and the identity of the communicating peers. Simply sharing the symmetric keys with forwarding nodes is not possible because malicious relays could use these keys to manipulate data in transit. Hence, packet manipulation and unauthorized transmission are only detected by the destination host and cannot be filtered by intermediate nodes. While public-key cryptography does not suffer from this limitation, it is computationally more complex than the symmetric approaches. This overhead and the resulting impact on energy consumption and communication latency are prohibitive for per-packet verification in the vast majority of multi-hop scenarios.

Hash chains represent a practical basis for solving this problem as they are computationally efficient and are successfully employed in different specialized protocols, such as TESLA [7], CSA [8], ZCK [9], the Guy Fawkes Protocol [10], and WIMP [11]. However, existing solutions either lack on-path data verification or are too inefficient in wireless multi-hop networks for both infrequent low-volume and high-volume transfers. Moreover, they are designed for tightly restricted use- cases, making it difficult to apply them in a broader scope.

In this paper, considering both upper layer network capacity and physical layer cooperative communications, the topology control issues in MANETs with cooperative communications are studied. A Capacity-Optimized Cooperative (COCO) topology control scheme [12, 13] to improve the network capacity in MANETs by jointly optimizing transmission mode selection, relay node selection, and interference control in MANETs with cooperative communications is implemented. Then the COCO topology control scheme with an Adaptive and Lightweight Protocol for Hop-by-hop Authentication (ALPHA) [14] to provide hop-by-hop authentication are combined. Through simulations, it can be shown that physical layer cooperative communications have significant impacts on the network capacity, and the proposed COCO+ALPHA scheme can substantially improve the network capacity in MANETs with cooperative communications and ensure hop-by-hop authentication and message integrity in the network.

The remainder of the paper is structured as follows. Cooperative communications and the topology control problem in MANETs are introduced. Network capacity, authentication schemes and the proposed COCO+ALPHA scheme are presented. The implementation results and discussions are listed and are concluded.

II. Mobile Ad hoc Networks with Cooperative Communications

In this section, the concept of cooperative communications is introduced. Then the topology control problem in MANETs with cooperative communications is presented.

A. Cooperative Communications

Cooperative communication typically refers to a system where users share and coordinate their resources to enhance the information transmission quality. It is a generalization of the relay communication, in which multiple sources also serve as relays for each other. Early study of relaying problems appears in the information theory community to enhance communication between the source and destination [15]. Recent tremendous interests in cooperative communications are due to the increased understanding of the benefits of multiple antenna systems [1]. Although multiple-input multiple-output (MIMO) systems have been widely acknowledged, it is difficult for some wireless mobile devices to support multiple antennas due to the size and cost constraints. Recent studies show that cooperative communications allow single antenna devices to work together to exploit the spatial diversity and reap the benefits of MIMO systems such as resistance to fading, high throughput, low transmitted power, and resilient networks [1].

In a simple cooperative wireless network model with two hops, there is a source, a destination, and several relay nodes. The basic idea of cooperative relaying is that some nodes, which overheard the information transmitted from the source node, relay it to the destination node instead of treating it as interference. Since the destination node receives multiple independently faded copies of the transmitted information from the source node and relay nodes, cooperative diversity is achieved. Relaying could be implemented using two common strategies,

- Amplify-and-Forward
- Decode-and-Forward.

In amplify-and-forward, the relay nodes simply boost the energy of the signal received from the sender and retransmit it to the receiver. In decode-and-forward, the relay nodes will perform physical-layer decoding and then forward the decoding result to the destinations. If multiple nodes are available for cooperation, their antennas can employ a space-time code in transmitting the relay signals. It is shown that cooperation at the physical layer can achieve full levels of diversity similar to a MIMO system, and hence can reduce the interference and increase the connectivity of wireless networks.

Most existing works about cooperative communications are focused on physical layer issues, such as decreasing outage probability and increasing outage capacity, which are only link-wide metrics. However, from the network's point of view, it may not be sufficient for the overall network performance, such as the whole network capacity. Therefore, many upper layer network-wide metrics should be carefully studied, e.g., the impacts on network structure and topology control. Cooperation offers a number of advantages in flexibility over traditional wireless networks that go beyond simply providing a more reliable physical layer link. Since cooperation is essentially a network solution, the traditional link abstraction used for networking design may not be valid or appropriate. From the perspective of a network, cooperation can benefit not only the physical layer, but the whole network in many different aspects.

With physical layer cooperative communications, there are three transmission manners in MANETs: direct transmissions (Fig. 1a), multi hop transmissions (Fig. 1b) and cooperative transmissions (Fig. 1c). Direct transmissions and multi-hop transmissions can be regarded as special types of cooperative transmissions. A direct transmission utilizes no relays while a multi-hop transmission does not combine signals at the destination. In Fig. 1c, the cooperative channel is a virtual multiple-input single-output (MISO) channel, where spatially distributed nodes are coordinated to form a virtual antenna to emulate multi-antenna transceivers.

B. Topology Control

The network topology in a MANET is changing dynamically due to user mobility, traffic, node batteries, and so on. Meanwhile, the topology in a MANET is controllable by adjusting some parameters such as the transmission power, channel assignment, etc. In general, topology control is such a scheme to determine where to deploy links and how the links work in wireless networks to form a network topology which will optimize the energy consumption, the capacity of the network, or end-to-end routing performance. Topology control is originally developed for wireless sensor networks (WSNs), MANETs, and wireless mesh networks to reduce energy consumption and interference. It usually results in a simpler network topology with small node degree and short transmission radius, which will have high-quality links and less contention in medium access control (MAC) layer. Spatial/spectrum reuse will become possible due to the smaller radio coverage. Other properties like symmetry and planarity are expected to obtain in the resultant topology. Symmetry can facilitate wireless communication and two-way handshake schemes for link acknowledgment while planarity increases the possibility for parallel transmissions and space reuse.

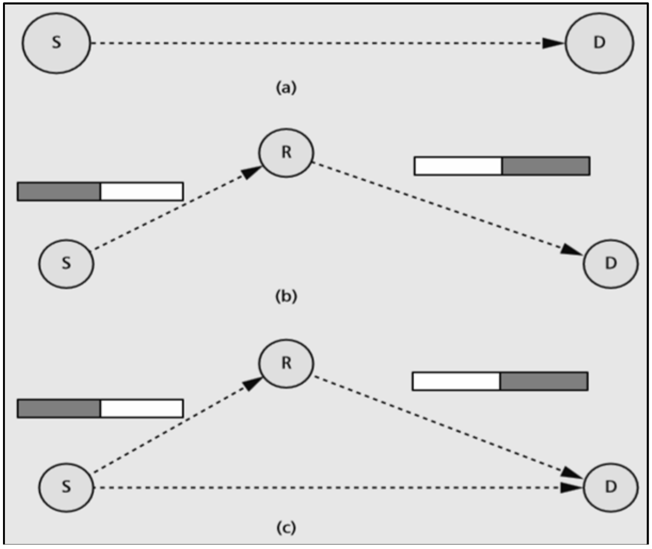

Fig.1. Three transmission protocols. (a) Direct transmissions via a point-to-point conventional link. (b) Multi-hop transmissions via a two-hop manner occupying two time slots. (c) Cooperative transmissions via a cooperative diversity occupying two consecutive slots. The destination combines the two signals from the source and the relay to decode the information.

Power control and channel control issues are coupled with topology control in MANETs while they are treated separately traditionally. Although a mobile node can sense the available channel, it lacks the scope to make network wide decisions. It therefore makes more sense to conduct power control and channel control via the topological viewpoint. The goal of topology control is then to set up interference-free connections to minimize the maximum transmission power and the number of required channels. It is also desirable to construct a reliable network topology since it will result in some benefits for the network performance.

Topology control focuses on network connectivity with the link information provided by MAC and physical layers. There are two aspects in a network topology: network nodes and the connection links among them. In general, a MANET can be mapped into a graph $\mathcal{G}\ (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes in the network and $\mathcal{E}$ is the edge set representing the wireless links. A link is generally composed of two nodes which are in the transmission range of each other in classical MANETs. The topology of such a classical MANET is parameterized by some controllable parameters, which determine the existence of wireless links directly. In traditional MANETs without cooperative communications, these parameters can be transmission power, antenna directions, etc. In MANETs with cooperative communications, topology control also needs to determine the transmission manner (i.e., direct transmission, multi-hop transmission, or cooperative transmission) and the relay node if cooperative transmission is in use.

As topology control is to determine the existence of wireless links subject to network connectivity, the general topology control problem can be expressed as

$$\mathcal{G}^* = \arg\max f(\mathcal{G}), \qquad (1)$$
s.t. network connectivity.

The problem Eq. 1 uses the original network topology $\mathcal{G}$, which contains mobile nodes and link connections, as the input. According to the objective function, a better topology $\mathcal{G}^*(\mathcal{V}, \mathcal{E}^*)$ will be constructed as the output of the algorithm. $\mathcal{G}^*$should contain all mobile nodes in $\mathcal{G}$, and the link connections $\mathcal{E}^*$ should preserve network connectivity without partitioning the network. The structure of resulting topology is strongly related to the optimization objective function, which is $f(\mathcal{G})$ in Eq. 1.

It is difficult to collect the entire network information in MANETs. Therefore, it is desirable to design a distributed algorithm, which generally requires only local knowledge, and the algorithm is run at every node independently. Consequently, each node in the network is responsible for managing the links to all its neighbours only. If all the neighbour connections are preserved, the end-to-end connectivity is then guaranteed. Given a neighbourhood graph $\mathcal{G}_N$ ($\mathcal{V}_N$, $\mathcal{E}_N$) with N neighbouring nodes, a distributed topology control problem can be defined as $\mathcal{G}^*_N$ = arg max $f(\mathcal{G}_N)$, s.t. connectivity to all the neighbours. The objective function $f(\mathcal{G})$ in Eq. 1 is critical to topology control problems. Network capacity is an important objective function. Work in [16] shows that topology control can affect network capacity significantly. In the following section, a topology control scheme with the objective of optimizing network capacity in MANETs with cooperative communications is presented.

III. Topology Control For Network Capacity Improvement In Manets With Cooperative Communications

In this section, the capacity of MANETs is described first. Then, the COCO topology control scheme for MANETs with cooperative communications is presented.

A. *The Capacity of MANETs*

As a key indicator for the information delivery ability, network capacity has attracted tremendous interest since the landmark paper by Gupta and Kumar [17]. There are different definitions for network capacity. Two types of network capacity are introduced in [17]. The first one is transport capacity, which is similar to the total one-hop capacity in the network. It takes distance into consideration and is based on the sum of bit-meter products. One bit-meter means that one bit has been transported to a distance of one meter toward its destination. Another type of capacity is throughput capacity, which is based on the information capacity of a channel. Obviously, it is the amount of all the data successfully transmitted during a unit time. It has been shown that the capacity in wireless ad hoc networks is limited. In traditional MANETs without cooperative communications, the capacity is decreased as the number of nodes in the network increases. Asymptotically, the per-node throughput declines to zero when the number of nodes approaches to infinity [17]. In this paper, the second type of definition is adopted.

The expected network capacity is determined by various factors: wireless channel data rate in the physical layer, spatial reuse scheduling and interference in the link layer, topology control presented earlier, traffic balance in routing, traffic patterns, etc. In the physical layer, channel data rate is one of the main factors. Theoretically, channel capacity can be derived using Shannon's capacity formula. In practice, wireless channel data rate is jointly determined by the modulation, channel coding, transmission power, fading, etc. In addition, outage capacity is usually used in practice, which is supported by a small outage probability, to represent the link capacity.

In the link layer, the spatial reuse is the major ingredient that affects network capacity. Link interference, which refers to the affected nodes during the transmission, also has a significant impact on network capacity. Higher interference may reduce simultaneous transmissions in the network, thus reduce the network capacity, and vice versa. The MAC function should avoid collision with existing transmission. It uses a spatial and temporal scheduling so that simultaneous transmissions do not interfere with each other. Nodes within the transmission range of the sender must keep silent to avoid destroying on- going transmissions. In addition, there are some factors that prevent the channel capacity from being fully utilized, such as hidden and exposed terminals, which need to be solved using handshake protocols or a dedicated control channel in wireless networks.

Routing not only finds paths to meet quality of service (QoS) requirements, but also balances traffic loads in nodes to avoid hot spots in the network. By balancing traffic, the network may admit more traffic flows and maximize the capacity. With the focus on topology control and cooperative communications, an ideal load balance in the network is assumed, where the traffic loads in the network are uniformly distributed to the nodes in the network.

The study in [3] shows that cooperative transmissions do not always outperform direct transmissions. If there is no such relay that makes cooperative transmissions have larger outage capacity, information is directly transmitted or via multi-hops. For this reason, one needs to determine the best link block (Fig. 1) and the best relay to optimize link capacity. On the other hand, other nodes in the transmission range have to be silent in order not to disrupt the transmission due to the open shared wireless media. The affected areas include the coverage of the source, the coverage of the destination, as well as the coverage of the relay.

B. Improving Network Capacity using Topology Control in MANETs with Cooperative Communications

To improve the network capacity in MANETs with cooperative communications using topology control, the network capacity can be set as the objective function in the topology control problem in Eq. 1. In order to derive the network capacity in a MANET with cooperative communications, one needs to obtain the link capacity and inference model when a specific transmission manner (i.e., direct transmission, multi-hop transmission, or cooperative transmission) is used.

Definition 1 (Node coverage). *The coverage of a node refers to its neighbours, i.e.,*$Cov(u)=V_N(u)$ *for node* u*. In the physical meaning, it includes nodes covered by this node.*

Definition 2 (Link interference). *It refers to the number of influenced nodes during the transmission.*

Definition 3 (Network capacity). *Network capacity refers to the maximum achievable throughput of bits per second for each node on average that can be sent to its destination.*

When traditional direct transmission is used, given a small outage probability, the outage link capacity can be derived. Since only two nodes are involved in the direct transmission, the interference set of a direct transmission is the union of coverage sets of the source node and the destination node. In this paper, the interference model in [17] is adopted, which confines concurrent transmissions in the vicinity of the transmitter and receiver. This model fits the medium access control function well (e.g., the popular IEEE 802.11 MAC in most mobile devices in MANETs). Herein, interference of a link is defined as some combination of coverage of nodes involved in the transmission.

Multi hop transmission can be illustrated using two-hop transmission. When two-hop transmission is used, two time slots are consumed. In the first slot, messages are transmitted from the source to the relay, and the messages will be forwarded to the destination in the second slot. The outage capacity of this two-hop transmission can be derived considering the outage of each hop transmission. The transmission of each hop has its own interference, which happens in different slots. Since the transmission of the two hops cannot occur simultaneously but in two separate time slots, the end-to-end interference set of the multi-hop link is determined by the maximum of the two interference sets.

When cooperative transmission is used, a best relay needs to be selected proactively before transmission. In this study, the decode-and-forward relaying scheme is adopted. The source broadcasts its messages to the relay and destination in the first slot. The relay node decodes and re-encodes the signal from the source, and then forwards it to the destination in the second slot. The two signals of the source and the relay are decoded by maximal rate combining at the destination. The maximum instantaneous end-to-end mutual information, outage probability, and outage capacity can be derived [3]. For the interference model, in the broadcast period, both the covered neighbours of the source and the covered neighbours of the relay and the destination have to be silent to ensure successful receptions. In the second slot, both the covered neighbours of the selected relay and the destination have to be silent to ensure successful receptions.

After obtaining the link capacity and inference models, the network capacity can be derived [16] as the objective function in the topology control problem in Eq. 1. By considering direct transmission, multi hop transmission, cooperative transmission, and interference, the proposed COCO topology control scheme extends physical layer cooperative communications from the link-level perspective to the network-level perspective in MANETs. The proposed scheme can determine the best type of transmission and the best relay to optimize network capacity.

IV. Authentication Schemes in Wireless Networks

In the remainder of this section, key concepts of hash-chain-based authentication and integrity protection are reviewed and related work in the field of hop-by-hop authentication is discussed.

A. Hash-chain-based Signatures

The fundamental idea behind hash chains is the iterated application of a cryptographic hash function H (e.g., SHA-1 or a block-cipher-based hash function) on a random seed value s. The first result $H(s) = h_1$ is used as input for the next round, yielding $H(H(s)) = H(h_1) = h_2$ until the hash chain has reached the desired length n. The last element of the chain h_n is called the anchor. The elements of this one-way hash chain are used in reverse order of creation, i.e., beginning with the anchor h_n and proceeding with h_{n-1}. In terms of a protocol, the owner of a hash chain first exchanges the anchor with its peer. When required to authenticate itself, the owner reveals the next undisclosed hash chain element, and thus enables the receiver of the element to verify that it is in possession of the hash chain. Attaching a notion of identity to a hash chain, hosts can prove their identity for re-authentication by disclosing previously undisclosed elements of the chain as used by Hauser et al. [18]. This re-authentication property is important for mobile multi hop networks as identities cannot be tied to non-cryptographic node characteristics, such as IP addresses, without security risks. Note that additional identity providing techniques, such as public-key authenticated hash chain anchors, are required for a strong assurance of identities. There are three conceptually different approaches for signing and verifying messages with hash chains: one-time signatures, time-based, and interaction-based.

Neither the time-based nor the interactive approaches lend themselves to securing point-to point communication in combination with on path authentication of packets to suppress unsolicited traffic within the network. Moreover, the protocols lack adaptation capabilities regarding varying latency, bandwidth, and reliability requirements, and hence, each approach is restricted for a specific use-case. One-time signature schemes (e.g., [19, 20]), are not considered further because of their prohibitively high computational costs and large signature sizes.

B. Hop-by-hop Authentication

LHAP [22, 23] and HEAP [21] were specifically designed for hop-by-hop authentication in MANETs. LHAP uses TESLA for bootstrapping trust relationships between nodes, and it uses authentication tokens when forwarding data packets. Lu and Pooch [23] propose HEAP, a system that builds on LHAP but uses a TESLA-like protocol for securing data transmission between two adjacent routers. HEAP uses pair-wise symmetric keys and a modified HMAC function to authenticate packets hop-by-hop. Gouda et al. present three protocols for hop integrity protection [24], in which symmetric keys between adjacent routers are used to identify injected and modified packets. All of the aforementioned protocols aim at preventing outsider attacks by unauthorized senders. However, they cannot mitigate insider attacks such as forged or manipulated messages by otherwise trusted nodes. Protection against these attacks would require end-to-end integrity protection that can be verified on every hop. Zhu et al. [25] and Ye et al. [26] solved the problem of efficient en-route verification with probabilistic approaches. However, both techniques are tightly coupled to a large sensor-network scenario with multiple cooperating sensors, sensing and sending the same information to a fixed sink (base station). Hence, the employed methods are not suitable for point-to-point communication between single hosts in networks of all sizes. Zhang et al. [27] use polynomial-based cryptography for authenticating packets in WSNs. Their approach assumes the presence of a central security server that provides keying-material to all nodes before deployment. Although this assumption is viable for many WSN scenarios, it is inapplicable to many dynamic and decentralized deployments.

V. Design of ALPHA Protocol

In this section, the design of the Adaptive and Lightweight Protocol for Hop-by-hop Authentication (ALPHA) is presented. ALPHA protects the communication between two arbitrary nodes in multi-hop networks. It uses the notion of a protected path between these nodes. Before sending potentially large data packets, a small path reservation packet is sent to the destination, enabling the receiver and all intermediate nodes to efficiently check the integrity of the data packet. ALPHA is adaptive in the sense that it can be used for occasional signalling traffic as well as for high-volume data streams. Moreover, it provides integrated support for reliable and unreliable data transmission.

A. Basic ALPHA Protocol

For a better understanding, an overview of the basic ALPHA signature process is done before discussing extensions that enable the adaptation of ALPHA. The signature process takes place after an initial handshake in which the anchors of the hash chains are exchanged.

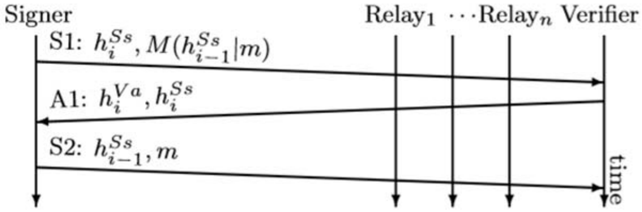
Signer
Relay$_1$ $\cdots$Relay$_n$ Verifier
S1: $h_i^{Ss}, M(h_{i-1}^{Ss}|m)$
A1: h_i^{Va}, h_i^{Ss}
S2: h_{i-1}^{Ss}, m
time

Fig. 2. Basic ALPHA signature scheme. Relays can authenticate *m* before forwarding it.

An unprotected handshake provides each peer of a security association with an ephemeral anonymous identity that is only of use in the corresponding association. Even with an anonymous identity, hosts can use ALPHA to securely signal changes concerning an association (e.g. signalling new IP addresses, throttling the transmission rate, closing an association, etc.) to their peers. Relays learn the hash chain elements or anchors by observing a handshake. A protected handshake binds hash chains to strong cryptographic identities (e.g., public-key-based certificates) and vice versa, which allows for identifying hosts (e.g., insiders and outsiders) or certain roles (e.g., coordinator, server, and client). To protect bootstrapping, the anchor of a hash chain is signed with signatures based on asymmetric cryptography, such as RSA, DSA, and Elliptic Curve Cryptography (ECC). Because of the high resource requirements of asymmetric cryptography, ALPHA explicitly limits its use to this bootstrapping process. For strong hop-by-hop authentication towards relays, the public-key signature of the sender needs to be verified by each relay for bootstrapping and revalidated each time the set of relays changes. Due to the CPU complexity and energy consumption imposed by such cryptographic operations, such a strong hop-by-hop authentication can be assumed to be prohibitively resource intensive for MANETs with their frequently changing routes. However, it may be feasible for WSNs and WMNs in which routes fluctuate only occasionally.

The goal of the signature process is to transmit an integrity-protected message *m* from a signer to a verifier in a way that lets relays verify that *m* was (a) sent by a legitimate sender, (b) the sender is authorized to send *m*, and (c) *m* has not been altered by an attacker on the path. The basic ALPHA signature scheme consists of a three-way packet exchange for each protected payload message *m*. Figure 2 depicts the packet exchange. The ALPHA signature scheme belongs to the class of interactive hash chain signatures. Hence, ALPHA uses deferred secret disclosure in combination with an interlocking scheme. The first packet announces a Message Authentication Code (MAC) *M* of *m* keyed with a fresh hash-chain element of the signer. In the second packet, the verifier acknowledges the receipt of the MAC and in the third packet, the signer sends *m* and discloses the hash chain element that was used as the MAC key. In the following the three-way signature process is discussed in detail.

Typically, an end-host acts both as a signer and a verifier on a bi-directional packet flow. Each host uses separate hash chains for signing outgoing and acknowledging incoming packets. Therefore, the shared security context between two hosts A and B consists of the respective anchors $\{h_n^{As}, h_n^{Aa}, h_n^{Bs}, h_n^{Ba}\}$. The two hash chains with superscript A are owned by host A while the other hash chains are owned by host B. Hosts use the first hash chain for signing data (i.e., it provides temporary keys for creating MACs) while they use the second chain for acknowledging the receipt of a message. Hence, the hash chains are denoted *signature chain* and *acknowledgment chain* and are signified by the second superscripts s and a.

Each pair of a sender's signature chain and a receiver's acknowledgment chain protects a simplex channel. Hence, using the 4-tuple protects a duplex-channel between the hosts. Note that a different set of hash chains is to be used for each path. In the remainder of the section, the protection of such simplex channels between a signer S and a verifier V with the respective anchors being h_n^{Ss} and h_n^{Va} without loss of generality is discussed.

By using two hash chains per host, ALPHA creates a full-duplex channel consisting of two simplex channels. Each signature packet exchange is initiated with an S1 packet from the signer to the verifier.

The packet fulfils three objectives. First, a fresh hash chain element of the signer's signature chain h_i^{Ss} identifies the signer. Second, a MAC keyed with the signer's next undisclosed signature chain element M (h_{i-1}^{Ss}, m) ensures the integrity of *m*. Since attackers are not in possession of the undisclosed hash chain elements, they cannot forge valid MACs. The verifier and relays buffer the MAC until *m* and its key are disclosed through a subsequent S2 packet. Third, the S1 packet triggers the verifier to send an acknowledgment packet A1. The A1 packet indicates that the verifier buffered the MAC and it expresses the willingness of the verifier to receive *m*. To authenticate the A1 packet, the verifier attaches the next undisclosed hash chain element of its acknowledgment chain h_i^{Va} to the A1.

Similar to S1 packets, attackers cannot forge A1 packets as they are not in possession of h_i^{Va} before the verifier has received the S1 packet. On receipt of a valid A1 packet, the signer discloses the key of the MAC h_{i-1}^{Ss} and the message *m* in the S2 data packet. With this key, the verifier and all relays that buffered M (h_{i-1}^{Ss}, m) can check the integrity of *m* by re-computing the MAC. Tampering with the message *m* is ineffective because the verifier can check its validity against the tamperproof MAC from the S1 packet.

B. *Efficient On-path Authentication*

For efficiency, similar to the broadcast authentication scheme in [28], ALPHA only transmits the MAC of a message in the first packet and sends *m* in the S2 packet, so the first packet only contains small hash values. The message *m* is still protected by the MAC and the temporal separation between the creation and delivery of the signature and the disclosure of the MAC key is still guaranteed. These signatures are referred with delayed message disclosure as pre-signatures. Pre-signatures drastically reduce the amount of data buffered on verifiers and relays. Although the benefit for today's typical Internet end hosts is marginal, this reduction makes hash-chain-based signatures feasible on low-end devices, such as sensor nodes. On forwarding devices in particular, pre-signatures offer significantly better scalability with the number of flows than regularly signed messages. Additionally, the lower buffer requirements render memory exhaustion attacks more difficult. In the spirit of the Guy Fawkes protocol, pre-signatures in ALPHA do not reveal a message m until it can be verified. Thus, an attacker's window of opportunity to react to m and influence the verifier is reduced by a full round-trip time. The relaying nodes on a path can verify the integrity and origin of a message if they have forwarded all previous signatures between the signer and the verifier. However, two colluding attackers can replay forged signatures to a victim relay after diverting genuine signature packets around the victim (bypass attack). While the end-to-end integrity protection and the on-path filtering function of unsolicited packets are not affected by this attack (the second attacker must be located on the path behind the victim and it must express interest in receiving the replayed packets), the secure extraction of signed data by forwarding nodes suffers. The solution for preventing this attack is to keep the set of relaying nodes static throughout the use of a hash chain.

VI. Implementation of COCO+ALPHA Scheme and Results

Java programming language is used to implement the proposed COCO+ALPHA scheme. In the remainder of this section, first the proposed COCO algorithm that is used to control the topology is discussed then COCO scheme is combined with existing ALPHA scheme to provide hop-by-hop authentication.

A. Design of COCO+ALPHA Algorithm

Key formulae used in this algorithm are, Objective function that optimizes network capacity, outage capacity and interference.

Objective function, $g\left(\gamma(R_j)\right) = C_\varepsilon\left(\gamma(R_j)\right)/I(R_j)$

Outage capacity,

$$C_\varepsilon\left(\gamma(R_j)\right) = \begin{cases} \log_2\left(1+\gamma_0 \ln\frac{1}{1-\varepsilon}\right), \; R_j = 0 \\ \frac{1}{2}\log_2\left(1+\ln\frac{1}{u_\varepsilon\left(\gamma(\theta_j)\right)}\right), \; 0 < R_j \le m \\ \frac{1}{2}\log_2\left(1+\frac{1}{\frac{1}{\gamma_1}+\frac{1}{\gamma_2}}\ln\frac{1}{1-\varepsilon}\right), m < R_j \le 2m \end{cases}$$

The case $R_j = 0$ corresponds to direct transmissions. For the other two relaying cases, if R_j is selected for cooperative relaying, $R_j + m$ is the same selected relay node but for multi-hop relaying.

$\gamma(R_j) = (\gamma_0, \gamma_1, \gamma_2)$ denote the received SNRs from the source to the destination, from the source to the relay and from the relay to the destination, respectively.

Interference,

$$I(R_j) = \begin{cases} I_{DT}(R_j), R_j = 0 \\ I_{CT}(R_j), 0 < R_j \le m \\ I_{MT}(R_j), m < R_j \le 2m \end{cases}$$

$$I_{DT} = Cov(S) \cup Cov(D)$$

$$I_{MT} = max\{Cov(S) \cup Cov(R), Cov(R) \cup Cov(D)\}$$

$$I_{CT} = Cov(S) \cup Cov(R) \cup Cov(D)$$

Algorithm 1. *COCO+ALPHA Algorithm*

Step 0: Select a relay node, $R_j[n]$ in a random fashion. Where, j is the neighbour and n is the #iteration.

Step 1: Calculate outage capacity (C_ε) of the channel between $R_j[n]$ and $R_j[n+1]$.

And also calculate outage capacity of the channel between $R_j[n]$ and $\widetilde{R}_j[n]$.

Step 2: Calculate interference in the selected channels.

Step 3: Evaluate objective function.

Step 4: Acceptance

```
IF $g(\widetilde{R}_j[n]) > g(R_j[n])$
        $R_j[n+1] = \widetilde{R}_j[n]$. (Alternative node)
ELSE
        $R_j[n+1] = R_j[n]$. (Next node)
END IF
```

Go back to *Step 1* till you complete all the links. Implement next steps on the established path.

Step 5: Send S1 packet from source to destination. S1 packet consists of SK_2 and MAC [SK_1+Message].

Step 6: Upon Successful reception of S1 packet at destination, send A1 packet to source. A1 packet consists of DK_1 and SK_2.

Step 7: Upon successful reception of valid A1 packet, send S2 packet to destination. S2 packet consists of SK_1 and Message.

Step 8: Calculate MAC [SK_1 and Message] and compare it with received MAC to check the integrity of the transferred message.

B. Implementation and Results

Several nodes are deployed randomly to form a MANET using a custom simulator which is developed using Java. The performance of the proposed scheme with that of an existing well-known topology control scheme [29], called LLISE, which only considers traditional multi hop transmissions without cooperative communications and preserves the minimum interference path for each neighbour link locally. Figure 3 shows the performance graph. It may be seen from the figure, the proposed COCO+ALPHA scheme has the highest network capacity regardless of the number of nodes in the network. Similar to COCO, LLISE is executed in a distributed manner. It preserves all the edges on the minimum interference path for each link in the resulting topology, thus minimizes the interference to improve network capacity. Nevertheless, COCO+ALPHA can achieve a much higher network capacity than LLISE, since LLISE only considers multi hop transmissions. The performance gain of the proposed scheme comes from the joint design of transmission mode selection, relay node selection, and interference minimization in MANETs with cooperative communications. At the end it is verified that Received MAC and calculated MAC match with each other. It means the proposed COCO+ALPHA scheme has successfully ensured hop-by-hop authentication and integrity of the transferred message.

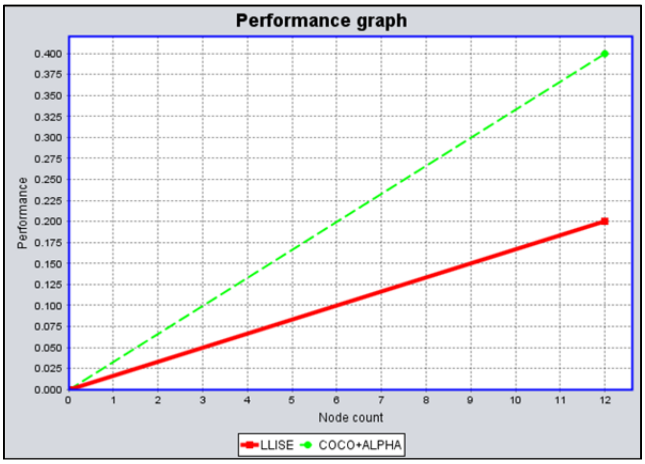

Fig. 3. Performance comparison between LLISE and proposed COCO+ALPHA scheme

VII. Conclusion

In this paper, physical layer cooperative communications, topology control, network capacity, and authentication schemes in MANETs are introduced. To improve the network capacity and ensure hop-by-hop authentication of MANETs with cooperative communications, we have proposed a Capacity-Optimized Cooperative (COCO) +ALPHA topology control scheme that considers both upper layer network capacity and physical layer relay selection in cooperative communications. Simulation results have shown that physical layer cooperative communications techniques have significant impact on the network capacity, and the pro- posed topology control scheme can substantially improve the network capacity in MANETs with cooperative communications. Moreover, the scheme also ensures authentication and integrity of the communication in MANETs.

References

[1] J. Laneman, D. Tse, and G. Wornell, “Cooperative Diversity in Wireless Networks: Efficient protocols and Outage Behavior,” *IEEE Trans. Info. Theory,* vol. 50, no. 12, 2004, pp. 3062–80.

[2] P. H. J. Chong et al., “Technologies in Multihop Cellular Network,” *IEEE Commun. Mag.,* vol. 45, Sept. 2007, pp. 64–65.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] 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, 2009.

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

[6] 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.

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

[8] A. Perrig, R. Canetti, D. Tygar, and D. Song, “The TESLA broadcast authentication protocol.” *Cryptobytes 5* (2002).

[9] F. Bergadano, D. Cavagnino, and B. Crispo, “Chained Stream Authentication.” *Selected Areas in Cryptography: 7th Annual International Workshop, SAC 2000* (2000).

[10] A. Weimerskirch and D. Westhoff, “Zero Common-Knowledge Authentication for Pervasive Networks.” *SAC ’03* (2003).

[11] R. Anderson, F. Bergadano, B. Crispo, J. Lee, C. Manifavas, and R. Needham, “A new family of authentication protocols.” *Operating systems review* 32, 4 (1998).

[12] V. Torvinen, and J.Ylitalo, “Weak Context Establishment Procedure for Mobility Management and Multi-Homing.” *IFIP Conference on Communications and Multimedia Security* (2004).

[13] Q. Guan, F.R. Yu, S. Jiang, V.C.M. Leung, H. Mehrvar, “Topology control in mobile ad hoc networks with cooperative communications,” *IEEE Wireless Comm*. 19, 74-79 (2012).

[14] Q. Guan et al., “Capacity-Optimized Topology Control for MANETs with Cooperative Communications,” *IEEE Trans. Wireless Commun.*, vol. 10, July 2011, pp. 2162–70.

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

[16] T. Cover and A. E. Gamal, “Capacity Theorems for the Relay Channel,” *IEEE Trans. Info. Theory,* vol. 25, Sept. 1979, pp. 572–84.

[17] Q. Guan et al., “Impact of Topology Control on Capacity of Wireless Ad Hoc Networks,” *Proc. IEEE ICCS,* Guangzhou, P. R. China, Nov. 2008.

[18] P. Gupta and P. Kumar, “The Capacity of Wireless Networks,” *IEEE Trans. Info. Theory,* vol. 46, no. 2, 2000, pp. 388–404.

[19] R. Hauser, A. Przygienda, and G. Tsudik, “Reducing the Cost of Security in Link State Routing.” *NDSS ’97* (1997).

[20] R. C. Merkle, “A digital signature based on a conventional encryption function.” *CRYPTO ’87* (1988).

[21] K. Zhang, “Efficient protocols for signing routing messages.” *NDSS ’98* (1998).

[22] R. Akbani, T. Korkmaz, and G. Raju, “HEAP: Hop-by-hop Efficient Authentication Protocol for Mobile Ad-hoc Networks.” *CNS 07* (2007).

[23] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks.” *Distributed Computing Systems Workshops, 2003* (2003).

[24] B. Lu, and U. W. Pooch, “A Light-weight Hop-by-hop Authentication Protocol for Mobile Ad Hoc Networks.” *International Journal of Information Technology* 11, 2 (2005).

[25] M. G. Gouda, E. N. Elnozahy, C. Huang, and T. M. McGuire, “Hop integrity in computer networks.” *IEEE/ACM Transactions on Networking* 10 (2002).

[26] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks.” *Security and Privacy* (2004).

[27] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks.” *IEEE Journal on Selected Areas in Communications 23* (2005).

[28] W. Zhang, N. Subramanian, and G. Wang, “Lightweight and compromise-resilient message authentication in sensor networks.” *INFOCOM 2008* (2008).

[29] T. Yao, S. Fukunaga, and T. Nakai, “Reliable broadcast message authentication in wireless sensor networks.” *EUC Workshops* (2006).

[30] M. Burkhart et al., “Does Topology Control Reduce Interference?,” *Proc. 5th ACM Int’l. Symp. Mobile Ad Hoc Networking and Computing, Tokyo, Japan,* May 2004, pp. 9–19.