Security Enabled Relay Selection in Cooperative Communication Networks

by

Ramya Ramamoorthy

A thesis submitted to the

Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Master of Applied Science in Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering (OCIECE)

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

August 2010

Your file Votre référence
ISBN: 978-0-494-71565-9
Our file Notre référence
ISBN: 978-0-494-71565-9

The undersigned hereby recommends to the

Faculty of Graduate Studies and Research

acceptance of the thesis

Security Enabled Relay Selection in Cooperative Communication Networks

submitted by

Ramya Ramamoorthy, B.Eng.

in partial fulfillment of the requirements for the degree of

Master of Applied Science in Electrical and Computer Engineering

---

Chair, Professor Howard Schwartz,
Department of Systems and Computer Engineering

Thesis Supervisor, Professor Fei Richard Yu

Carleton University

August 2010

Abstract

Cooperative communication is considered a promising technique for both infrastructure-based networks like cellular systems and IEEE 802.16j, and for infrastructure-less networks like mobile ad hoc networks. However, it also raises serious security issues as the communication approach is dependent upon the integrity of the relays. In this thesis, a *prevention*-based security technique for cooperative communication is proposed taking into consideration authentication protocol, based on hash chains and Merkle trees, along with throughput quality of service (QoS) optimization making use of physical layer parameters. The proposed Joint Authentication and QoS Scheme (JAQS) is implemented to select the best relay proactively considering both end-to-end and hop-by-hop authentication and integrity protection, and to confirm the identity of the node and the integrity of the message during the transmission process. An integrated design approach is taken to optimize the number of messages in the Merkle tree, an important parameter in the authentication scheme, and relay selection in cooperative communication networks. As part of our work, we derive closed-form secured throughput equations defining the time constituents taking into consideration error control schemes. We present simulation results to show that the proposed relay selection scheme, which provides authentication and integrity protection, outperforms the existing relay selection scheme based on outage capacity in terms of throughput performance.

Acknowledgments

I would like extend my heartfelt thanks and sincere gratitude to my supervisor Professor F. Richard Yu for his guidance while I was carrying out this project. He has helped me from the time I registered in the graduate programme, and provided a constant source of support and encouragement when I was troubled by uncertainties. This thesis would not have been possible without his invaluable support.

I would like to dedicate my work to my family and friends for their continued and constant support and love throughout the course of my studies. I thank them for their kind understanding and encouragement, and for having put up with me throughout my study years.

I would also like to thank all my colleagues for their encouragement, support and assistance during the duration of my studies.

Thank you all!!!

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMT	Acknowledgment Merkle Tree
ALPHA	Adaptive and Lightweight Protocol for Hop-by-hop Authentication
AES	Advanced Encryption Standard
AF	Amplify-and-Forward
ARQ	Automatic Repeat reQuest
BPSK	Binary Phase Shift Keying
BER	Bit Error Rate
CA	Certification Authority
CSA	Chained Stream Authentication
CTS	Clear-to-Send
DES	Data Encryption Standard
DF	Decode-and-Forward
DC	Direct Communication
ECC	Elliptic Curve Cryptosystem
FSDF	Fixed Selective Decode-and-Forward
FEC	Forward Error Correction
GBN	Go-Back-N
HMAC	Hash Message Authentication Code
HEAP	Hop-by-Hop Efficient Authentication Protocol
IBE	Identity Based Encryption
TrustCom	International Symposium on Trusted Computing and Communications
ITU	International Telecommunications Union

JAQS	Joint Authentication and QoS Scheme
KAMAN	Kerberos assisted Authentication in Mobile Ad hoc Networks
LHAP	Lightweight Hop-by-Hop Authentication Protocol
MRC	Maximal Ratio Combining
MT	Merkle Tree
MAC	Message Authentication Code
MD	Message Digest
MANET	Mobile Ad hoc NETwork
MCN	Multihop Cellular Network
MIMO	Multiple-Input Multiple-Output
nack	Negative Acknowledgment
OREL	Orthogonal Opportunistic Relaying
ack	Positive Acknowledgment
P2P	Peer-to-Peer
PKG	Private Key Generator
PKI	Public Key Infrastructure
QoS	Quality of Service
RTS	Ready-to-Send
SHA	Secure Hash Algorithm
SR	Selective Repeat
SNR	Signal-to-Noise Ratio
SC	Smart Cooperation/Smart Cooperative
SSDF	Smart Selective Decode-and-Forward
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TTP	Trusted Third Party
UWB	Ultrawideband
WIMP	Weak Identifier Multihoming Protocol
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

WSN	Wireless Sensor Network
ZCK	Zero Common-Knowledge

List of Symbols

c	Speed of Light
S	Source
D	Destination
R	Relay
K	Number of Relay Nodes
R_k^*	Best Relay
SRD	Source-Relay-Destination
ϵ	Number or Element of
x *and* y	Nodes
h_{xy}	Channel Gain
r	Data Rate/Largest Rate of Transmission
α	Path Loss Exponent
$1/\lambda_{xy}$	Variance
P	Average Transmit Signal Power
W	Transmission Bandwidth
N_o	Noise
d_{xy}	Distance Between Nodes x and y
d_{R_kD}	Distance between Relay Node and Destination
d_{SD}	Distance between Source and Destination
d_{SR_k}	Distance between Source and Relay Node
γ	Average Transmitted SNR
$\overline{\gamma}$	Average Received Signal-to-Noise Ratio

$\overline{\gamma_{R_k D}}$	Average Received SNR between Relay and Destination
$\overline{\gamma_{SD}}$	Average Received SNR between Source and Destination
$\overline{\gamma_{SR_k}}$	Average Received SNR between Source and Relay
$\|h_{SD}\|$	Channel between Source and Destination
$\|h_{SR_k}\|$	Channel between Source and Relay
$\|h_{R_k D}\|$	Channel between Relay and Destination
I	Mutual Information
I_{coop}	Mutual Information in the Cooperative Mode
$I_{non-coop}$	Mutual Information in the Non-Cooperative Mode
I_{SC}	Mutual Information in Smart Cooperative (SC) Relaying System
I_{SR_k}	Mutual Information between Source and each of the Relay
I_{MRC}	Mutual Information between Source-Destination and Destination-Relay
P_{out}	Outage Probability
ε	Fixed Outage Probability
$P_{out}^{SC,k}$	Outage Probability for a Relay in SC Relaying System
$P_{out}^{SR_k}$	Outage Probability from Source to Relay
$C_{\epsilon}^{SC,k}$	Outage Capacity for a Relay in SC Relaying System
$P_e^{SC,k}$	End-to-end Bit Error Rate for a Relay in SC Relaying System
P_e^{SD}	Probability of Error in Direct Transmission
$P_e^{div,k}$	Probability of Error in Combined Transmission
P_c	Packet Error Rate
ip	Input for One-way Function
F	One-Way Function
z	Result of $F(ip)$
h_i	Hash Chain Anchor
h_i^S	Anchor of Hash Chain at the Source
h_i^D	Anchor of Hash Chain at the Destination
i	Hash Chain Length
θ	Hash Chain Random Seed Variable

H	Hash Function SHA-1
S_h	Hash Output
S_1	Initial Packet containing Pre-signature sent by Source
S_2	Message Packet sent by Source
A_1	Acknowledgment Pre-signature initial packet from Destination
A_2	Acknowledgment Packet sent by Destination
$S_{payload}$	Amount of Payload that can be transmitted with a Single Pre-signature
S_{packet}	Size of Packet
T_1	Time for Initial Pre-signature process between Source and Destination
T_2	Time for Actual Message Transmission and Delivery
t_{ack1}	Packet Transmission Time for A_1
t_{ack2}	Packet Transmission Time for A_2
t_{f1}	Packet Transmission Time for S_1
t_{f2}	Packet Transmission Time for S_2
m	Message
m_j	Message Blocks
u_{ack1}	Number of Bits in A_1
u_{ack2}	Number of Bits in A_2
u_{f1}	Number of Bits in S_1
u_{f2}	Number of Bits in S_2
t_{proc1}	Processing Time in T_1
t_{proc2}	Processing Time in T_2
t_{prop1}	Propagation Time for S_1
t_{prop2}	Propagation Time for S_2
n	Number of Leaves in Merkle Tree or Messages or Data Blocks
$\log_2(n)$	Number of Sibling Nodes in Merkle Tree
n^*	Optimal Number of Messages in Merkle Tree providing Maximum Throughput
n_k^*	Optimal Number of Messages in Merkle Tree for Relay R_k
$\{B_c\}$	Set of Sibling Nodes on the Path from Message to Root in the Merkle Tree

W_s	Window Size

Chapter 1

Introduction

1.1 Research Overview

"*Cooperation is not a natural characteristic attributed to human beings. The typical human horizon is focused on short-term gains, which might be due to our instinct-driven subconscious occupying a grander importance than we dare to admit (Gray, 2002). Cooperating with other individuals or entities, however, usually means that short-term losses may translate into long-term gains.... Any cooperative technology depending solely on human decisions is hence a priori doomed to fail; history has shown this on numerous occasions. By contrast, if we rely on machines that have access to some decision making engines, cooperative schemes become viable communication techniques and are likely to occupy an important place in the technological landscape of the 21st century*" [1].

In all parts of our life, we are continuously making use of wireless technologies. We cannot imagine living in a world where we do not have access to wireless devices. We now make use of applications that feed hungrily on bandwidth and power and the usage is destined to grow further. Cooperative communication is a way to maximize the available resources to expand coverage and at the same time reduce the power

consumption.

Wireless communication systems are traditionally conceptualized such that users individually communicate with the associated base stations and vice versa. Cooperation is referred to as any architecture that deviates from this traditional approach, wherein a users communication link is enhanced in a supportive way by relays or in a cooperative way by other users [2].

In wireless communication systems, when the source desires to transmit a message to a destination, the message is broadcasted with the signal traveling through a wireless channel in all directions before finally reaching the destination. However, the destination may not receive the complete transmitted signal and may receive only a faded signal. Fading is observed in all wireless channels with the quality of the signal varying significantly over the course of transmission. While it is possible to mitigate or restrict the impact of fading by transmitting independent copies of the signal and thereby creating diversity, it is not practical to have the signals transmitted from multiple locations or to have the signal transmitted from multiple antennas in a single location on account of the size, space, and cost constraints. However, it is within the realms of possibility to achieve spatial diversity through cooperation between the source and the adjacent nodes.

Consider two nodes that want to communicate with each other, and let one of them be the source and the other, the destination, with other nodes located adjacent to them. When the source desires to transmit the signal to the destination, it broadcasts the signal and this is picked up by the destination and also by the multiple adjacent nodes. These nodes can then act as relays and retransmit the signal to the destination. The destination therefore gets more than one copy of the signal and can combine them to achieve the good quality transmitted signal. In a way, each node has multifold functions. It can act as the source, destination, or as a relay node. Apart from

transmitting not only its own information, it also can forward the information from its cooperative partners. This is the principle of cooperative communication where the wireless node transmits not only its own information, but also acts as a relay transmitting the information sent by its partner. Although each of the nodes has only one antenna and cannot generate spatial diversity on its own, through this kind of cooperation and partnering with the adjacent nodes, spatial diversity is achieved. This is also termed cooperative diversity because the nodes share their antennas and other resources to create a virtual array through distributed transmission and signal processing [3].

The broadcast nature of the wireless medium is the key attribute that helps in cooperative communication as the transmitted signal from the source could be received and processed by any node that can hear the signal [3]. Therefore, the cooperative communication uses the relays as virtual antenna to forward the information of the other nodes. In the cooperative communication system, two or more active nodes in a network partner and share to jointly transmit their signal to get better efficiency and reliability that can not be attained on an individual basis. By capitalizing on the statistically independent fading of the links between nodes, the reliability is significantly improved.

In brief, cooperative communication involves the following two main concepts [4]:

- Using relays (or multi-hop) to provide spatial diversity in a fading environment.
- Envisioning a collaborative scheme where the relay also has its own information to send so that the nodes help one another to communicate by acting as relays for each other (called as partners).

Cooperative communication is useful and is applicable to all types of wireless networks. In particular, it is well suited for ad hoc networks due to the inherent nature of the ad hoc network with its minimal configuration, decentralized approach

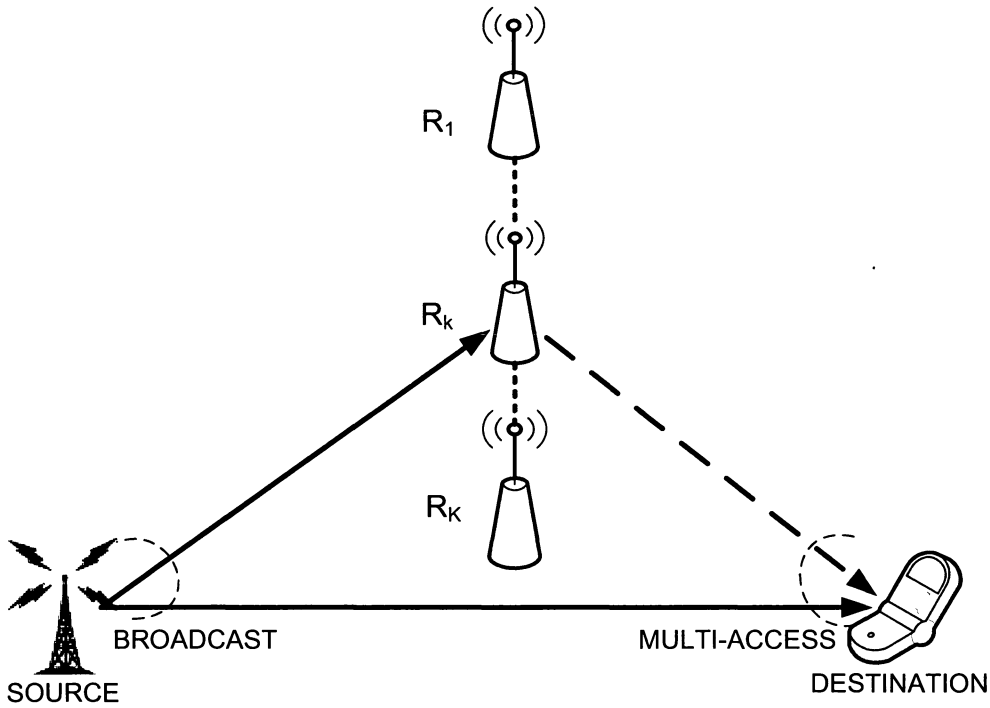

Figure 1.1: A cooperative communication network.

and self-configuration. It also finds a prominent place in the IEEE 802.16j standard that increases system coverage and performance through the use of relay stations located between the source base station and the destination mobile station.

A simple cooperative communication network is illustrated in Fig. 1.1. The communication takes place in two stages with the initial broadcast by the source in the first stage and retransmission of the signal by the relay in the second stage with the destination combining the received signals from both the source and the relays.

Our work is focused on a slowly-fading Rayleigh distribution channel with three-nodes, i.e., a two-hop network consisting of a source, destination, and multiple intermediate relays. Based on the channel conditions, the proactive opportunistic relay selection process can determine the best node amongst the multiple intermediate nodes that are available between the source and the destination that is best suited to

fit as the relay for the particular time slot or data transmission process. Currently, many conventional relay selection schemes have been proposed on the basis of outage capacity as a performance metric. Following the selection of the best relay, the actual data transmission process is initiated and the payload is transmitted by the source.

While cooperative communication provides significant performance and coverage benefits, it also raises security issues on account of the nature of the system with its decentralized approach, lack of centralized control, dynamic nature, and self-organization. The security vulnerabilities can be addressed either by *prevention*-based or *detection*-based techniques, and in this thesis, the focus is on *prevention*-based techniques, such as authentication, particularly data origin authentication, and integrity protection to act as the front line of defense in cooperative communication for integrity, confidentiality, and non-repudiation.

Public key cryptography and other asymmetric approaches can be used for end-to-end authentication, but they can lead to higher computational complexity. On the other hand, symmetric approaches that do not really permit integrity checking on forwarding nodes and distribution of shared keys are a critical problem. Therefore, a combined solution making use of hash chains and Merkle trees can be applied for effective authentication and integrity protection. Hash chains are simple and computationally efficient means of authenticating nodes in a network when tied to identities. Merkle tree is a tree of hashes and can be used to ensure that the messages are not tampered with.

In this thesis, a *prevention*-based security technique for cooperative communication is proposed taking into consideration authentication along with physical layer parameters which relate to the channel state information. We use an authentication protocol based on hash chains and Merkle trees to provide both hop-by-hop as well as end-to-end authentication and integrity protection. An integrated approach is

taken to optimize the number of messages/data blocks in the Merkle tree for different packet sizes, an important parameter in the authentication protocol, and to consider this protocol in the throughput quality of service (QoS) to determine proactively the best relay among the available relays. To the best of our knowledge, combining authentication and QoS for cooperative communication networks, and security enabled relay selection have not been considered in the existing work. We have not come across any solution in cooperative communication offering end-to-end and hop-by-hop authentication and integrity protection to enable the source, destination and the relay nodes to confirm the message identities and verify that the messages and the acknowledgements have not been tampered with during the transmission process. We carried out extensive simulation that showed the effectiveness of our proposed scheme. The best relay selected under our proposed scheme outperforms the relay selected through the conventional relay selection scheme using outage capacity in terms of throughput, and in addition is security-enabled providing both end-to-end and hop-by-hop authentication.

1.2 Research Motivation

Our motivation for carrying out this research originates from these following problems noticed in the cooperative communication network.

- While best relay selection has been suggested to be carried out on the basis of various parameters in cooperative communication, security, a critical aspect, has not been considered.

- In cooperative communication, the relay selection process is dynamic based on the channel conditions. The selection of best relay among the available relays is crucial to improve the performance of the cooperative communication network.

- While relay selection can be carried out proactively or reactively, proactive relay selection is efficient as it consumes less energy.

- It is relevant to consider any relay selection in terms of throughput performance as a performance metric as this value illustrates the effectiveness of the data transmitted over the cooperative communication network.

- The inherent assumption in the cooperative communication appears to be that the relays will cooperate and will provide fool-proof integrity protection for cooperative communication.

- Malicious nodes can compromise the security in cooperative communication and cause the cooperation to cease. Consideration has been given, to date, only for *detection*-based techniques. It is worthwhile to consider and implement *prevention*-based techniques to prevent or mitigate the activities of malicious nodes.

- Available authentication processes have some drawbacks when used in cooperative communication due to the nature of the cooperative communication network.

- Joint authentication and QoS for cooperative communication networks has not been considered in existing work.

- The nodes in cooperative communication, i.e., source, destination, and relays, are not able to confirm that the signal had not been tampered during transmission.

In order to address the above problems, we propose an efficient and easily implementable scheme in this thesis.

1.3 Research Objectives

The main objective of our research is to develop a security-enabled relay selection scheme to select the best relay in order to facilitate a higher secured throughput through the cooperative communication network. More precisely, we want to:

- Evaluate the existing relay selection techniques in cooperative communication and assess whether security has been considered for relay selection.
- Evaluate the security issues gaining prominence in cooperative communication.
- Propose a *prevention*-based security technique to be used in opportunistic relaying so that our proposed scheme acts as the front line of defense and selects the best relay prior to data transmission.
- Compare the results of our proposed scheme with the results of the conventional relay selection scheme to evaluate the effectiveness of our proposed scheme.

1.4 Thesis Contributions

Based on these above objectives, we advance a *prevention*-based security technique and use it to select the best relay among the available relays in an opportunistic relaying scheme. This proposed "Joint Authentication and QoS Scheme (JAQS)" selects the relay that has the maximum secured throughput and is also security enabled as the best relay. Some distinct features of JAQS include:

- The JAQS selects proactively the best relay for a cooperative communication network to aid the transmission between the source and the destination, while taking into account both end-to-end and hop-by-hop authentication and integrity protection.

- The JAQS expands on the conventional relay selection scheme that currently uses outage capacity as the selection measure by deriving bit error rate and packet error rates and arriving at closed-form secured throughput equations. The best relay is the one that has the highest throughput QoS, and as a result, the proposed scheme improves the overall performance of the network.

- Throughput equations for JAQS have been formulated catering to both direct communication and communication through a relay, and has been derived to take into consideration the different Automatic Repeat reQuest (ARQ) error control retransmission schemes.

- The JAQS makes use of an authentication protocol, which is based on hash chains and Merkle trees, and adapts it to apply in cooperative communication networks in order to attain authentication and integrity protection.

- The JAQS offers end-to-end as well as hop-by-hop authentication and integrity protection to confirm the identity of the nodes and verify that the message received from a node is complete and has not been tampered with during the transmission process.

- The number of leaves (or data blocks) in Merkle tree is optimized under an integrated approach for different packet sizes as it is an important parameter in the authentication protocol.

- The JAQS is distributed and is proposed for a two-hop relay channel with three nodes, i.e., source, destination, and a relay, with the relay selected proactively among multiple intermediate nodes.

More detailed information on our scheme is presented in Chapter 3.

1.4.1 Submitted Papers

Based on this work, the following papers have been submitted:

- R. Ramamoorthy, F. R. Yu and H. Tang, "Combined Authentication and Quality of Service in Cooperative Communication Networks," submitted to the *Sixth IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom)'2010*, Hong Kong, Dec. 2010.

- R. Ramamoorthy, F. R. Yu and H. Tang, "Combined Authentication and Quality of Service Design in Cooperative Communication Networks," submitted to *IEEE Trans. on Wireless Commun.*, Sep. 2010.

1.5 Thesis Organization

The rest of the thesis is organized as follows.

- Chapter 2: In this chapter titled "Background and Related Work", we describe the research background of this thesis, where we introduce the concepts of cooperative communication, opportunistic relaying, security issues in cooperative communication, authentication, etc., and point out the related work that has been carried out in these areas.

- Chapter 3: In this chapter titled "Proposed Joint Authentication and QoS Scheme", we describe our proposed scheme in detail by presenting the system model, the equations for outage probability, outage capacity, and bit error rate (BER), the throughput in our authentication process by deriving throughput-specific equations, and the relay selection process using our proposed scheme.

- Chapter 4: In this chapter titled "Simulation Results and Discussions", we provide the simulation results on our proposed scheme and present discussions

comparing our results to the conventional relay selection scheme based on outage capacity.

- Chapter 5: This chapter wraps up this thesis by presenting our conclusions and highlighting areas for future work.

Our simulation program is presented in Appendix A.

Chapter 2

Background and Related Work

In this chapter, we present the background for this thesis by looking broadly at cooperative communication, the issues of cooperative communication in ad hoc networks, opportunistic relaying, the security issues that affect cooperative communication differentiating between the *detection*-based and *prevention*-based techniques, and describe the importance of authentication and integrity protection. From the literature, we also submit the related work that has been carried out and ideas proposed in these areas, where we see that *prevention*-based techniques appear to have been largely ignored in the discussion connected with security in cooperative communication. We have considered our background with reference to a classical relay channel with three-nodes and two-hops comprising of a source, a destination, and a relay.

2.1 Cooperative communication

Cooperative communication or cooperative diversity has gained popularity in the recent years because of the ability to achieve spatial diversity from single-antenna nodes thereby improving system capacity, coverage, throughput and reliability mitigating the effects of fading. This makes use of the broadcast nature of the wireless medium, as the adjacent nodes overhear the signals transmitted by the source and

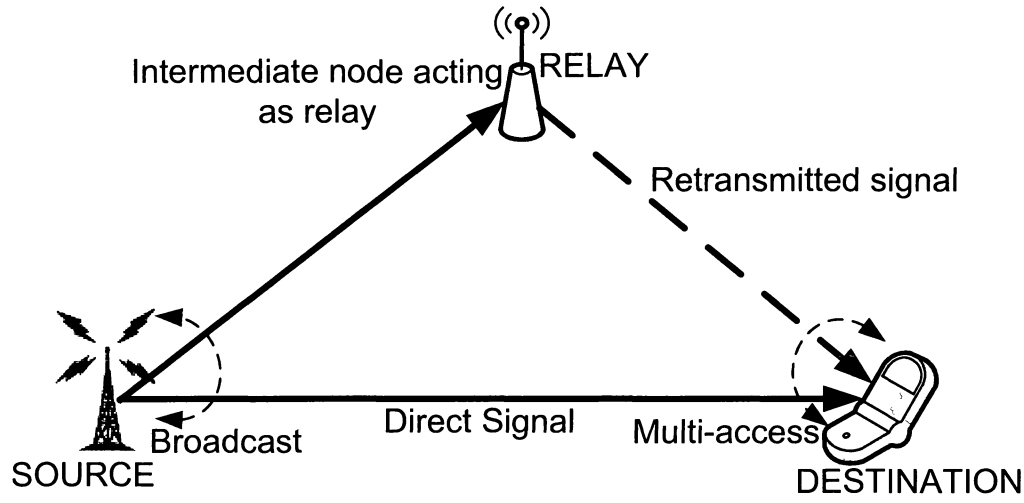

Figure 2.1: Three-Node cooperative communication model.

assist the transmission by relaying the overheard messages to the destination. Cooperative communication is a way in which each wireless user transmits not only its own information, but also act as an assisting agent, called relay, for the other user [5, 6]. Figure 2.1 shows a simple cooperative communication system. The communication takes place in two stages. In the first stage, the source broadcasts the message to the destination, and the destination and the relays receive the message. In the next stage, the relays that overhear the signal, or a subset thereof, re-transmit the same message to the destination. The destination, then, combines the signals received from both paths, i.e., directly from the source and from the relays, thus achieving spatial diversity. Cooperative communication eliminates the need to have multiple antennas at each node, and the single-antenna node shares its antenna to create a virtual multiple-input multiple-output (MIMO) environment acting both as a transmitter and a relay. The spatial diversity is achieved as the destination receives and combines two or more versions of the signal and this is accomplished through cooperation at the physical layer [7].

While MIMO communication system provides significant improvement in link reliability and spectral efficiency through the use of multiple antennas at the transmitter and/or receiver side and have been widely deployed in cellular applications, particularly in base stations, it is not always feasible to use MIMO in mobile devices due to size and power constraints, such as in cellular mobile devices or wireless sensor and ad hoc networks. However, cooperative communication achieves the spatial diversity without the need to deploy multiple antennas.

The constraints affecting system performance in wireless channels such as channel quality and resource constraints can be avoided by getting the users to share resources and collaborate in transmitting each other's signals. As stated in [8], cooperative communication exploits the spatial diversity inherent in multiuser systems by allowing users with diverse channel qualities to cooperate and relay each other's messages to the destination. Each transmitted message is passed through multiple independent relay paths and thus, the probability that the message will fail to reach the destination is significantly reduced. Transmitting independent copies of the signal generates diversity and can effectively combat the deleterious effects of fading [6]. Even if the fading is severe between the source and the destination, the signal can be received by the destination through the relay. The desired quality of service (QoS) can be achieved by users experiencing deep fade by utilizing quality channels provided by the other relaying nodes. The key is to get the relays to cooperate and add coherently the multiple independent faded signals at the destination, analogous to the traditional maximal ratio combining (MRC) in MIMO [9]. This combining can be achieved through various means such as pre-coding, orthogonal transmissions, and a maximal-ratio-combiner, or through distributed space-time codes.

Although cooperative communication forms a virtual MIMO system, it is different from the classical MIMO system and they both have contrasting characteristics [10]:

- MIMO uses multiple antennas, but in cooperative communication, each nodes has only a single antenna.

- In MIMO, multiple terminals transmit to the destination at the same time and frequency. This is not the case in cooperative communication as the relay receives the transmitted signal from the source and then, subsequently retransmits to the destination.

- Antenna selection in cooperative communication is more onerous as the number of available relay nodes are not known and they vary with time. In addition, the usefulness and the effectiveness of the relay is unknown as this depends upon the channel conditions.

- Cooperative communication requires better coordination due to the distributed nature and appropriate protocols to regulate the traffic and this can take up precious network resources.

- The role of a node in cooperative communication is multifold as it can either be the source, destination, or a relay, and it has the capability to send its own information and also forward other user's information.

The seminal work on cooperative communication was carried out by Cover and El Gamal. They discussed different ways through which a relay can assist the transmission and evaluated the capacity results for degraded relay channel in [11]. Their work was built upon Van der Meulen's paper on communication channel with three different terminals, which can be considered as a classical relay channel with a three-node network comprising of a source, destination, and a relay [12]. While the capacity of the relaying framework exceeded the capacity of a direct link, there are limitations to their model as they did not consider wireless fading channel and power loss/gain. However as stated in [6], recent work in cooperation has taken a different emphasis

motivated by the desire to not consider cooperation exclusively as only a relay problem. In this regard, [13] proposes a very simple and effective user cooperation protocol to boost the uplink capacity and lower the uplink outage probability for a given rate. The simple cooperative protocol has been extended to contemplate the concept of diversity in a fading channel and incorporate the fact that the nodes act both as a source and as a relay [14]. [15] provided a conceptual and mathematical extension to [13] and showed noticeable diversity and outage gains through their energy-efficient multiple access relaying protocols in comparison with direct communication.

Cooperative communication offers significant performance gains in terms of link reliability, spectral efficiency, system capacity, and transmission range [9]. [16] states that sharing power and computation with neighbouring nodes through cooperative communication can lead to savings in overall network resources. In cooperative communication, a positive trade-off is observed with respect of coding gain (i.e., the useful bit rate) and transmit power. On account of cooperative diversity, there is a noticeable increase in the channel code rate due to an improvement in spectral efficiency for each user although the user transmits its own signal and also its partner's signal. Likewise, a net reduction in the baseline transmit power is observed on account of diversity gain, although more power might be required for each node as it transmits for both the users. Using cooperative communication, the achievable rate and the error rate performance is seen to be significantly higher than for non-cooperative communication, with the cooperative communication rate double the rate of the non-cooperative mode [5]. In [7], it is stated that cooperative transmission can improve the channel capacity significantly and has a great potential to improve wireless network capacity. [6] shows that cooperative communication provides substantial improvement in error rate performance even while the interuser channel quality is poorer than the uplink channel. Cooperative communication is a cost effective solution, and also enables

users at shadow coverage regions to overcome capacity problems and avail equal QoS to all users [2]. [3] shows that cooperative diversity protocols result in large power or energy savings.

The transmission of information between the source and the destination through the relay nodes is made possible through the use of amplify-and-forward (AF), decode-and-forward (DF) and coded cooperation communication schemes. Apart from these three schemes, there are also other variants or hybrids derived from these schemes [17]. The relay nodes forward signals to the destination based on any of the above schemes. At the destination, rather than considering the relayed signal as an interference, the relayed signal is combined with the original direct signal in time, frequency, or spatial domain [18].

- Amplify-and-Forward: The relay simply amplifies the noisy signal received from the source and retransmits it to the destination. This scheme suffers from performance losses at low signal-to-noise ratios (SNRs) since the noise at the relay also gets amplified [19, 20].

- Decode-and-Forward: The relay decodes the noisy signal received from the source, re-encodes it and retransmits the message to the destination. This adds some complexity, but exhibits better performance than AF in low SNRs. This scheme is also termed as Detect-and-Forward. [3, 21, 22] deal with single relays forwarding the signal to the destination and [23–25] deal with multiple relays forwarding the signal simultaneously to the destination.

- Coded Cooperation: This integrates cooperation into channel coding by sending different portions of each users code word through two independent fading paths. While each user tries to transmit incremental redundancy for its partner, if it is not feasible, the system reverts to non-cooperative mode. There is no feedback between the users and is managed automatically through the code design.

There are different cooperative diversity protocols available that involve carrying out different types of processing at the intermediate relaying nodes and requiring different types of combining at the destination node. They include fixed relaying, selection relaying, incremental relaying, and opportunistic relaying with some variants that are hybrids of one another [26].

- Fixed Relaying: At all times, the relay node forwards the signal received from the source to the destination irrespective of the channel condition between the relay and the destination. Both standard AF and DF communication schemes fall under this category [3].

- Selection Relaying: The retransmission from the relay to the destination is dependant upon the channel condition between the relay and the destination. If the channel quality is bad, the relay does not forward any signal to the destination.

- Incremental Relaying: This makes use of feedback information of the link condition and whether the transmission is successful or not at the destination. Based on the feedback received by both the source and the relay nodes, the need for retransmission is decided [27].

- Opportunistic Relaying: This requires the selection of the best relay node amongst the multiple-relays that are available in the network to transmit the signal between the source and the destination. In a conventional three-node relay channel, this scheme selects the best relay out of all the intermediate relay nodes to be used for data transmission rather than using all the relays.

In this report, we consider opportunistic relaying in detail by examining the case of a two-hop network with one intermediate relay node, selected amongst multiple relays,

between the source and destination. A schematic representation of the opportunistic relaying scheme is presented in Figure 2.2. Consider the source and destination nodes with multiple-relays located between them. In the first stage, the source broadcasts the signal to the destination and is overheard by the multiple-relays. A best relay is selected amongst the multiple-relays and this alone forwards the received signal to the destination, where the two signals are combined. There are two approaches within the opportunistic relaying scheme, proactive where the relay selection is carried out prior to the data transmission by the source and reactive where the relay selection is carried out after the source has broadcast the data to the destination and relays [28]. Opportunistic relaying is beneficial mitigating performance loss at low SNR values as the use of multiple-relay transmissions in a relay channel could lead to a loss of bandwidth efficiency [29]. [30] shows that that cooperative communication is useful and that opportunistic relaying with single-relay selection significantly outperforms multiple-relay transmissions. Further information on opportunistic relaying is presented in the subsequent section.

Cooperative communication is applicable to both infrastructure-based networks, where the physical and/or logical infrastructure is available even prior to execution such as in cellular systems, WLANs (wireless local area networks), or WMANs (wireless metropolitan area networks), and infrastructure-less networks, where the physical and/or logical infrastructure may not be available or becomes available only after deployment such as in ad hoc and WSNs (wireless sensor networks). To maximize the advantages offered by cooperative communication, research is currently continuing to integrate cooperative transmission into cellular, WiMAX, WiFi, Bluetooth, ultra-wideband (UWB), cognitive radio, ad hoc, and sensor networks [7]. Recently, cooperative relaying has been considered as a promising technique, and has been involved in the standard of IEEE 802.16j [7, 31] and is also expected to be integrated

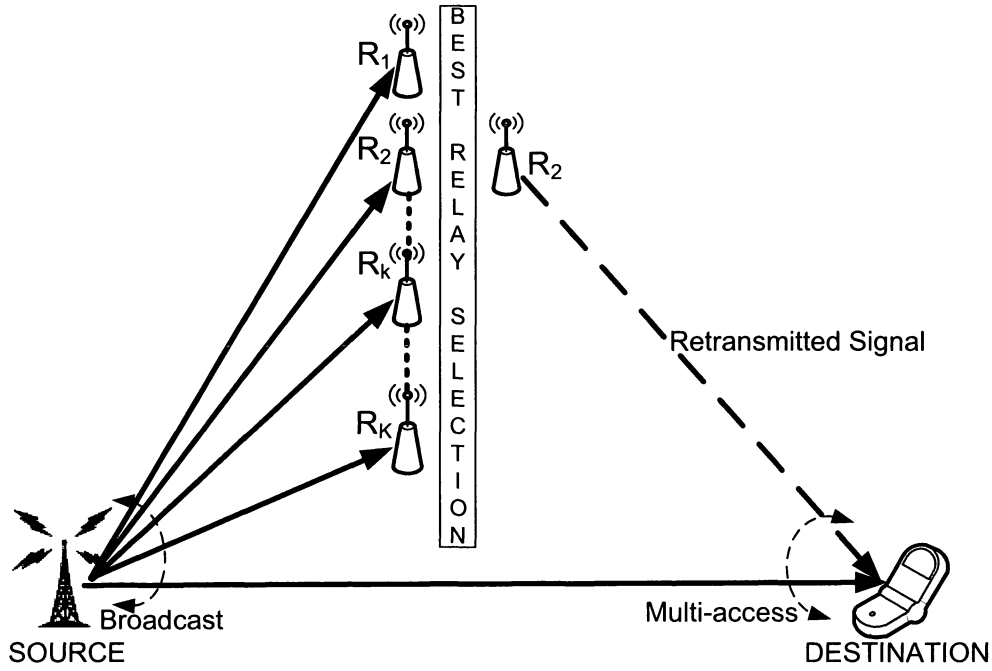

Figure 2.2: Opportunistic Relaying in a two-hop network.

in 3GPP-LTE multi-hop cellular networks [32]. IEEE 802.16j aims at defining a multi-hop solution for WMANs by expanding the standard IEEE 802.16 model of direct communication between the mobile station and base station through the use of relaying stations. Cooperative transmission and relaying is one of the important features provided by the IEEE 802.16j standard [19]. Recently, attention is also focused on cooperative multi-hop cellular networks (MCNs) as it can reduce the number of base stations and access points and improve the overall throughput performance [19]. While [6] and [14] take the view that cooperative communication will be more suited for ad hoc and WSNs, we are of the view that the concepts and techniques in cooperative communication are equally suited and applicable across all kinds of wireless technologies.

The inherent nature of the ad hoc networks with its lack of fixed infrastructure and of a central unit for controlling, and using direct node-to-node communication

or using relaying node to communicate makes ad hoc networks a prime candidate for cooperative communication. Cooperative communication in ad hoc networks provides higher throughput and robustness to channel variations for both the transmitting and relaying nodes [14].

2.2 Ad Hoc Networks

Wireless ad hoc networking has recently attracted growing interest and has emerged as a key technology for next-generation wireless networking [33]. A wireless ad hoc network is a decentralized wireless network with no pre-existing fixed infrastructure and requiring nodes to forward data to other nodes on a dynamic basis depending on the status of the network. They are normally decentralized in nature having no central control or command. The inherent features of ad hoc with its minimal configuration, quick deployment, self-configuration and self-organization make it a prime candidate for use in military applications and in emergency situations like natural disasters. Based on the nature of application, they could be classified as mobile ad hoc networks (MANETs), wireless mesh networks, and wireless sensor networks. In this report, we restrict our focus to cooperative communication in MANETs.

A MANET is a temporary infrastructureless network formed by a set of wireless mobile hosts that dynamically establish their own network *on the fly* without relying on any central administration [34]. Each device in MANET is free to move independently in any direction, and will therefore frequently change its links to other devices. A MANET node can function both as a network router for routing packets from the other nodes as well as a network host for transmitting and receiving data. On account of the distributed nature and lack of centralized command, MANET nodes cooperate with each other to achieve the common goal. Accordingly, cooperative communication

or diversity arises naturally in ad hoc networks and this enables greater power savings with cheap, simple and mobile nodes, while supporting decentralized routing and control algorithms [35, 36]. AF cooperative strategy is suggested for ad hoc networks on account of its simplicity and addressing the critical power constraints [37].

MANET imposes constraints on the network architecture in terms of functional physical layer communication link originating from only one transmitter and the concurrent transmission from multiple transmitters as this can potentially result in interference, collision, and distortion at the destination. However, cooperative communication is not affected by these constraints, and therefore, there is a great deal of room for design of network architectures in MANET that integrates cooperation [38].

Scaglione et al [38, 39] proposed two MANET models using cooperative communication and showed their advantages in flexibility compared to the standard MANETs. In one of the models, cooperative transmission is centrally activated and controlled by cluster access points and all nodes communicate through this access point, which handle routing to other clusters using multiple gateway nodes and thereby provide significant cooperative gains compared to the single gateway solution. Better links translate into better network connectivity compared to multi-hop solutions. In the second model, a random source conveys extra control information and link parameters in the message to enable recipients to self-select and form a random cooperative cluster in a MANET. The nodes in the cluster can rely upon the synchronization data available in the source packet.

2.3 Opportunistic Relaying

Opportunistic relaying or Orthogonal Opportunistic Relaying (OREL) or Selection Cooperation [9, 10, 40] demands the selection of the best relay node among the multiple-relay nodes that may be available for the data transmission between the

source and the destination. It is inefficient to use all the available relays for the data communication as the system requirements increase and become complex when the number of relay nodes expand with all adjacent nodes participating in the communication. Therefore, the best relay should be selected to transmit the message to the destination. Accordingly, relay selection amongst the available relays is crucial in improving the performance of cooperative relaying [17, 40–47].

Bletsas, Lippman, and Reed first introduced the concept of opportunistic relaying with orthogonal use of time/frequency in [48]. According to [10], the term opportunistic relates to the dynamic exploitation of wireless channel changes, both in time (due to the nonconstant wireless channel) as well as space (due to several potential relay paths). Bletsas et al took a radically different approach by devising a simple distributed scheme to select a best relay on the basis of the best channel path from source to relay as well as relay to destination to address the problem of efficient cooperative diversity in the presence of multiple-relays . The advantage of this scheme is its simplicity with no requirement for prior knowledge on the network topology or the wireless channel conditions and its suitability for distributed implementation, with the selection based only on the instantaneous channel measurements.

Under the scheme proposed by Bletsas et al [48], the factor that influences the selection of the best relay is the state of the wireless channels between the source and the relays, and between these relays and the destination. As illustrated in the flowchart presented in Figure 2.3 [10], the source initiates communication by transmitting a test sequence comprising a ready-to send (RTS) packet towards the relay and the destination, which aids the relays to estimate the signal strength towards the source. The destination responds with a clear-to-send (CTS) packet towards the relays and the source, which correspondingly aids the relays to estimate the signal strength towards the destination. Through this, both the forward and the backward

signal strengths are estimated, and the relays individually initiate a timer with speed inversely proportional to the signal strength. The relay with the best channel condition will expire the time first and this triggers a flag packet making it obvious to all the other nodes that the best relay has been found. As a consequence, the other relays stay away from the data transfer. In the case of relays not able to listen to each other, the source or destination can broadcast details about the best relay so that the other relays do not get involved in the data transfer. This scheme consequently requires time synchronization between the source, the destination, and the relay nodes. Based on the above scheme, Zou et al [49] proposed a heuristic relay selection protocol.

The state of the wireless channel can be decided on the basis of various measures, such as average signal strength [50, 51], distance [52–55], instantaneous signal strength [41, 56] or measured SNR [57, 58]. This process of relay selection is carried out for each time slot or transmission process, comprising of best relay selection and the subsequent data communication, and the exercise is repeated and a new relay selected at the beginning of the next time slot or whenever there is a change in the channel conditions. While it is evident that the fastest method would be to exploit the instantaneous signal strength, in all cases, the intermediate relays have to continually keep the wireless channel appraised regarding when the wireless channel can be assumed to be constant based on the carrier wavelength, mobility speed, and the coherence time of the wireless channel. Relay selection has been proposed independently for both AF [40, 59] and DF [40, 43] communication schemes.

As stated above, the relay selection can employ both proactive [28, 60, 61] or reactive [57, 62] means. A schematic representation of these two methods is presented in Figure 2.4. Proactive relay selection involves selecting the best relay before transmitting the data from the source to the destination. This restricts the requirement for all of the intermediate relays to listen to the source and saves on the energy that

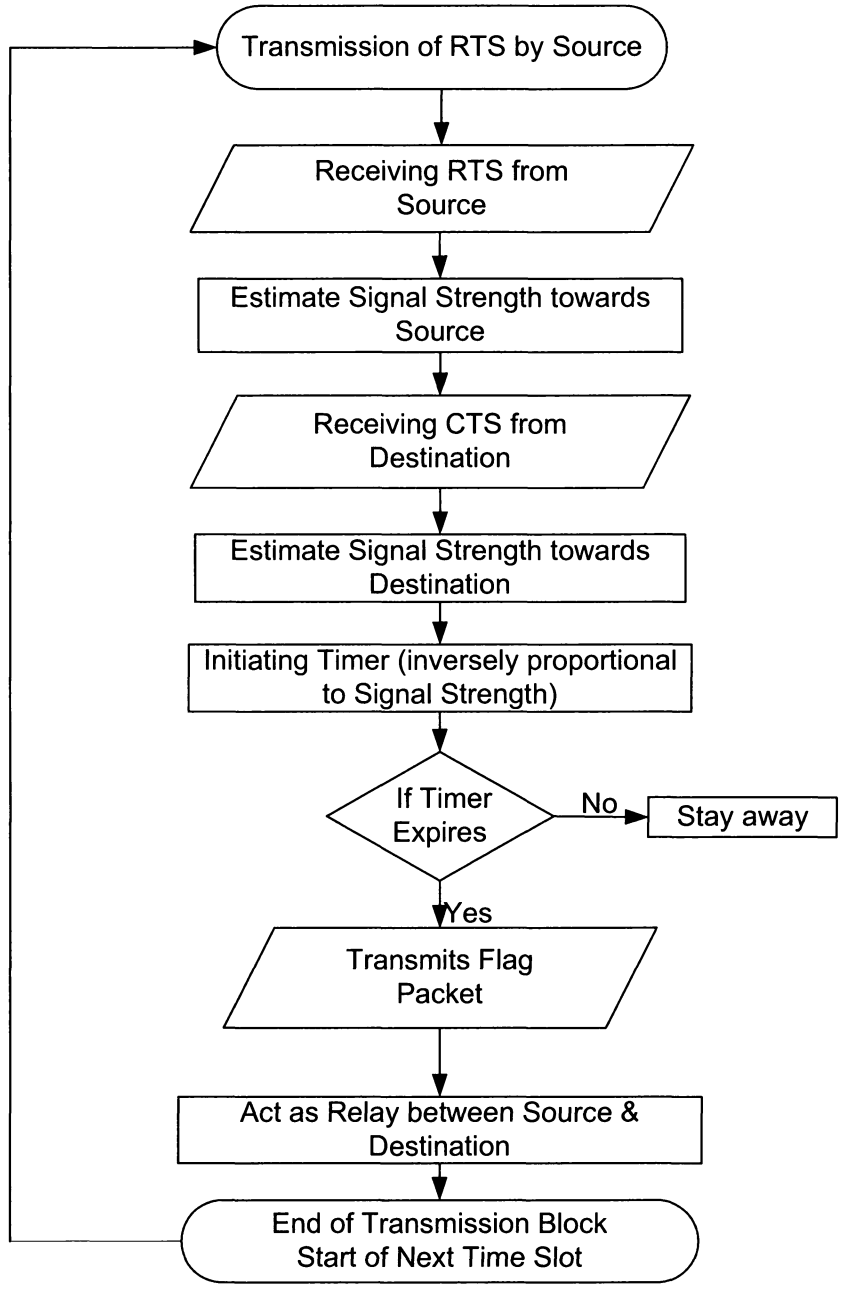

Figure 2.3: Flowchart for an Opportunistic Relay.

would have been unnecessarily spent by the rest of the relays for message reception. Only the selected best relay is required to listen to the transmission and therefore, only a small quantity of energy would be expended for this purpose. Using the proactive scheme, the total energy requirement for the network is not increased with an increase in the number of relays. Proactive schemes can be facilitated with either regenerative (decode-and-forward) or transponder (amplify-and-forward) relays [10]. Reactive relay selection involves all the intermediate relay nodes taking part in the cooperative communication by listening to the signal transmitted by the source in the first phase. Only after the receipt of the signal by all of the relays, the best relay is selected and this relay alone carries out the retransmission to the destination. However, as all the relays listen to the signal broadcasted by the source, energy is expended, and with the energy used for reception comparable to the energy used for transmission, the energy utilization in reactive mode is considerably higher in comparison to the proactive mode. In addition, the energy consumption in the network increases in direct proportion to an increase in the number of relays. Despite the improved transmission energy savings offered by the reactive relay selection scheme through the single broadcast to multiple nodes, reception energy expenditures may become an overkill for cooperative communication, especially in battery-constrained networks [10].

In this study, we look at proactive opportunistic relay selection, which is carried out through the following schemes:

- Fixed Selective Decode-and-Forward (FSDF) combined with direct link: The best relay is selected and the message transmitted by the source is decoded, and if the decoding is successful, the relay forwards the information to the destination. The destination uses MRC to combine the signals from the source and the relay nodes [60, 63].

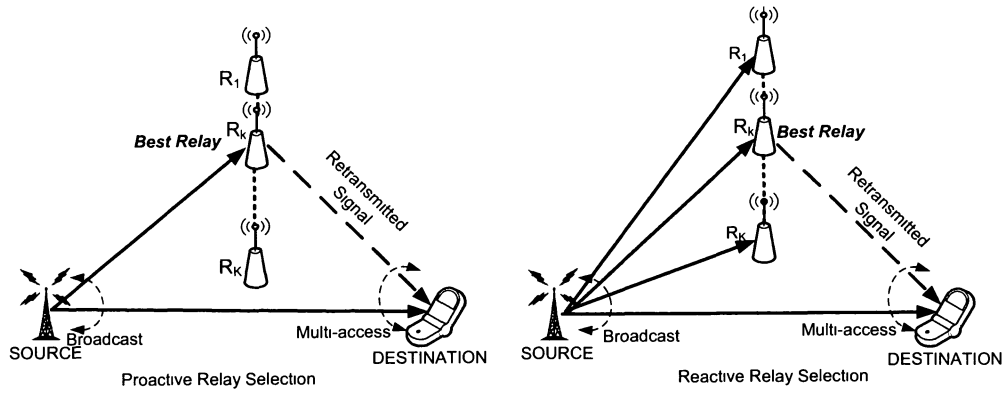

Figure 2.4: Proactive and Reactive Relay Selection.

- FSDF without direct link: This is similar to the above, but the destination does not receive direct communication signal from the source [28].

- Smart Selective Decode-and-Forward (SSDF): This makes use of the selected best relay only if it is beneficial for cooperative communication, and if not, only direct communication is used [61]. This model is also called as Smart Cooperation (SC) [61].

The bit error rate (BER) or outage probability and outage capacity are normally used as performance metrics in slow fading channels. BER is the percentage of bits that have errors relative to the total number of bits received in a transmission, and is an indication of how often data had to be retransmitted because of an error. Relay selection schemes based on the performance of BER are discussed in [49, 58].

Wireless channels experience fading and this affects system performance as the signal components received over different propagation paths are combined in a destructive manner. The slowly fading channels do not guarantee reliable communication for any transmission rate and have zero capacity. The error probability is due to the deep fade levels and the channel noise. When the wireless channel experiences a deep fade and the channel cannot support the transmission rate, the channel is said to be in outage. If the channel is in outage, the error probability is almost equal

to 1. If there is no outage, the error probability will be very small. Accordingly, the outage event dominates the error event and probability of error is approximately equal to probability of outage [64]. Therefore, outage probability is the probability that the channel cannot support the transmission rate when the mutual instantaneous information between any two nodes falls below the transmission rate leading to unsuccessful data transmission, and outage capacity is the largest rate of reliable communication at a certain outage probability. Currently, the conventional relay selection schemes in cooperative communication have been proposed on the basis of outage capacity [28, 42, 61].

2.4 Security Issues in Cooperative Communication

Although cooperative communication brings in significant benefits, it also raises serious security issues on account of its decentralized system, dynamic nature, and self-organization. Cooperative communication is designed with the assumption that the nodes always help each other and cooperate in a socially efficient manner. However, this assumption may not be valid as a node might misbehave for selfish or malicious intentions. A node could either be the source, destination, or a relay, and its role depends upon the requirement. Therefore, the security concerns in cooperative communication is similar to the security concerns in other scenarios that also require collaboration among distributed entities such as in MANETs and peer-to-peer (P2P) networks.

Cooperative communication depends primarily on the behaviour of the nodes and if they behave opposite to what they are expected to do, they can affect the performance of the system and raise serious security issues. For example, it is possible

for malicious nodes to join the network as relays and relay unsolicited, unwanted, modified or falsified messages to the destination thereby degrading the performance of the system. Malicious nodes can also send arbitrary information instead of the correct information and the other nodes may pass on the information without being aware that the information has originated from a malicious node. A malicious behaviour is characterized by a relay node that violates the cooperation strategy with the objective of disrupting communication between source and destination at the expense of its own power. Moreover, malicious nodes can also feed false information about the channel state to the source and destination so that they would be selected as the relays to be used for forwarding the message to the destination. As a result, if the source and destination cannot hear one another, the malicious relays can provide false acknowledgements to the source and spoof the source into thinking that its message is received by the destination. In this case, the source would continue to transmit messages which can then prolong the exhaustive attack by the malicious relays. In addition, some nodes can act in a selfish manner to conserve their own energy or display security and privacy concerns leading them not to cooperate and relay information from other nodes thereby discouraging cooperation. In the absence of a mechanism to detect and resolve these issues, cooperative communication can exhibit severe performance degradation and dissuade cooperation.

The following characteristics of cooperative communication make it vulnerable to attacks and discourage collaboration between the nodes, which is adapted from [34]:

- Possibility of Free-riders: Although relay nodes are required to expend power and bandwidth resources to provide services for the cooperating partner, there is no mechanism to enforce cooperation. This may lead to the existence of free-riding nodes that may refuse to cooperate but reap benefits to their advantage. Therefore, well-behaved nodes may refuse to relay for their potential partners

without the assurance that the partners will reciprocate.

- Absence of Centralized Control: Nodes are independent and are free to roam and form transient relationships. No centralized host relationship is possible in this network and it is not possible or practical to distinguish relay nodes in advance as reliable or non-reliable nodes. There is no mechanism to provide incentive for the cooperation or to tackle misbehavior.

- Frequent Topology Changes: Due to the behavioural diversity of different nodes, it is hard for the nodes to put in effective measures to prevent any kind of possible malicious behaviours. There is no fixed form or shape to the network and changes are possible on a frequent basis. As cooperative relaying involves more than single hop, all the nodes have to be reliable.

- Nature of Wireless Medium: Wireless medium is inherently vulnerable as no physical access is required and both legitimate and malicious nodes can access the network and any node can be attacked or compromised. Therefore, all the nodes have to be defended.

- Resource Constraints: The relay nodes are small and have limited power resources leading to the possibility of attackers carrying out energy starvation or sleep deprivation attacks targeting, disconnecting them, and partitioning the network. It will also be difficult to implement high complex security solutions.

- Scalability: Any security solution should be scalable to cater to the dynamic nature of the incoming relays and the expansion of the network.

Therefore, it is quite apparent that security is essential for the widespread adoption and spread of cooperative communication. A good security system should have the goals of confidentiality, i.e., protecting the information, integrity, i.e., any change

in the information should be done only by authorized entities and authorized mechanisms, and availability, i.e., information is available and accessible to authorized entities [65]. The attributes of a good security regime related to the above security goals as defined by the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) is given below [65–67]:

- Data Confidentiality: To make sure that the data can not be accessed by unauthorized users or nodes who are not the designated recipients, which could be generally achieved through cryptography.

- Data Integrity: To conform that the data has not been altered or destroyed during the transmission process and to detect any data modifications, which could be generally achieved through the use of hash functions.

- Authentication: To prevent any impersonation of a user or node in a network and assist in correct identification of an entity. In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication) which generally is carried out through a central authority, but is difficult in the cooperative communication network due to the lack of centralized control. In connectionless communication, the authentication is on the source of the data (data origin authentication). Data origin authentication is the security service that enables verification of the originator and validity of a message. Verification is therefore possible at a later time to check whether the content of a message, or more generally, of data is still exactly the same as created by its originator [67].

- Non-repudiation: To prevent nodes or users from rejecting the ownership of their messages by verifying that they were sent only with the node's credentials, which could be normally achieved through public key cryptography.

- Access Control: To prevent unauthorized use of network services and system resources, and to provide protection against unauthorized access to data.

A variety of security mechanisms have been invented and are currently available to counter malicious attacks. Based on the mode of application, they could be classified as preventive and reactive mechanisms, or as *prevention*-based and *detection*-based techniques on the basis of their timing and the targeted area of their application.

- Preventive Mechanism: This works as the first layer of defense and includes conventional authentication and encryption schemes based on cryptography, hash chain, access control and digital signature.

- Reactive Mechanism: This operates as the second layer of defense to counter malicious attacks and misbehavior that had bypassed the initial preventive mechanism and includes the adoption of statistical-based intrusion detection systems to detect any potential anomalies.

- Prevention: It is the front line defense and works to prevent any attacks or unauthorized actions by malicious or adversarial nodes.

- Detection: This is to make sure that any malicious, adversarial, or misbehaving node that had entered the network can be traced and separated from the network. This prevents the nodes from acting selfishly and punishes any misbehaving nodes.

Whereas all these security concerns exist in cooperative communication, the majority of the work and research in cooperative communication has so far been focused only on communication efficiency, capacity analysis, protocol design, power control, relay selection, and cross layer optimization [7]. However, in the literature, there are

few studies that discuss the security considerations for the cooperative communication network emphasizing the *detection*-based schemes.

[68, 69] discuss a *detection*-based technique with a cross-layer tracking scheme to trace adversarial nodes that transmit garbled signals to the destination by using adaptive signal detection at the physical layer along with pseudorandom tracing symbols at the application layer. A security regime after opportunistic selection of two relays is presented in [70] with the first relay acting as a conventional node and the second relay creating intentional interference from the eavesdroppers. In addition, a hybrid security scheme switching between jamming and non-jamming protection is also proposed. In [71], a noise-forwarding strategy is proposed by having the relays to act as trusted third parties by sending codewords independent of the message sent by the source so as to confuse the eavesdropper. An approach to detect selfishness and enforce distributed cooperation based on monitoring neighbors to identify a misbehaving node that does not cooperate during data transmission is proposed in [72]. In [73] and [74], an additional punishment mechanism to isolate the misbehaving and non-cooperating nodes has been proposed. [75] proposes cooperative jamming to enable secure communication to take place using an untrusted relay wherein the destination or other node jams the relay and uses the jamming signal as side information. A physical layer approach for AF nodes to safeguard the network from eavesdroppers is proposed in [76] by designing the system to accentuate the secrecy capacity and presenting closed-form solutions for optimization. A similar approach for DF is presented in [77], and both approaches involve relay nodes transmitting a weighted version of the noisy signal received from the source and optimizing the weights to maximize secrecy capacity or minimize transmit power. A similar scheme taking into account cooperative jamming is proposed in [78] with a relay having multiple antennas, assigning weights to the antenna elements and maximizing system

secrecy by optimizing closed-form equations. [79] combines these three cooperative schemes of AF, DF, and cooperative jamming and the concepts outlined in the earlier papers. [80] proposes two new security schemes in the media access control layer to address the security concerns arising in cooperative communication with emphasis on IEEE 802.11 architecture. [81] discusses methods to prevent eavesdropping through a cooperative secrecy setup, where relay nodes facilitate secure communication between source and destination. A statistical detection technique is proposed in [82] to mitigate malicious behavior by getting the destination to examine the relay's signal prior to applying diversity combining with the direct signal from the source. [83] proposes a low-overhead self-learning cooperative transmission scheme that solves problems connected with untrustworthy nodes and channel estimation errors by modeling a Beta function based on SNR and enabling the Beta function to be propagated from the source to the destination. [7] and [84] explores the question of trust and uses it to get the relays to collaborate.

Different from the above *detection*-based techniques, the *prevention*-based techniques, such as authentication, are crucial as the front line defense for integrity, confidentiality, and non-repudiation [85]. In the next section, we discuss a *prevention*-based technique with emphasis on authentication in detail.

2.5 Authentication

The above security issues show the importance of integrity of data and the need to have reliable relationship amongst the different nodes. For this purpose, authentication is important, with the consequent need to know exactly who we are talking to and making sure that the message received from a node is really the message that had been sent by that node. Authentication, therefore, supports privacy, confidentiality,

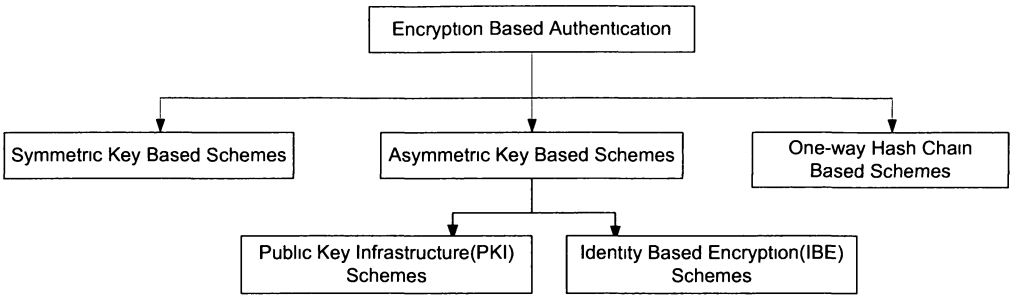

Figure 2.5: Classification of authentication schemes.

and access control by verifying and validating the information. All nodes in the cooperative communication network should be able to carry out the authentication, and therefore the *prevention*-based technique should allow for end-to-end and hop-by-hop authentication and integrity protection.

Authentication has been classified based on the authentication function (homogeneous and heterogeneous), the type of credentials (identity based and context based), and establishment of credentials (pre-deployed, derived and post deployed) [86]. In [87], the classification has been based on cryptographic algorithms, as cryptography plays an important role in any strong authentication scheme. This report follows a similar mode of classification as the key techniques such as public key infrastructure (PKI), identity based encryption (IBE), and one-way hash functions, and most of the models in literature fall under this approach. This classification is represented in Figure 2.5.

Symmetric Key Scheme: In symmetric encryption algorithm, both parties use the same unique secret key for both encryption and decryption. Both parties share the secret that is unique between these two nodes, and is not known to any other node. Each node stores the unique keys that define the encrypted relationships between itself and the other node. This scheme is simple and fast, and is less resource intensive on account of the reduced computational complexity. Symmetric-key ciphers have

higher rates of data throughput. However, this scheme is not scalable and is difficult to maintain for a larger network since it is hard to refresh the keys. The key must remain secret at both ends and must be changed frequently leading to the need to manage many number of key pairs for larger networks. Distributing the shared keys becomes a problem in networks that do not have any centralized control, such as in cooperative or ad hoc networks. Commonly used symmetric algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Kerberos assisted Authentication in Mobile Ad hoc Networks (KAMAN).

Asymmetric Key Scheme: In asymmetric encryption algorithm, different keys are used for encryption and decryption. This is based on personal secrecy. Each node in this network has two keys, a public key and a private key, with only the private key kept secret. They can be divided into:

- PKI Scheme: In this scheme, a node has both public and private keys. A certification authority (CA), which can be a trusted third party (TTP), validates the public key that is known to all and this is used to encrypt a message that can only be decrypted using the corresponding private key. This scheme is scalable by having the public key bound to a digital certificate. Traditional PKI-based authentication approach is gaining popularity in wireless networks. The distribution of the key does not require any secure channel as the digital certificate can be public, and the public/private key pair can be retained for a longer period of time. A small number of keys are sufficient for a large network. However, this approach is complex and requires high computation power and communication overhead. It is relatively expensive in terms of generating and verifying digital signatures which limit their practical application in cooperative communication networks where the nodes have limited power and computational capability. In addition, the very nature of cooperative communication with its lack of fixed

infrastructure makes it hard to interact through the TTP or to have a central repository for the digital certificates. The throughput rate is comparatively smaller than the symmetric scheme. Public-key cryptography facilitates key management and efficient signatures (particularly non-repudiation). Commonly used asymmetric PKI algorithms include RSA cryptosystem, Rabin cryptosystem, Elliptic Curve Cryptosystem (ECC), etc.

- IBE Scheme: This scheme is an adaptation of the PKI scheme. Asymmetric key with IBE approach was proposed to make key management easier through the use of a private key generator (PKG), which can be a TTP, generating a master public key known to public and a master secret key known only to the PKG. Encryption is carried out using the master public key and the recipients ID. To decrypt, a private key is requested through a secure channel from a PKG after authenticating through a CA. The pair-wise shared key is used for authentication. As in the other asymmetric approach, this scheme is also easily scalable, and it is up to the receiver to obtain the private key to decrypt as only the public key is generated based on the ID. As the identities are pre-approved in the PKG to receive private keys, this scheme provides for implicit and non-interactive pre-authentication among the network nodes. This approach is not computationally resource intensive as compared to PKI. However, as the public key is not bound to a digital certificate, this can give rise to possible key escrow problem and in addition, key revocation can be challenging. As like the PKI approach, this scheme is also not suited for cooperative communication on account of lack of centralized control in cooperative communication and the limited power and computational capability in the nodes. Commonly used asymmetric IBE schemes include Boneh/Franklin's pairing-based encryption scheme, Cocks's encryption scheme, etc.

One-Way Hash Chain Scheme: A one-way function, according to [88], is constructed on a secure encryption algorithm. [89] further explains the nature of one-way functions. Assuming that F is a one-way function acting on input ip, and if z is the result of $F(ip)$, the person who computed $z = F(ip)$ will be the only person knowing ip. If z is publicly revealed, only the originator of z can know ip. The creator of z, if required, can provide ip which will allow others to compute $F(ip)$ to arrive at z and confirm that it was created only by that party. The one-way function prevents any one from reversing the function and calculating ip from the value of z. A one-way cryptographic hash function is a procedure where a message can be hashed to a unique cryptographic hash value or message digest, and even a small change in the message would vary the hash value. Therefore, if the source hashes the information with his hash key, the destination having the same key and the hashed information as the source can regenerate the message digest and verify the claimed identity of the source. Cryptographic hash function is easy to use due to its simplicity in computing the hash value for any given message. It is impossible to break a hash value, modify a message without changing its hash, or find any two separate messages with the same hash value or message digests. Cryptographic hash function is used mainly for verification of message integrity, i.e., identifying if the message had been tampered or not by comparing the cryptographic hash values/message digests before and after transmission. Based on the the nature of the compression function, cryptographic hash functions are grouped as hash functions made from scratch (Message Digest (MD), Secure Hash Algorithm (SHA), etc.) or as hash functions based on block ciphers (Rabin scheme, Davies-Meyer scheme, etc.).

In case of data origin authentication and integrity protection in cooperative communication network, while public key cryptography and other asymmetric approaches will be able to provide the end-to-end authentication and integrity protection, the

computational complexity is high leading consequently to increased costs. Symmetric approaches of shared secrets and symmetric ciphers do not really permit authentication and integrity checking on hop-by-hop basis as forwarding nodes do not generally have access to shared secrets, and distribution of shared keys becomes a critical problem. In these circumstances, hash chains can be employed to meet the security requirements as they are simple and computationally efficient means of authenticating nodes in a network when tied to identities [90]. This could be used for authentication and integrity protection, particularly for on-path verification with high-volume data in cooperative communication networks. The computation of hash chains is several orders of magnitude faster than PKI.

A hash chain is formed by hashing a random seed variable θ multiple times using any cryptographic hash function. The resulting value serves as the input for the next hashing, and continues on until the desired length i is reached. A hash chain of length i is generated as $[\theta, H(\theta) = h_1, H(h_1) = H(H(\theta)) = h_2, H(h_2) = H(H(H(\theta))) = h_3, ..., h_{i-1}, h_i]$ with h_i as the *anchor* of the hash chain corresponding to the last hashed value for that hash chain. The hash chain can be computed only in this sequence, but the usage is from the opposite end, i.e., $[h_i, h_{i-1}, ..., h_3, h_2, h_1, \theta]$. The hash chain uses a one-way function where hashing h_i would not reveal h_{i-1}, but h_{i-1} can be hashed to arrive at h_i. To authenticate, the owner can initially provide the anchor h_i to a verifier, and for subsequent use, can reveal the next element of its hash chain, i.e., h_{i-1}, from which the verifier can easily confirm the authenticity of the owner. There are three different approaches to securely distribute messages using hash chain: one-time signature, which has large signature size and consequently computationally expensive, time-based approach, which has significant computational load and is not suited for hop-by-hop integrity protection, and interaction-based approach, which makes use of initial signature with delayed message disclosure.

Hash chains have been used successfully in different specialized authentication protocols. A broadcast authentication protocol based on loose time synchronization is proposed and presented as a timed efficient stream loss-tolerant authentication (TESLA) scheme [91], where one-way hash functions are used to authenticate data and control packets. However, this scheme does not provide hop-by-hop authentication. The computational overhead is also high due to the existence of network latencies and redundant hash elements, and has been rated as having poor throughput [92]. A lightweight hop-by-hop authentication protocol (LHAP) based on the principles of TESLA is proposed to carry out both packet authentication and hop-by-hop authentication, wherein intermediate nodes authenticate all the packets they receive prior to forwarding them [93]. However, this protocol is vulnerable to attacks and is not designed to prevent inside attacks. [94] presents a lightweight authentication protocol, again based on TESLA, utilizing an one-way hash function to provide effective and efficient authentication. However, this scheme also suffers from long latency and poor throughput, and is not designed to prevent insider attacks [90, 92]. To overcome the deficiencies, a hop-by-hop efficient authentication protocol (HEAP) is proposed to authenticate packets at every hop by using a modified hash message authentication code (HMAC) based algorithm along with two keys and dropping any packet that originates from outsiders. The distributed trust model is based on the assumption that no single node can be trusted and relied on, and requiring each packet to be authenticated at every hop [92, 95, 96]. While this protocol performs very well in comparison with the other protocols, it again suffers from its inability to prevent insider attacks and from not catering to end-to-end authentication. Apart from these, hash chains have also been successfully employed in various protocols like chained stream authentication (CSA), zero common-knowledge (ZCK), Guy Fawkes protocol, and weak identifier multihoming protocol (WIMP) [90], and has been suggested for

ad hoc [97] and sensor networks [98].

Although hash chains are uncomplicated to calculate and easy to use, they are not sufficient to prevent insider attacks by relay nodes. In order to provide both end-to-end and hop-by-hop authentication and integrity protection, an authentication protocol referred as adaptive and lightweight protocol for hop-by-hop authentication (ALPHA), which makes use of interaction-based hash chains and Merkle trees, has been proposed in [90]. Three models have been introduced, namely basic ALPHA, ALPHA-C, and ALPHA-M. While basic ALPHA and ALPHA-C are based only on interaction-based hash chains, ALPHA-M combines the interaction-based hash chains with Merkle trees.

The basic ALPHA uses three way packet exchange where the source and destination maintain their own separate hash chains. They initially exchange their respective hash chain anchors through an initial handshaking process (h_i^S corresponding to the anchor of the hash chain at the source, and h_i^D corresponding to the anchor of the hash chain at the destination). In the case of communication passing through a relay, the anchor information is also passed on to the relay. Subsequently, the source will send S_1 with a fresh element of its hash chain h_{i-1}^S and a message authentication code (MAC) or pre-signature calculated over the message m with the next undisclosed hash chain element. The destination acknowledges with an A_1 packet. Finally, the source discloses the key of the MAC/pre-signature h_{i-2}^S and the message m in the S_2 packet. When the destination receives S_2 packet, it can recreate the pre-signature and confirm that the calculated value is the same to the one received in the S_1 packet and thereby make sure that the message m had not been tampered with during the transmission. It can also confirm the value of h_{i-1}^S received in the S_1 packet by hashing h_{i-2}^S received in the S_2 packet. The actual message is transmitted only in S_2 while S_1 contains only the hashed output of the message. This allows the source/ destination

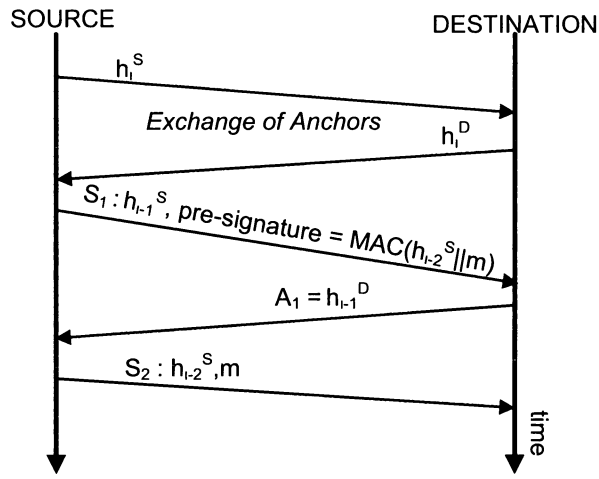

Figure 2.6: Basic form of ALPHA scheme.

and the intermediate relay nodes to check the integrity of the message and confirm that the message has been sent by a legitimate source. Tampering with the message m is ineffective since the destination can check its validity against the tamper-proof MAC received from the S_1 packet. This basic ALPHA model is illustrated in Figure 2.6.

This procedure of individual packet exchange is not possible or practical for larger data transfer volumes, and therefore, ALPHA-C is intended for cumulative transmission of messages. In this model, only one S_1 packet is used containing multiple pre-signatures for the multiple messages, which are obtained by hashing the individual messages in the same manner as in the basic model. Following the receipt of the single S_1 packet, the destination sends a single A_1 to the source which then triggers the source to transmit multiple messages to the destination through the S_2 packets. The S_2 packet will contain the individual messages along with the single hash chain element that was used to create the pre-signature. As in the basic ALPHA model, the destination and the intermediate relays can buffer the pre-signature, and following receipt of S_2, confirm that the messages received have not been tampered with.

However, to avoid the the huge buffer requirements arising out of the multiple pre-signatures in ALPHA-C, a third adaptation of ALPHA has been proposed making use of Merkle trees (ALPHA-M).

A Merkle tree (MT) is a binary hash tree where leaves are the hashes of the messages/data blocks and each internal node is the hash of the concatenation of their respective children [89]. A simple Merkle tree is illustrated in Figure 2.7. The top node is referred as the root of MT and is dependent upon the content of all leaves and the internal nodes. MT can be used to authenticate the message on an individual basis and verify its integrity. Using the example in Figure 2.7, to enable the verifier (or destination) to authenticate m_2 independently of other messages, the signer (or source) constructs the MT, and then discloses the root h_{15}, m_2, and the set $\{B_c\}$ of the sibling nodes on the the path from m_2 to the root (h_1, h_{10}, *and* h_{14}). The verifier can then reconstruct the root h_{15} from $H[[H[[H[[H(m_2)]||h_1]]||h_{10}]]||h_{14}]$ and compare it with the root value received earlier from the signer. The same root value would mean that the received message has not been altered. An MT with n leaves or messages requires $\log_2(n)$ sibling nodes to be included with each message.

When hash chains are combined in a Merkle tree, the hash chain authenticates identities and the MT provides integrity protection for each packet on an individual basis, which is especially useful for on-path verification with the high-volume data in cooperative communication networks. In ALPHA-M, as like the basic ALPHA model, the source and destination maintain their own separate hash chains and initially exchange their respective hash chain anchors through an initial handshaking process (h_i^S and h_i^D), which is also passed on to the relays. The source constructs the MT with hashes of data blocks, m_j, and sends the pre-signature, which is obtained by hashing the root with the next element of the hash chain (i.e., key of the pre-signature), in an initial S_1 packet along with a fresh element of the hash chain. The destination builds

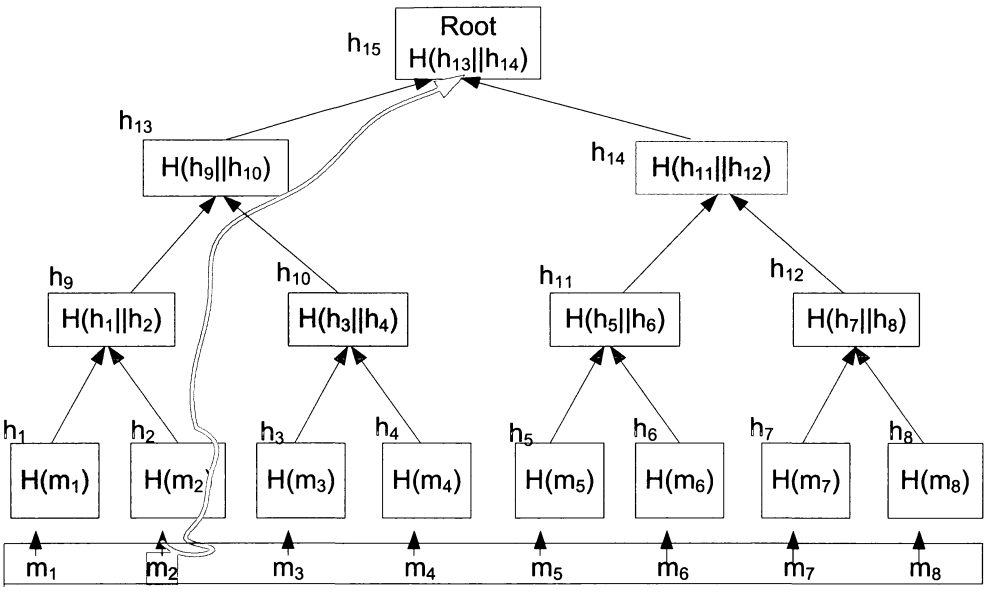

Figure 2.7: A Merkle tree.

an Acknowledgment Merkle tree (AMT) and sends the acknowledgment A_1 with its own pre-signature. The actual message transfer process is then initiated with the source sending S_2 packets corresponding to the number of messages/data blocks in the MT along with the respective set $\{B_c\}$ and key of the pre-signature. Following receipt of this information, the destination can rebuild the MT corresponding to the message block and verify the integrity of the pre-signature, from which we can conclude that the message block has not been tampered with. Based on this, the destination sends either a positive or negative acknowledgment (acks/nacks) through the A_2 packets. The key of the pre-signature received in the S_2 packet can be hashed by the recipient node to arrive at the hash chain anchor value thus confirming the authenticity of the source. Accordingly, both end-to-end as well as hop-by-hop authenticity and integrity protection is available at all nodes and can be used as building block for secure signaling between end-hosts and relays. This is illustrated in Figure 2.8.

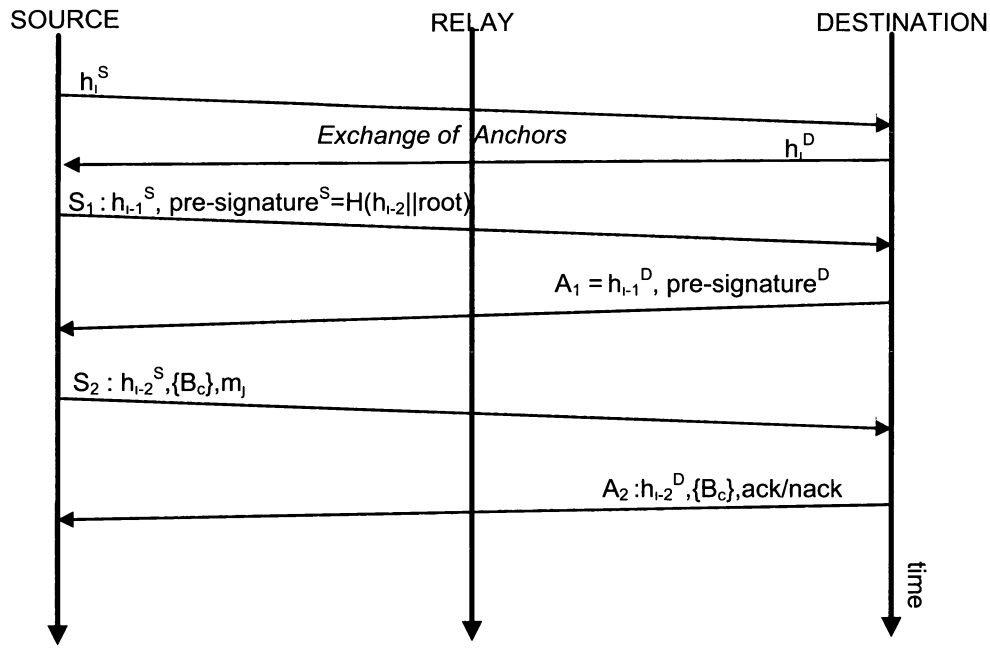

Figure 2.8: Alpha using Merkle tree.

2.6 Summary

In this chapter, we presented the background knowledge and related work of this thesis by looking at the fundamentals of cooperative communication, evaluating cooperative communication in ad hoc networks, opportunistic relaying, security issues in cooperative communication, authentication, hash chains, and Merkle trees. Because of the inherent nature of the cooperative networks with the use of any available intermediate nodes as relays, the dynamic relay selection processes and the lack of centralized control, it is crucial to have an efficient *prevention*-based security scheme in order to obtain both end-to-end and hop-by-hop authentication and integrity protection. To this end, the ALPHA-M authentication protocol was described. The existing relay selection schemes have a narrow focus and have not considered security as a prerequisite for relay selection. In the following chapter, we will look at the proposed JAQS in detail.

Chapter 3

Proposed Joint Authentication and QoS Scheme

In this chapter, we describe our proposed security-enabled relay selection scheme entitled "joint authentication and QoS scheme (JAQS)" in detail by initially setting out the system model and presenting the equations for outage probability, outage capacity, and BER. Subsequently, we elucidate specifically about JAQS by deriving closed-form secured throughput equations for the authentication process, jointly optimizing the number of messages in the Merkle tree and explaining the implementation of the proposed relay selection process in conjunction with our combined Merkle trees and hash chains based authentication and integrity protection scheme.

Our contribution includes adapting the ALPHA authentication protocol to cooperative communication and using the hash chains and Merkle trees to offer both end-to-end and hop-by-hop authentication and integrity protection and selecting the best relay on a proactive basis amongst a set of available multiple relays between the source and the destination. Taking cognizance of the physical layer parameters, we derive closed-form secured throughput equations for the authentication protocol considering various scenarios and applying error control schemes, which we use to select the relay that provides the highest throughput and security.

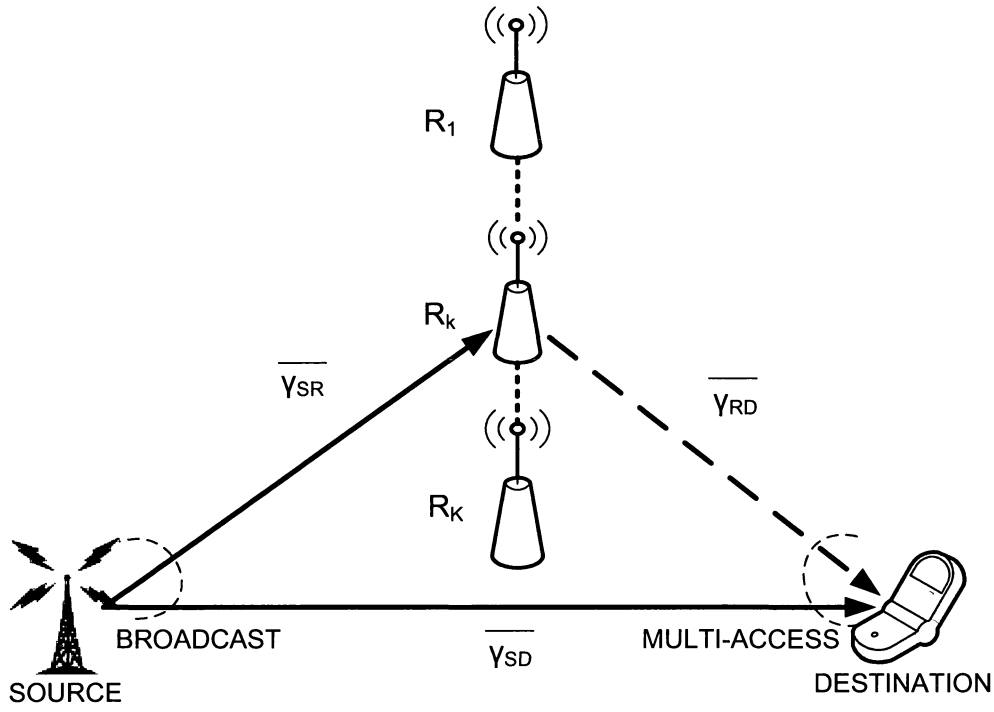

Figure 3.1: Cooperative communication network with SNR.

3.1 Model Description

We consider a simple cooperative wireless network with two-hops, as shown in Figure 3.1, comprising of a source (S) node communicating with a destination (D) node through potentially K relay nodes, $R_1, R_2, ..., R_k, ...R_K$. The channel between two nodes, x and y, is considered to be a flat and slowly-fading Rayleigh distribution with variance $1/\lambda_{xy}$, which is independent of channels between the remaining nodes. We take h_{xy} as the channel gain, which captures the effect of fading and path loss, with $|h_{xy}|^2$ having an exponential distribution with the parameter $\lambda_{xy} = d_{xy}^{\alpha}$, where d_{xy} is the distance between nodes x and y, and α is the path loss exponent. The fading is slow enabling the coherence time of the channel to be long enough for the system to complete the transmission of the block of data. All nodes are considered to be transmitting with the same average transmit signal power.

We denote the average transmitted SNR between any nodes as γ,which is given by:

$$\gamma = \frac{P}{N_o \cdot W}, \tag{3.1}$$

where P is the average transmit signal power, W is the transmission bandwidth and N_o is the noise.

We denote the average received SNR as $\overline{\gamma}$. We also denote the distance between the source and the destination as d_{SD}, the distance between the source and a relay node as d_{SR_k}, and the distance between a relay node and the destination as d_{R_kD}. We further denote the average received SNR between the source and the destination as $\overline{\gamma_{SD}}$, the average received SNR between the source and the relay as $\overline{\gamma_{SR_k}}$, and the average received SNR between the relay and the destination as $\overline{\gamma_{R_kD}}$.

Accordingly, $\overline{\gamma_{SD}} = \frac{\gamma}{d_{SD}^{\alpha}}$, $\overline{\gamma_{SR_k}} = \frac{\gamma}{d_{SR_k}^{\alpha}}$, and $\overline{\gamma_{R_kD}} = \frac{\gamma}{d_{R_kD}^{\alpha}}$.

The source node can send information to the destination directly or through a relay. As the relay cannot transmit and receive simultaneously, on account of the half-duplex constraint, the transmission time in case a relay is used is divided into two time slots with transmission by the source in the first time slot, transmission by the relay in the second time slot and the destination finally combining the two received signals.

We present mutual information equations for non-cooperative and cooperative diversity schemes [42]. In the non-cooperative mode, the source node transmits the signal directly to the destination node. The mutual information between the source and the destination is simply:

$$I_{non-coop} = \log_2\left(1 + |h_{SD}|^2 SNR\right), \tag{3.2}$$

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

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

The mutual information between the source and each of the k^{th} relay nodes is given by:

$$I_{\substack{SR_k \\ (k \epsilon K)}} = \frac{1}{2} \log_2 \left(1 + |h_{SR_k}|^2 SNR\right), \tag{3.3}$$

where $|h_{SR_k}|$ is the channel between the source and the k^{th} relay. Given the half-duplex constraint, the factor $\frac{1}{2}$ mirrors the two time slots for relaying.

The mutual information between source-destination and destination-each of the k^{th} relay nodes is given by:

$$I_{MRC} = \frac{1}{2} \log_2 \left(1 + (|h_{SD}|^2 + |h_{R_k D}|^2) SNR\right), \tag{3.4}$$

where $|h_{R_k D}|$ is the channel between the k^{th} relay and the destination.

Thus, the maximum end-to-end mutual information is given by:

$$I_{coop} = \max_{k \epsilon K} min \left\{I_{SR_k}, I_{MRC}\right\}. \tag{3.5}$$

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

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

$$I_{SC} = max\{I_{coop},\ I_{non-coop}\}. \tag{3.6}$$

3.1.1 Outage Probability and Outage Capacity

The communication between the source and the destination targets an end-to-end data rate of r. Outage Probability (P_{out}) is defined as the probability that the mutual information (I) between the source and the destination, including relay falls below the required rate r, i.e.,

$$P_{out} = P\left[I < r\right], \tag{3.7}$$

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

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

$$P_{out}^{SC,k} = P\left[I_{SC} < r\right], i.e., \tag{3.8}$$

$$P_{out}^{SC,k} = P\left\{max\left\{I_{SD}, \max_{k\epsilon K} min\left\{I_{SR_k}, I_{MRC}\right\}\right\} < r\right\} \tag{3.9}$$

from which we arrive at [42],

$$P_{out}^{SC,k} = 1 - \upsilon + \left(\frac{\omega^{(d_{SR_k}^{\alpha} + d_{R_kD}^{\alpha})}\left(\upsilon^{(1-d_{R_kD}^{\alpha})} - 1\right)}{1 - d_{R_kD}^{\alpha}}\right), \tag{3.10}$$

where υ and ω are given by

$$\upsilon = \exp\left(-\left(\frac{2^r - 1}{\gamma}\right)\right), \tag{3.11}$$

$$\omega = \exp\left(2\ln\upsilon - (\ln\upsilon)^2\gamma\right). \tag{3.12}$$

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

$$r = C_{\epsilon}^{SC,k} = \log_2\left(1 + \gamma\ln\left(\frac{1}{\upsilon_{\varepsilon}, \gamma}\right)\right). \tag{3.13}$$

Outage capacity is used instead of Shannon capacity in slow fading channel as the nature of the slow fading channel is different from the additive white Gaussian noise channel as delay constraints are on the order of the channel coherence time [18].

3.1.2 Bit Error Rate

Bit error rate (BER) is the percentage of bits that have errors relative to the total number of bits received in a transmission. This end-to-end BER of SC transmission, $P_e^{SC,k}$, is given by [99]:

$$P_e^{SC,k} = P_{out}^{SR_k} \cdot P_e^{SD} + \left(1 - P_{out}^{SR_k}\right) \cdot P_e^{div,k}, \tag{3.14}$$

where $P_{out}^{SR_k}$ is the outage probability of the link from source to relay. If an outage occurs between source and relay, the relay will not decode, and falls back to direct transmission, i.e.,

$$P_{out}^{SR_k} = 1 - \exp\left(-\left(\frac{2^{2r}-1}{\overline{\gamma_{SR_k}}}\right)\right), \tag{3.15}$$

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

$$P_e^{SD} = \frac{1}{2}\left(1 - \sqrt{\frac{\overline{\gamma}_{SD}}{1+\overline{\gamma_{SD}}}}\right), and \tag{3.16}$$

$P_e^{div,k}$ is the probability that an error occurs in combined transmission from source and relay nodes at the destination. This occurs if the relay has decided to decode and forward the signal to the destination. To prevent error propagation, we assume that the relay decodes if it has correctly received the signal from the source. The error probability for MRC of two BPSK transmissions (binary phase shift keying) over Rayleigh fading channels with different SNRs ($\overline{\gamma_{SD}} and \overline{\gamma_{R_kD}}$) is given by

$$P_e^{div,k} = \frac{1}{2}\left[1 + \frac{1}{\overline{\gamma_{R_kD}} - \overline{\gamma_{SD}}}\left(\frac{\overline{\gamma_{SD}}}{\sqrt{1+\frac{1}{\overline{\gamma_{SD}}}}} - \frac{\overline{\gamma_{R_kD}}}{\sqrt{1+\frac{1}{\overline{\gamma_{R_kD}}}}}\right)\right]. \tag{3.17}$$

3.2 Analysis of JAQS

We derive the generic throughput for the ALPHA authentication protocol, and modify it to cater to both direct communication (DC) i.e., direct transmission between the source and the destination and source-relay-destination (SRD) i.e., transmission between the source and the destination making use of the intermediate relay node scenarios taking into consideration BER and packet error rate. We then formulate the throughput equations for both Selective Repeat (SR) and Go-Back-N (GBN) ARQ retransmission schemes taking the error rate into consideration, and then present the joint optimization of the number of messages in the Merkle tree and relay selection in cooperative communication networks.

3.2.1 Throughput for the Authentication Process

The payload for ALPHA-M process is given in [90] as:

$$S_{payload} = n \cdot (S_{packet} - S_h(\lceil \log_2(n) \rceil + 1)), \tag{3.18}$$

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

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

$$Throughput_{General} = \frac{S_{payload}}{T_1 + T_2}, \tag{3.19}$$

Table 3.1: Time Parameters in T_1.

	t_{prop1}	t_{f1}	t_{proc1}	t_{ack1}
T_1^{DC}	$2\left(\frac{d_{SD}}{c}\right)$	1	3	1
T_1^{SRD}	$2\left(\frac{d_{SR_k}}{c}\right) + 2\left(\frac{d_{R_kD}}{c}\right)$	2	5	2

where

- T_1 is the time for the initial pre-signature process between the source and the destination. It works like a basic Stop-and-Wait ARQ model (*explained below*) with transmission of S_1 packet by the source, processing at the destination, transmission of acknowledgment A_1 packet by the destination and processing at the source. The message delivery is complete only after the source receives the confirmatory acknowledgment from the destination.

- T_2 is the time taken for the actual message transmission and delivery, i.e., the actual transfer of messages from the source through the S_2 packets and the transfer of acknowledgments from the destination through A_2 packets.

The values for the time parameters in T_1 and T_2 vary according to the communication paths (DC and SRD), and are presented in Table 3.1 and Table 3.2. The message sequence charts showing the transmission of message from the source to the destination and the acknowledgment between the destination and the source, with and without the use of relay are illustrated in Figure 3.2.

The parameters identified in Tables I and II are explained as follows:

- t_{prop1} is the propagation time for the S_1 packet from the source to the destination or for the A_1 packet from the destination to the source. In case of DC, this is given by $\left(\frac{d_{SD}}{c}\right)$, where c is the speed of light. In case of SRD, this reflects

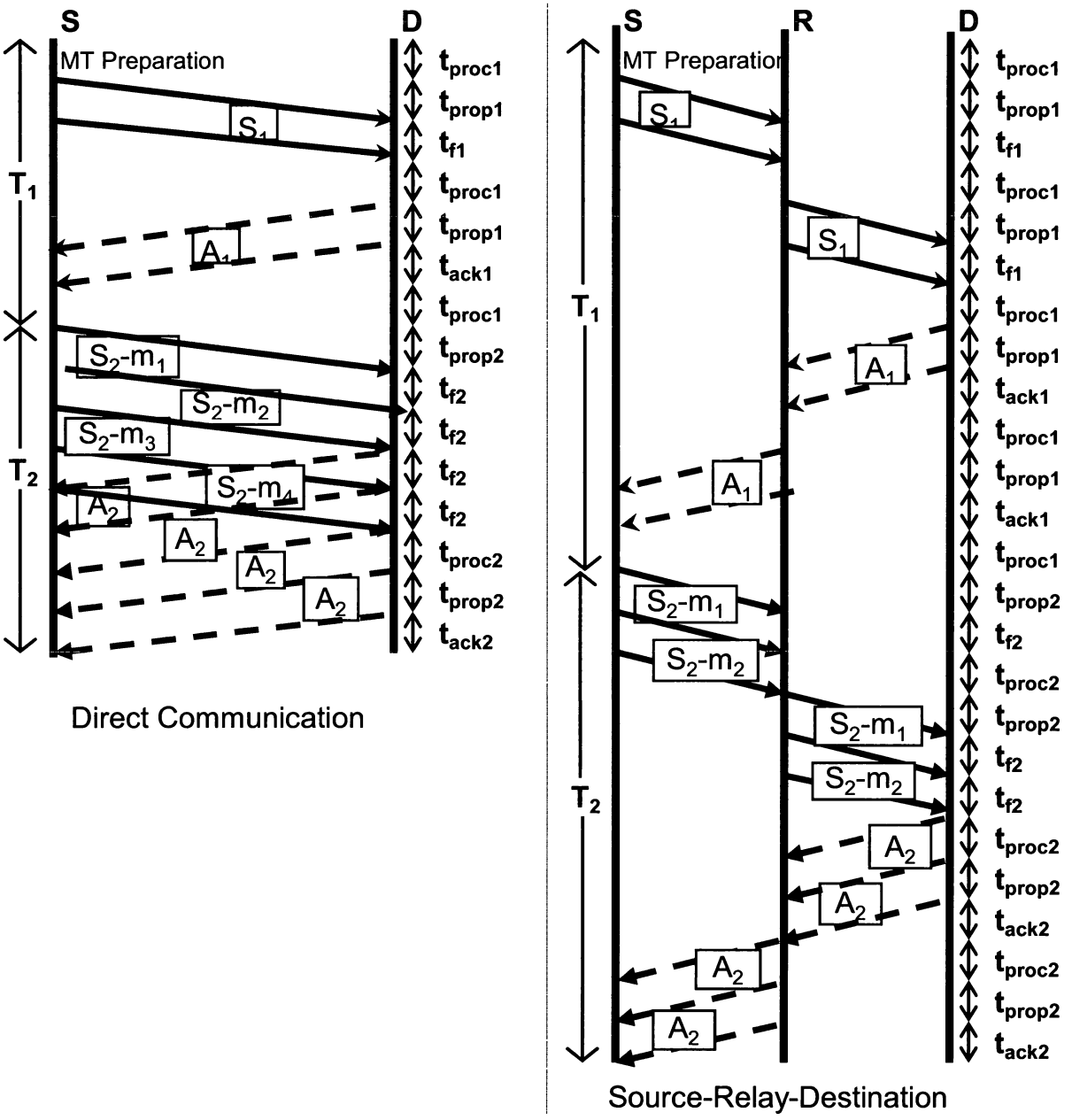

Figure 3.2: Message sequence charts in direct communication and source-relay-destination communication.

Table 3.2: Time Parameters in T_2.

	t_{prop2}	t_{f2}	t_{proc2}	t_{ack2}
T_2^{DC}	$2\left(\frac{d_{SD}}{c}\right)$	n	1	1
T_2^{SRD}	$2\left(\frac{d_{SR_k}}{c}\right) + 2\left(\frac{d_{R_kD}}{c}\right)$	$(n+1)$	3	2

the propagation time for the S_1 packet from the source to the relay and from the relay to the destination, or for the A_1 packet from the destination to the relay and from the relay to the source. This is given by the sum of $\left(\frac{d_{SR_k}}{c}\right)$ and $\left(\frac{d_{R_kD}}{c}\right)$.

- t_{prop2} is the propagation time for the S_2 packet from the source to the destination or for the A_2 packet from the destination to the source. In case of DC, this is given by $\left(\frac{d_{SD}}{c}\right)$. In case of SRD, this reflects the propagation time for the S_2 packet from the source to the relay and from the relay to the destination or for the A_2 packet from the destination to the relay and from the relay to the source. This is given by the sum of $\left(\frac{d_{SR_k}}{c}\right)$ and $\left(\frac{d_{R_kD}}{c}\right)$.

- t_{f1} is the packet transmission time for the S_1 packet. This is given by $\left(\frac{u_{f1}}{r}\right)$, where u_{f1} is the number of bits in the S_1 packet.

- t_{f2} is the packet transmission time for the S_2 packet. This is given by $\left(\frac{u_{f2}}{r}\right)$, where u_{f2} is the number of bits in the S_2 packet.

- t_{ack1} is the packet transmission time for the A_1 packet. This is given by $\left(\frac{u_{ack1}}{r}\right)$, where u_{ack1} is the number of bits in the A_1 packet.

- t_{ack2} is the packet transmission time for the A_2 packet. This is given by $\left(\frac{u_{ack2}}{r}\right)$, where u_{ack2} is the number of bits in the A_2 packet.

- t_{proc1} is the processing time at the source and destination for S_1 and A_1 packets in DC, which includes the preparation of Merkle tree for S_1 packet at the source and the preparation of AMT for A_1 packet at the destination along with processing at the relay node in SRD.

- t_{proc2} is the processing time at the source and destination for S_2 and A_2 packets in DC, along with processing at the relay node in SRD.

3.2.2 Throughput Using Error Control Schemes

Although reliable transfer of data is a critical requirement in any communication, the dependability of the process is affected by the unreliable state of the communication channels induced by channel noise and glitches caused in the transmission between a source and the destination. Two types of errors are possible resulting from lost and damaged packets. To mitigate them, error control techniques based on error detection, which detects errors caused by noise in the transmission between the source and the destination, and retransmission, where errors are corrected through reconstruction of the original error-free data, is implemented.

There are two categories of error control schemes [100]:

- Forward Error Correction (FEC) scheme: An error-correcting code is used for combating transmission errors and is encoded by the source prior to transmission. The destination uses the additional information, i.e., redundancy, added by the code to recover the original data. No retransmission of data is required in this scheme and no feedback channel is needed. Although the throughput is relatively constant, reliability is difficult due to the decoding error and requires complex error correcting codes and error patterns.

- Automatic Repeat reQuest (ARQ) scheme: This involves error detection and

retransmission of lost or corrupted packets, where every block of the received data is verified using the error detection code used, and if the verification fails, retransmission of the data is requested via a feedback channel, and this process is repeated to ensure that the data is delivered accurately to the destination despite errors that occur during the transmission. Using a proper error detection code, the probability of an undetected error can be made very small. ARQ schemes are used in data communication systems for error control as they are simple and provide a higher degree of system reliability.

We implement an ARQ based retransmission scheme, and therefore, look at this scheme in detail.

The most commonly used ARQ retransmission schemes are:

- Stop-and-Wait ARQ: In this arrangement, the source sends one packet at a time and will wait for an ack/nack from the destination. If a positive acknowledgment is received, the second packet is transmitted. If a negative acknowledgment is received, the source retransmits and waits for a positive acknowledgment. Although this scheme is simple, it is inefficient on account of the idle time waiting for a positive acknowledgment for each transmitted packet.

- Go-Back-N (GBN) ARQ: In this arrangement, the source continues to send a number of packets limited by a window size and stores them pending receipt of ack/nack from the destination. When a packet is received in error, the destination ignores that packet and all the subsequently received packets and sends a nack to the source. When the source receives a negative acknowledgment for a sent packet, it retransmits it and the other frames that were sent after that particular packet. The channel is kept busy and the throughput is higher than the Stop-and-Wait model. However, GBN is inefficient because of the need to

retransmit not only the errored packet, but also the packets sent subsequent to that, whether they were in error or not. It is not effective for communication systems with high data rates and large round-trip times [100].

- Selective Repeat (SR) ARQ: In this arrangement, which is similar to GBN, only the errored packet is retransmitted. The packets are transmitted continuously by the source, specified by a window size, and retransmits only the packets that are negatively acknowledged by the destination. The destination keeps track of the sequence number of the earliest packet it has not received and sends that number with every acknowledgment it sends until that particular packet is successfully received from the source.

To incorporate the error control schemes in our throughput equations, we vary the above generic throughput equation (3.19) and expand it by including the error rate. We have already explained $P_e^{SC,k}$ in (3.14) as the end-to-end BER, i.e., the probability that any given bit of received data is in error. We define the packet error rate P_c as the probability that the received packet comprising of S_{packet} bits contains no error [100], which is given by:

$$P_c = \left(1 - P_e^{SC,k}\right)^{S_{packet}} . \tag{3.20}$$

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

$$Throughput_{SR} = \frac{S_{payload}}{(T_1 + T_2)} \left(P_c\right) . \tag{3.21}$$

With respect of the Go-Back-N (GBN) ARQ scheme, the throughput equation is further modified to allow the retransmission of an error frame along with all frames

that had been transmitted until the time that negative acknowledgment is received from the destination. Accordingly,

$$Throughput_{GBN} = \frac{(S_{payload} \times P_c)}{T_1 + T_2 \left[P_c + (1 - P_c) W_s\right]}, \tag{3.22}$$

where W_s is the window size which is calculated by dividing the product of the data rate of the transmission channel and the reaction time by the packet size.

The following factors have an impact on the throughput performance in the proposed cooperative communication network model. However, these constraints do not affect the viability of using the combined MTs and hash chains based authentication and integrity protection scheme in wireless multi-hop networks, such as in cooperative communications, since varying latency, out-of-order delivery, and high loss rates can be tolerated due to the individual verifiability of each S_2 packet [90].

- As the number of messages or S_2 packets corresponding to the number of leaves increases, the set $\{B_c\}$ enlarges logarithmically consequently expanding the signature size overhead of the hash function in 3.18. This results in a reduction in the effective payload transmitted and decreases the throughput. The payload falls to zero after a particular n value as the overheads exceeds the size of S_{packet}.

- As the hash signature size overhead in 3.18 is the same for any size of the packet (S_{packet}), the signature size overhead is relatively lower for larger packet sizes and increases only with an expansion in the number of leaves in the MT.

- As the BER increases, the throughput decreases on account of the substantial reduction in the effective payload transmitted caused on account of an increase in the need to retransmit the errored packets using error control schemes.

- As the size of the individual packet (S_{packet}) increases, the error during the

transmission process also increases consequently leading to a higher BER value decreasing the throughput.

- As the number of messages (n) increases, the number of hash calculations required also increase, which is dependent upon the number of messages. For n messages and if MT alone is used, the source has to carry out $(n - 1)$ computations and the verifier and the relay have to carry out $(\lceil \log_2(n) \rceil - 1)$ computations. However, if the AMT is also used, the source and the relay will have to carry out $(2 \times (\lceil \log_2(n) \rceil - 1))$ additional computations and the destination has to carry out $(2 \times (n - 1))$ additional computations.

- As the number of messages (n) increases, the size of MT also increases requiring the transmission of a larger set $\{B_c\}$ with each message consequently decreasing the effective payload transmitted.

- As the bandwidth overhead per S_2 packet contains $(\lceil \log_2(n) \rceil)$ hashes and an undisclosed hash chain element, the bandwidth overhead increases with an increase in the number of messages (n).

- As the source has to buffer the complete set of n messages prior to building the MT and creating the pre-signature and in addition have to complete the exchange of S_1 *and* A_1 packets, the transmission of the actual message through the S_2 packet is delayed with a consequent increase in the time required for T_1.

3.2.3 Optimizing the Number of Messages in the Merkle Tree and Relay Selection

Consider a cooperative communication network with two hops that comprises source (S), destination (D), and K relay nodes, $R_1, R_2, ..., R_k, ..., R_K$. The source needs

to determine the optimal number of messages in the Merkle tree, and at the same time select the best relay prior to the commencement of the data transmission. The whole communication is divided into equal dimension time slots. At the start of each time slot, the source broadcasts pilot signal. This is received by the relays and the destination. All the participant relays and the destination estimate their own signal strength towards the source by calculating the average SNR between the source and the destination $\overline{\gamma_{SD}}$, and between the source and each of the relays $\overline{\gamma_{SR_k}}$, respectively. Along with the pilot signal, the relays forward $\overline{\gamma_{SR_k}}$ to the destination. Based on the received pilot signal from the relays, the destination can thereafter estimate the channel quality between the relay and the destination by calculating $\overline{\gamma_{R_kD}}$. All the average SNR values between the source and the destination$\overline{\gamma_{SD}}$, the source and each of the relays $\overline{\gamma_{SR_k}}$, and each of the relays and the destination $\overline{\gamma_{R_kD}}$ is then subsequently fed back by the destination to the source.

For each packet size (S_{packet}), the optimal value of the number of messages (n) in the Merkle tree, which corresponds to the number of S_2 packets, is the value that results in the highest throughput, which is denoted n^*. There is a trade-off as the throughput increases initially with the number of messages in the Merkle tree but then starts to decrease as a consequence of the larger signature size overheads from the increased number of messages in the Merkle tree. The optimal number of messages in the Merkle tree for relay R_k, n_k^*, is determined from:

$$n_k^* = \arg\max_{n_k} Throughput_k(R_k, n_k, S_{packet}), \tag{3.23}$$

where $n_k \epsilon \{1, 2, ...\}$ $for\ each\ k\ =\ 1, 2, ..., K$.

Using (3.20), the source determines P_c, which is the the packet error rate for each relay. The source applies the individual packet error rates for each relay in the throughput equations (3.21 and 3.22) to estimate the potential throughput values for

each relay with varying packet sizes at the optimal n value. It then selects the best relay, R_k^*, that gives the maximum throughput among the set of relays for each S_{packet} from:

$$R_k^* = \arg\max_{R_k} Throughput_k(R_k, n_k^*, S_{packet}), \tag{3.24}$$

where $k\epsilon\{1, 2, ..., K\}$.

Consider, for example, the case of four relays in Figure 3.3, where following the above explained relay selection process, R_3 is selected as the best relay and is then used in the actual communication of the messages. Following the selection of R_3 as the best relay, the source broadcasts details about the best relay so that the other relays do not get involved in the actual data transmission process. The source and the destination then exchange their anchor keys through an initial handshaking process, and R_3 is kept aware of this information. The source, destination, and the selected relay R_3 subsequently form a protected path. Once the anchors are exchanged, the system is ready to securely transmit messages between the source and the destination using the combination of hash chains and MTs, as explained in ALPHA-M. The source broadcasts the S_1 packet containing its pre-signature along with a fresh element of the source's hash chain. This message is received by the destination both through the direct transmission by the source and by means of the forwarded transmission from the relay R_3. Following the receipt of the S_1 message, the destination prepares the A_1 packet containing its own pre-signature of the acknowledgment hash chain and transmits it to the source. The source receives it both through the direct transmission by the destination and by means of the forwarded transmission from the relay R_3.

After the successful transmission and receipt of S_1 and A_1 packets, the source broadcasts the S_2 packets corresponding to the number of leaves in the MT, containing messages m_j along with the set $\{B_c\}$. After the S_2 packet is received by

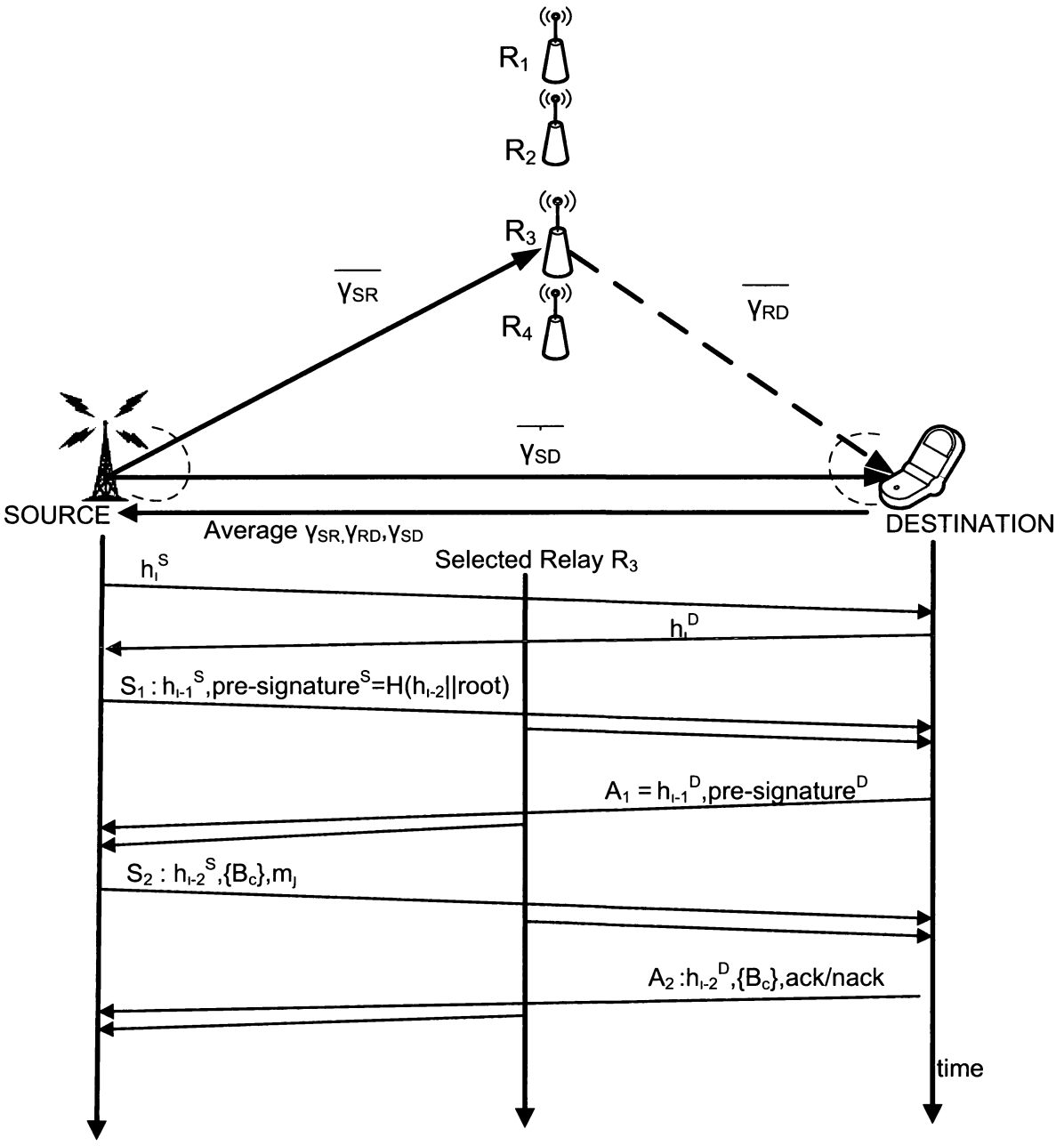

Figure 3.3: Relay selection using JAQS in a cooperative communication network.

the destination, the destination can independently reconstruct the MT corresponding to that message block and recompute the source's pre-signature value. If the pre-signature value transmitted in the S_1 packet and the computed value is the same, the destination is assured that the message has not been tampered with and the transmission is successful. Subsequently, the destination transmits the acknowledgment through the corresponding leaf of the AMT by selecting the corresponding ack or nack, depending upon the success or failure in the receipt of the message, and transmitting it through its A_2 packet. When the A_2 is received by the source, similar to the work done by the destination in recomputing the pre-signature of the source, the source reconstructs the AMT and recomputes the pre-signature value. If the result is a positive acknowledgment, the source is assured that the message delivery has been successful for the corresponding S_2 packet coinciding with a specific m_j message block. However, if the result corresponds to a negative acknowledgment, the source understands that the transmission was unsuccessful or the integrity has been compromised and retransmits the original S_2 packet through the above error control schemes (SR or GBN). Accordingly, the destination or the source or any of the relay nodes can re-compute the pre-signature values and validate the integrity of the messages and the acknowledgments. A flow chart of the entire JAQS process is illustrated in Figure 3.4.

In S_2, the source also transmits the key of the pre-signature, which in our case is h^S_{i-2}. This can be hashed by the destination and the relay R_3 to arrive at h^S_{i-1} sent by source in the S_1 packet and the hash chain anchor value h^S_i, thus confirming the identity of the source and authenticating the S_1 *and* S_2 packets. A similar exercise can also be carried out to confirm the identity of the destination and authenticate the respective A_1 *and* A_2 packets. Through this, both end-to-end and hop-by-hop authentication is facilitated in JAQS.

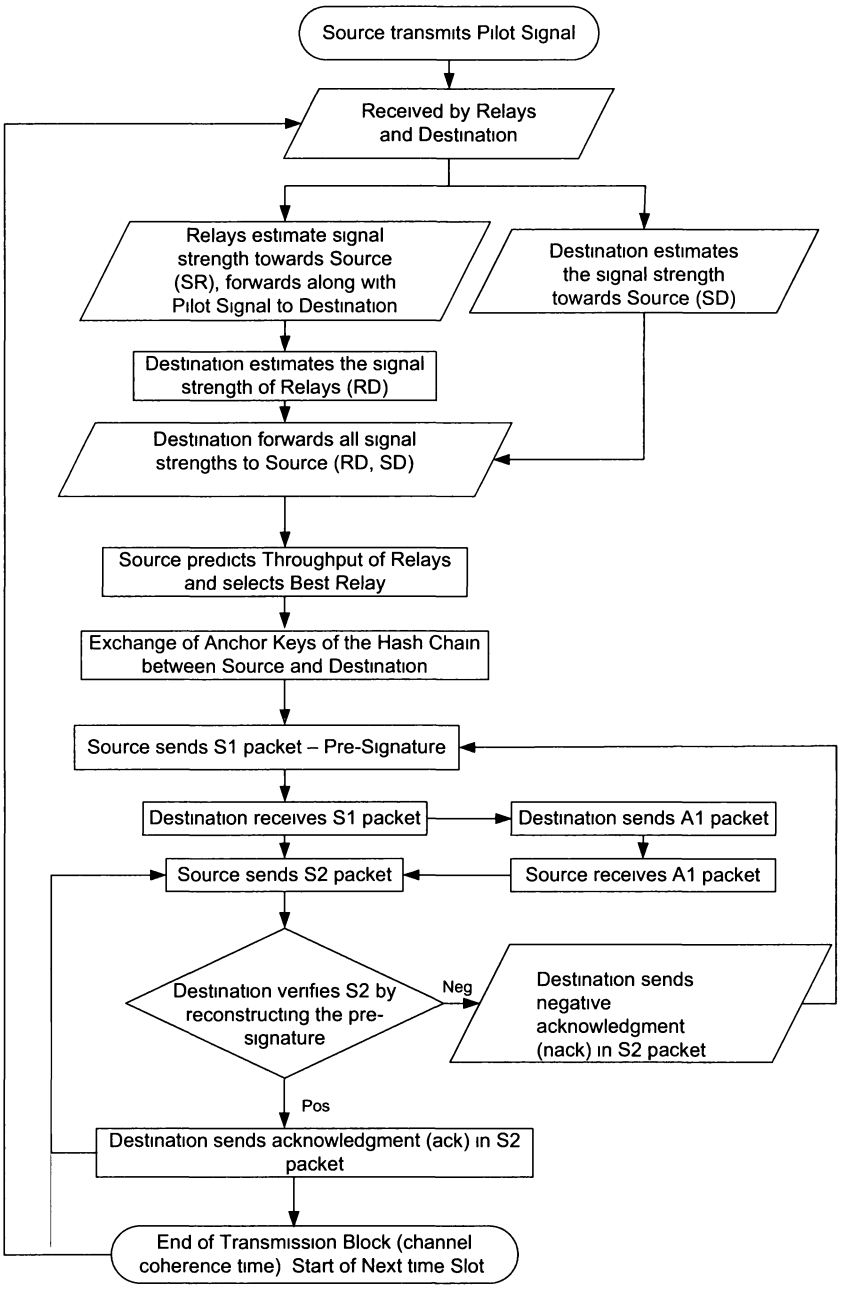

Figure 3.4: Flow chart of the proposed JAQS.

3.3 Summary

In this chapter we illustrated the system model of the proposed security enabled relay selection scheme that offers authentication and integrity protection through the combination of MTs and hash chains. We also presented the throughput equations in JAQS and explained the joint throughput QoS optimization and implementation. JAQS has been designed to improve the security in data transfer process and select the best relay among the multiple relays that can improve the throughput performance. Implementing JAQS provides both end-to-end and hop-by-hop authentication and integrity protection. In the following chapter, we will look at the performance of JAQS through simulation, and discuss the findings.

Chapter 4

Simulation Results and Discussions

In this chapter, we evaluate the performance of the proposed JAQS through simulation experiments. We carried out a set of simulation analysis using MATLAB. All simulations were run on a computer equipped with Windows XP, Intel T1350 CPU (1.86 Ghz), and 2 GB memory on MATLAB version 6.8.0.347 (R2009a) 32-bit. We considered a topology set-up, as depicted in Figure 4.1, with the source and destination located 1,000 meters apart, and four relays arbitrarily located between the source and the destination in an area of 1,000×300 square meters.

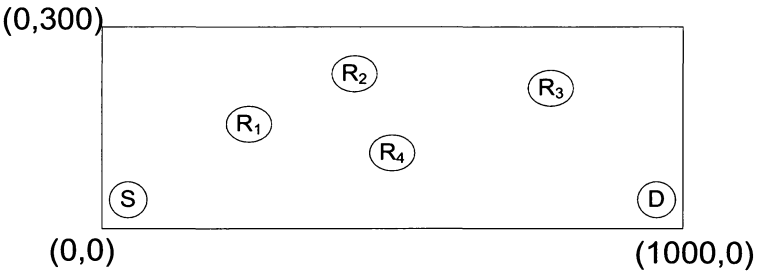

Figure 4.1: Random topology of the simulation.

We took the data rate as 1 Mbps, processing time at each node as 10 μs, path loss exponent as 3.5, and fixed outage probability as 0.01. In all figures, the values represent the average results of 20 different runs. Simulations were carried out by considering four different packet sizes (S_{packet}) of 128, 256, 512, and 1024 bytes,

respectively.

We present the MATLAB simulation program in Appendix A.

4.1 Optimal Number of Messages

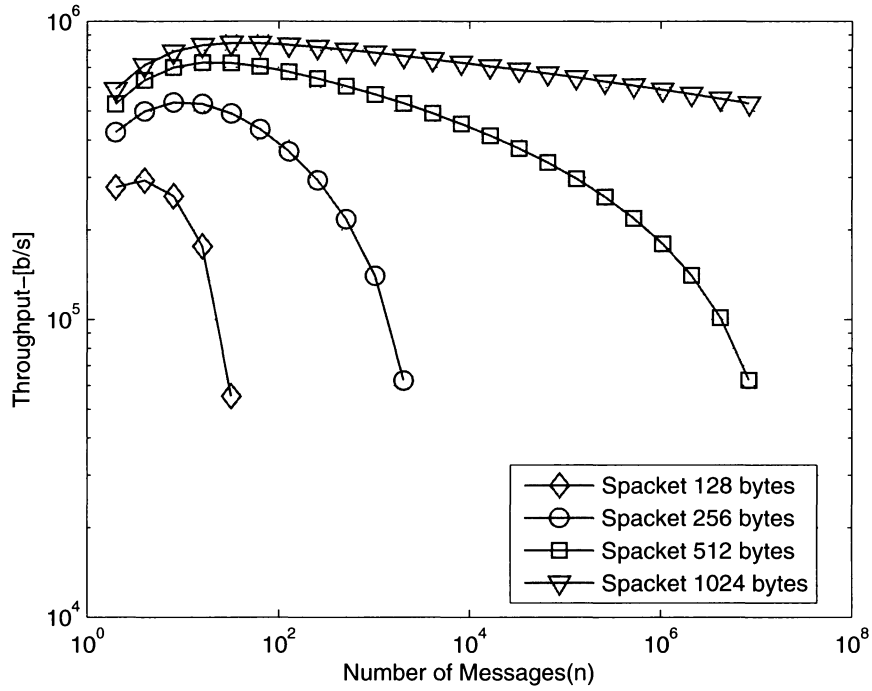

Figure 4.2: The effects of the number of messages in the Merkle tree (n) on the system throughput.

The number of messages in the Merkle tree varies by a power of 2 as the Merkle tree requires binary representation. Figure 4.2 shows the throughput vs. the number of messages and the optimal n value for each of the four packet sizes. As we can observe from this figure, the number of messages in the Merkle tree, i.e. the number of S_2 packets, has a significant effect on the system throughput. As stated in the previous chapters, there is a trade-off with the throughput starting to increase initially with an increase in the number of messages in the Merkle tree, but then decreasing on

account of large signature size overheads and the payload subsequently drops to zero. Therefore, the number of messages that provides the highest throughput, for a given packet size, is chosen as the optimal n value. The optimal number of messages in the Merkle tree for packet sizes 128, 256, 512, and 1024 bytes are 4, 8, 16, and 32, respectively.

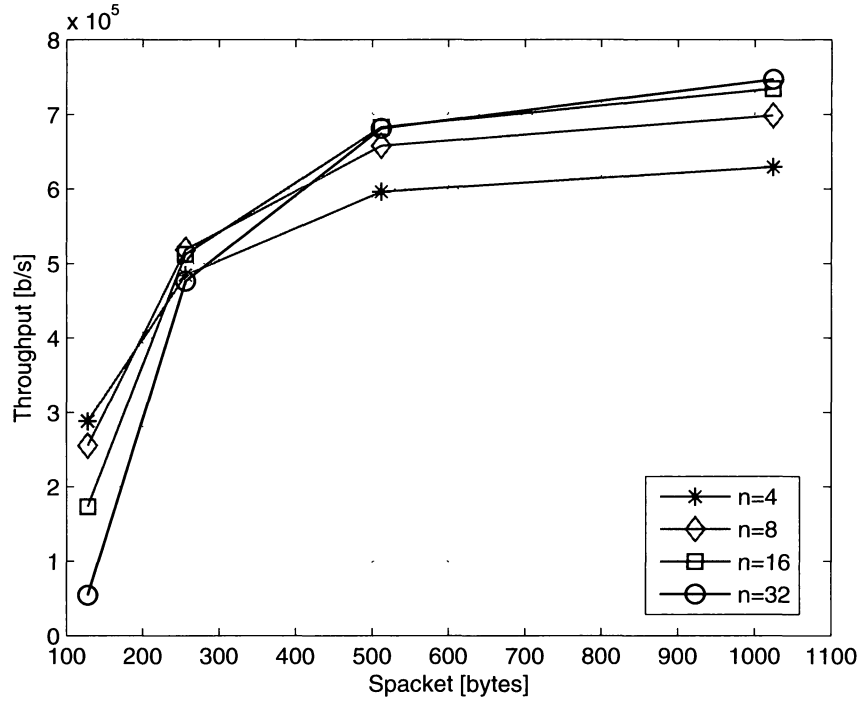

Figure 4.3: Utilizing optimal number of messages (n) in the Merkle tree.

Figure 4.3 illustrates the importance of determining and utilizing the optimal n value corresponding to the specific size of S_{packet}. This figure shows the throughput vs. S_{packet} for different number of messages (n values) in the Merkle tree (4, 8, 16, and 32, respectively) at a fixed SNR value of 20 dB. We infer that by varying the size of S_{packet}, the maximum throughput for each S_{packet} is attained only at particular n value that corresponds to the already determined optimal $n - S_{packet}$ relationship. Therefore, using non-optimal n values adversely affects the throughput performance.

4.2 Throughput Using Non-Optimal n

We also used different numbers of messages (non-optimal n values) in the Merkle tree and the results is presented in Figure 4.4. For this scenario, we considered a packet size (S_{packet}) of 512 bytes and used the SR ARQ model.

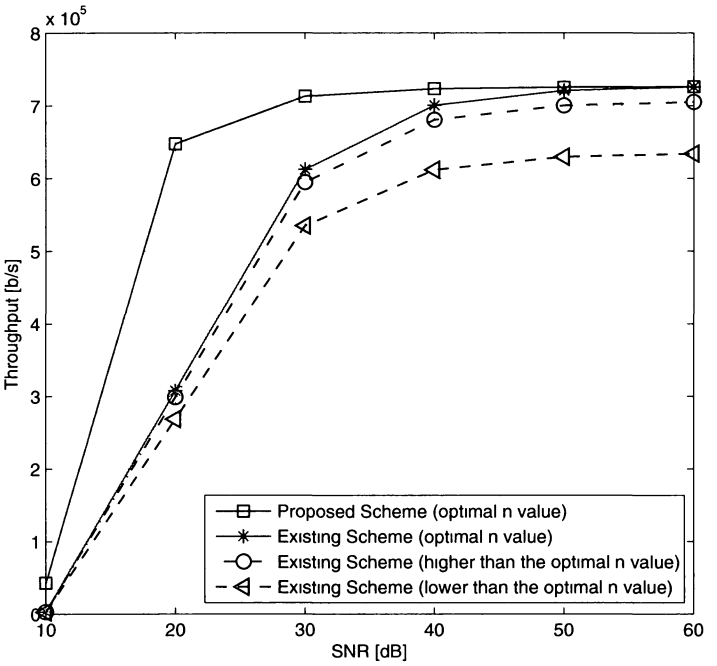

Figure 4.4: Results for different number of messages (n values) in the Merkle Tree.

From this figure, we note that the selected relay remains the same for both optimal n and non-optimal n values, but the throughput performance deteriorates when non-optimal n values are used.

4.3 Throughput Using the Optimal n

For each packet size, we evaluated the throughput-SNR simulations at different SNR values, ranging from 10 to 60 dB, using the already determined optimal n value as a

fixed parameter. The relay that has the best performance in terms of throughput was selected as the best relay based on JAQS. We compare our results with the existing conventional relay selection scheme using outage capacity [42].

4.3.1 Throughput Using SR Retransmission

The simulation results for the Selective Repeat (SR) retransmission schemes are shown in Figures 4.5, 4.6, 4.7, and 4.8, respectively, and is presented in Table 4.1.

Table 4.1: Selection of Best Relay in Selective Repeat Retransmission Scheme.

S_{packet}	Best Relay	
	Existing Scheme	Proposed Scheme
128 bytes	Relay 2	Relay 1
256 bytes	Relay 1	Relay 3
512 bytes	Relay 4	Relay 3
1024 bytes	Relay 2	Relay 1

The results show that the best relay selected under JAQS is different from the relay selected under the existing conventional scheme. This also illustrates that the relay selected under our proposed JAQS outperforms the relay that would have been selected under the conventional scheme, where the selection is based on outage capacity. This performance enhancement is noted on account of the fact that the best relay in our scheme has the lowest BER compared to the other relays. The best relay in our proposed scheme has a significantly higher throughput than the conventional scheme, and in addition, enables the nodes to authenticate and confirm that the messages and acknowledgments received are complete and have not been tampered with.

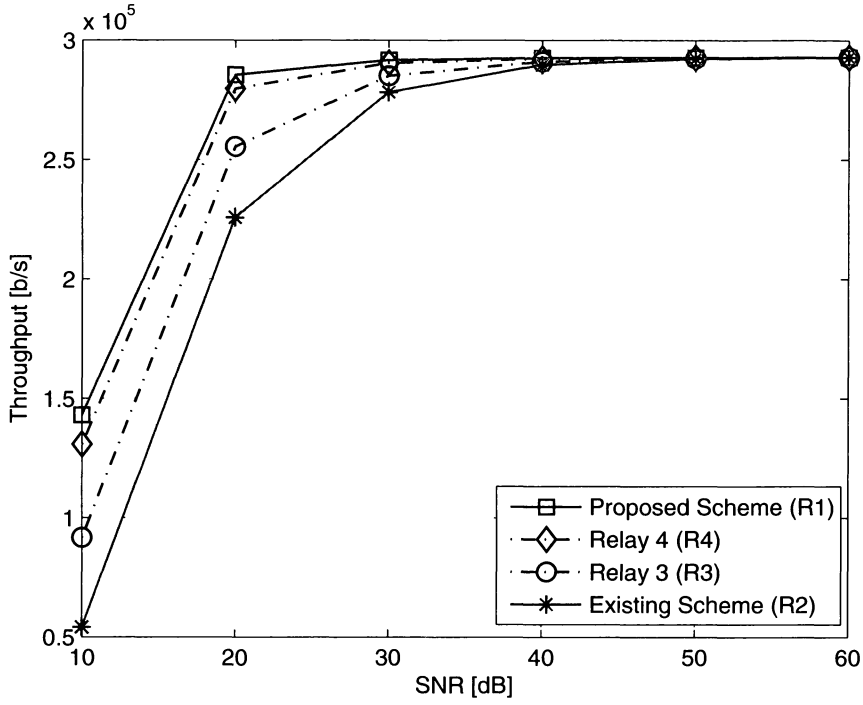

Figure 4.5: Selective Repeat ARQ with S_{packet} of 128 bytes.

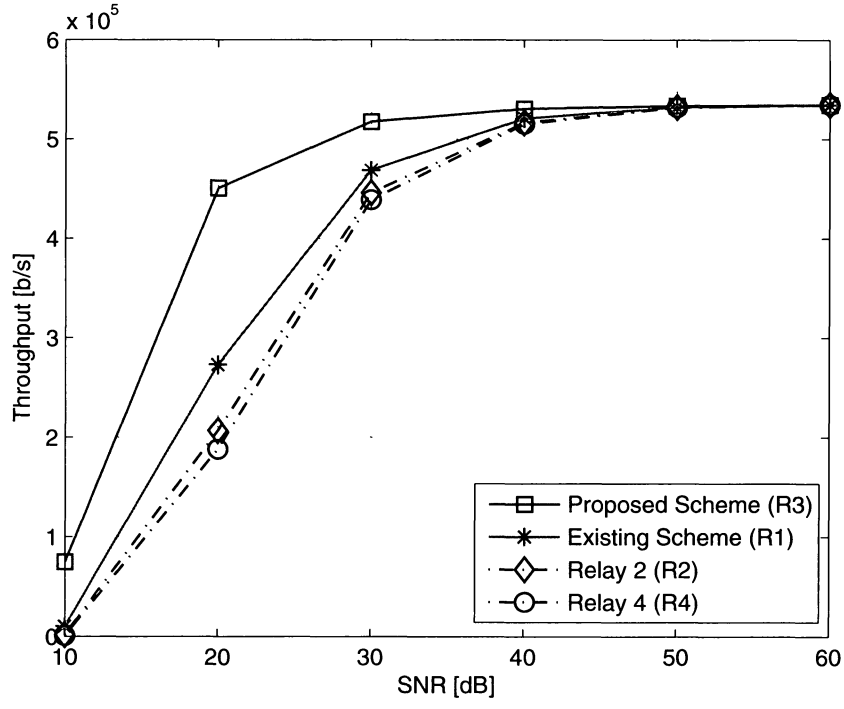

Figure 4.6: Selective Repeat ARQ with S_{packet} of 256 bytes.

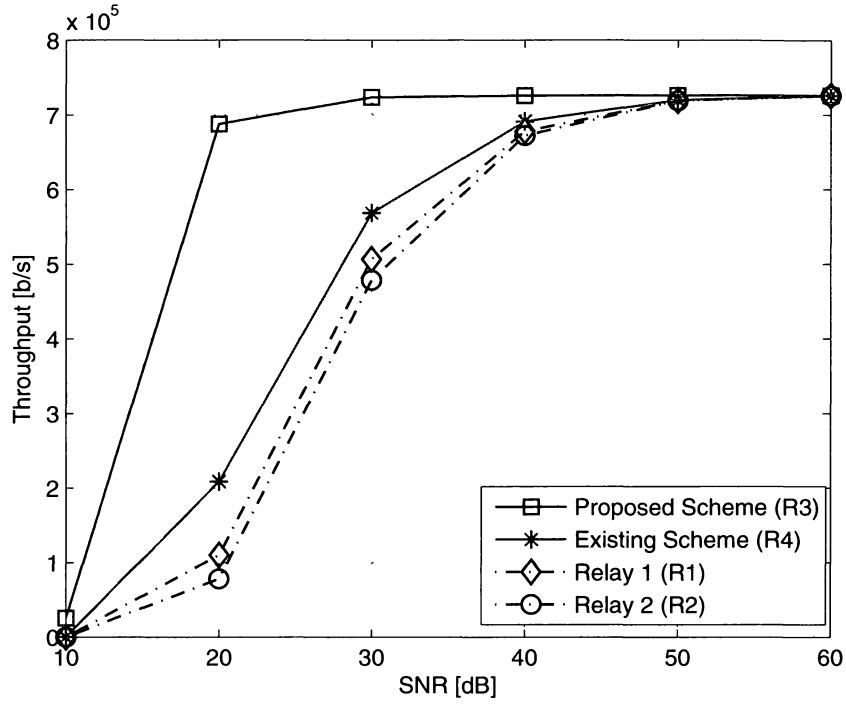

Figure 4.7: Selective Repeat ARQ with S_{packet} of 512 bytes.

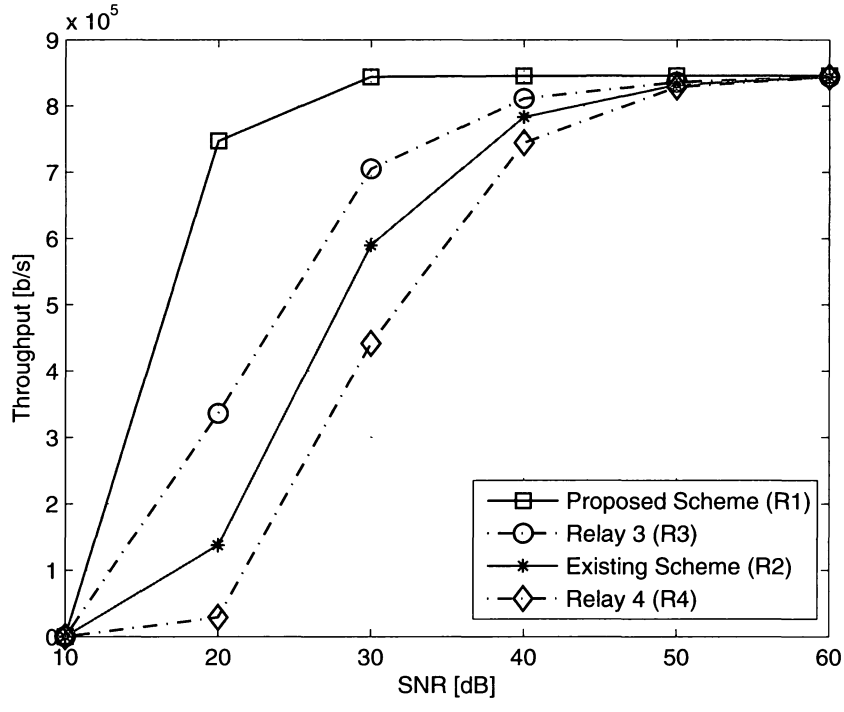

Figure 4.8: Selective Repeat ARQ with S_{packet} of 1024 bytes.

4.3.2 Throughput Using GBN Retransmission

The simulation results for Go-Back-N (GBN) retransmission schemes are shown in Figures 4.9, 4.10, 4.11, and 4.12, respectively, and is presented in Table 4.2.

Table 4.2: Selection of Best Relay in Go-Back-N Retransmission Scheme.

S_{packet}	Best Relay	
	Existing Scheme	Proposed Scheme
128 bytes	Relay 2	Relay 1
256 bytes	Relay 1	Relay 3
512 bytes	Relay 4	Relay 3
1024 bytes	Relay 2	Relay 1

The results are similar to the above SR retransmission scheme. This again establishes that the best relay selected under JAQS is different from the relay selected under the existing conventional scheme, and upholds the findings in SR confirming that the relay selected under JAQS has a higher throughput performance than the relay selected under the conventional scheme.

4.3.3 Throughput with Confidence Interval

We took a 95% confidence interval to assess the results of the existing and proposed schemes from 20 different runs performed on the simulation in order to evaluate the adequate confidence of our results. This was carried out for all the considered four packet sizes (S_{packet}) of 128, 256, 512 and 1024 bytes, and the results obtained from SR retransmission scheme is illustrated in Figures 4.13 to 4.16. The error bars depicted in the figures illustrate the 95% confidence interval.

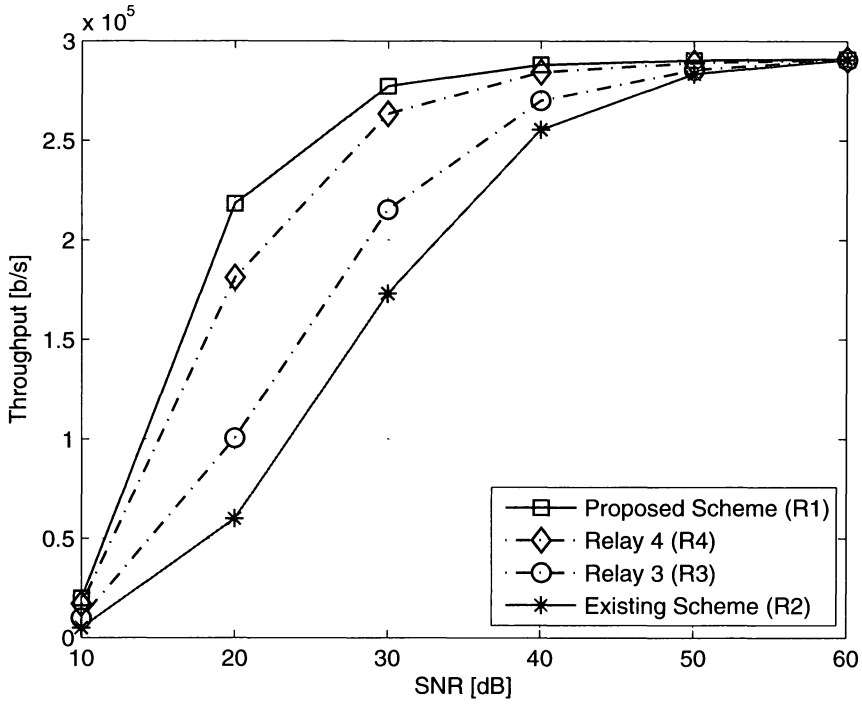

Figure 4.9: Go-Back-N ARQ with S_{packet} of 128 bytes.

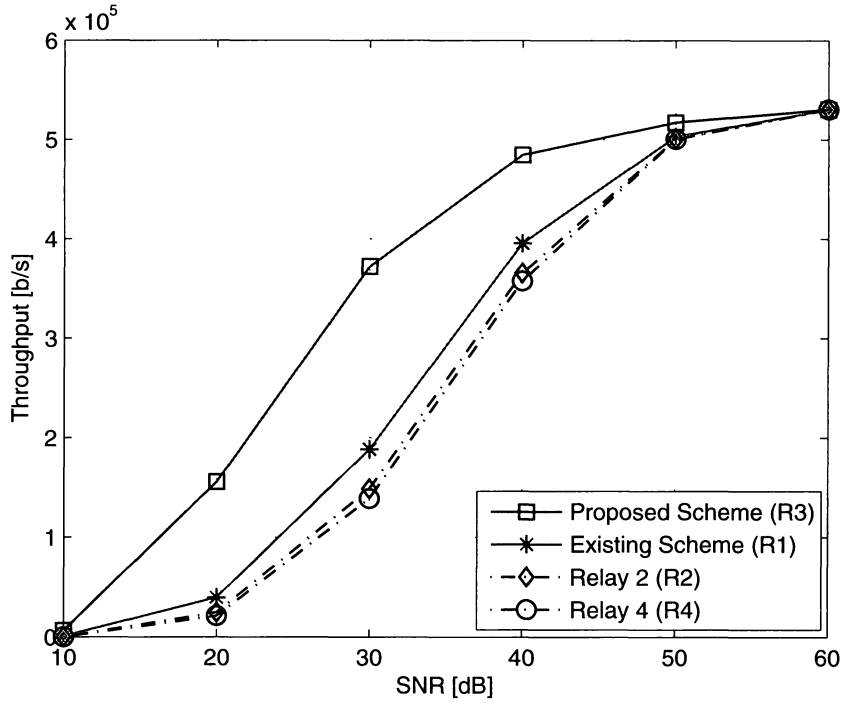

Figure 4.10: Go-Back-N ARQ with S_{packet} of 256 bytes.

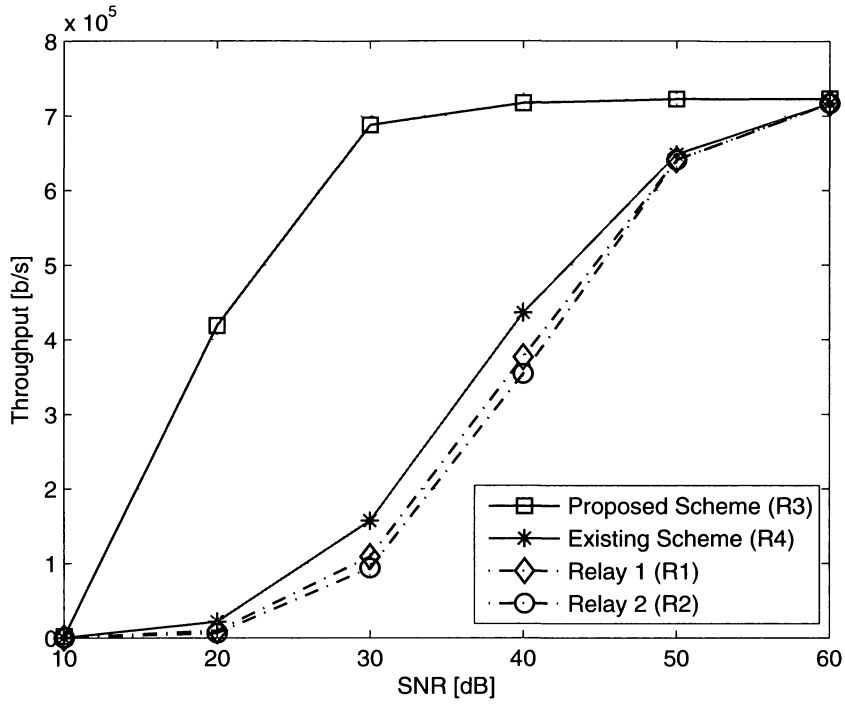

Figure 4.11: Go-Back-N ARQ with S_{packet} of 512 bytes.

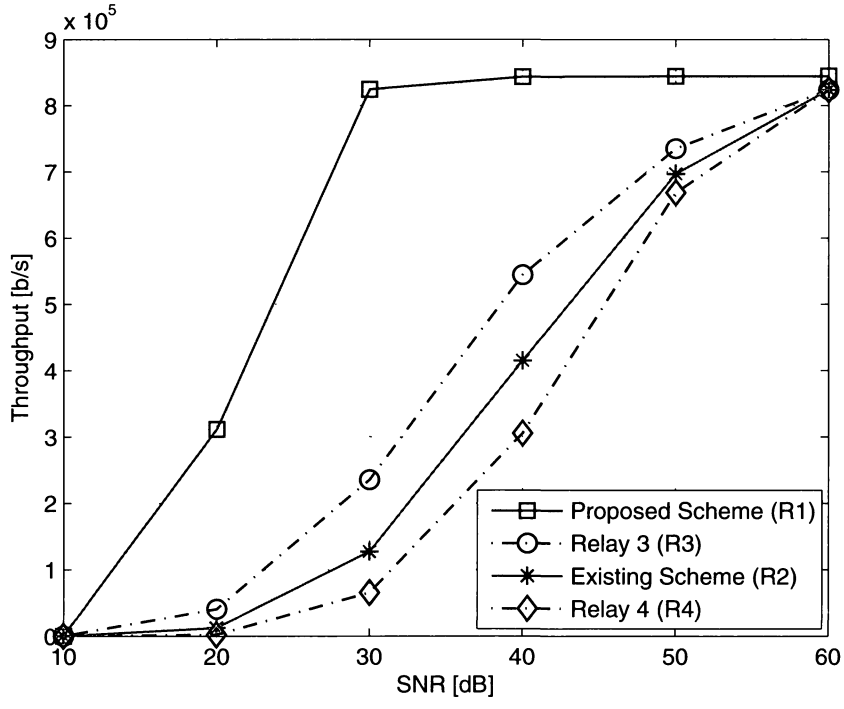

Figure 4.12: Go-Back-N ARQ with S_{packet} of 1024 bytes.

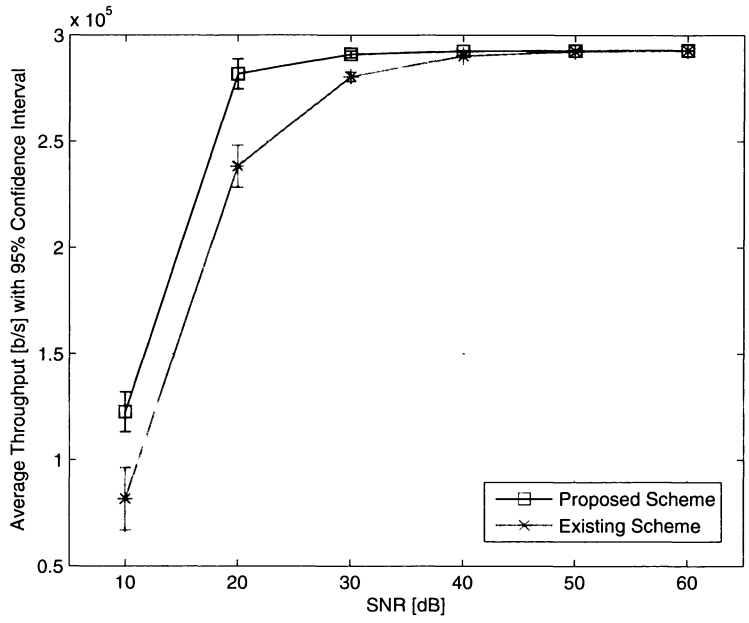

Figure 4.13: Throughput comparison of existing and proposed schemes with S_{packet} of 128 bytes at 95% Confidence Interval.

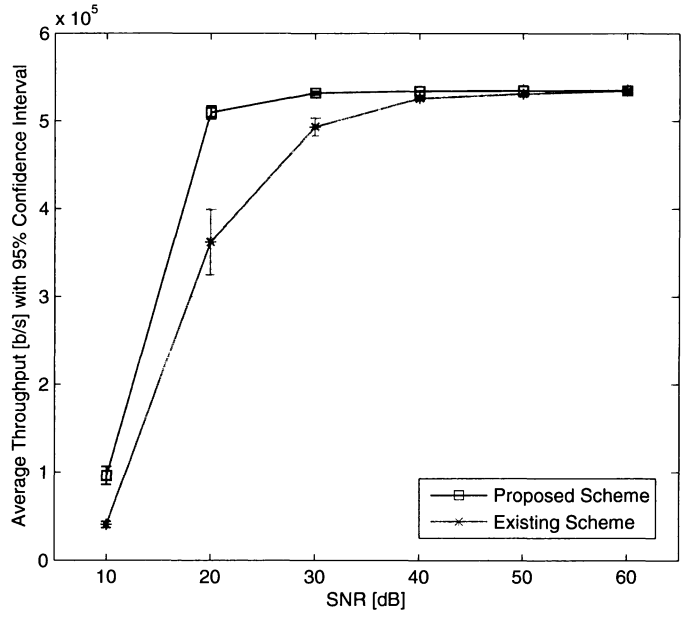

Figure 4.14: Throughput comparison of existing and proposed schemes with S_{packet} of 256 bytes at 95% Confidence Interval.

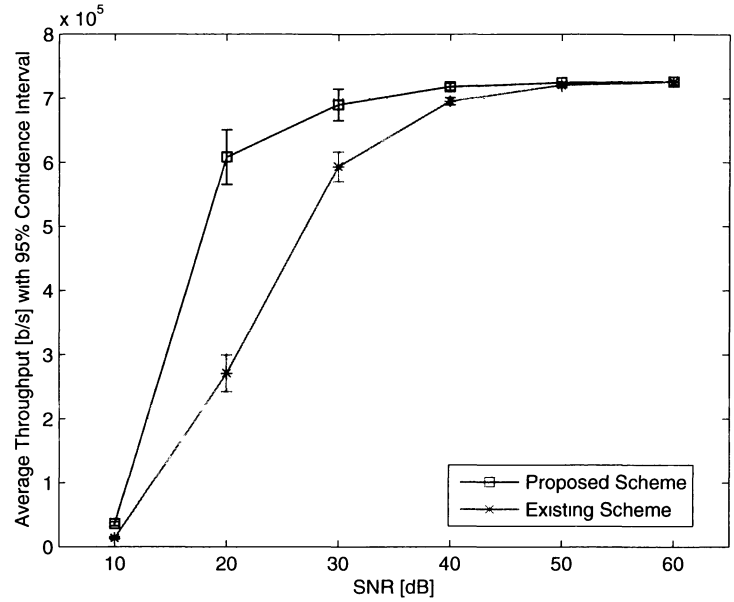

Figure 4.15: Throughput comparison of existing and proposed schemes with S_{packet} of 512 bytes at 95% Confidence Interval.

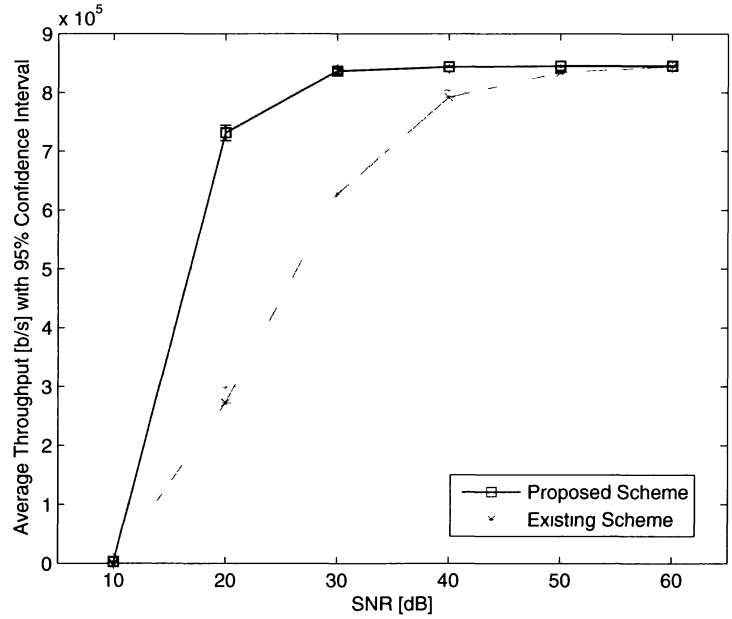

Figure 4.16: Throughput comparison of existing and proposed schemes with S_{packet} of 1024 bytes at 95% Confidence Interval.

The findings confirm the previous results and reiterate that the best relay selected under the proposed JAQS scheme offers higher throughput in comparison with the existing scheme. The confidence interval graphs demonstrates that the improved performance in JAQS is statistically significant and reliable as the throughput values of the relays selected under the proposed scheme and relays selected under the existing scheme population should fall within these intervals 95% of the time. The overlap of the confidence intervals occurs only at the higher SNR values as the throughput values converge between the two compared schemes with the error rate decreasing as a consequence of lower BER. We also find that the 95% confidence interval limits are within 10% of the mean affirming that the variance is limited and the average values are representative of the simulated results.

4.3.4 Comparison of Throughput from Retransmission Schemes

We compare the throughput performance of the proposed selected relays from both SR and GBN schemes, and this is presented in Figures 4.17 to 4.20.

From the figures, we observe that the throughput from the GBN ARQ scheme is lower than that of the SR scheme at low SNR values. This is due to the fact that any error in transmission would require the retransmission of all packets within the window in the GBN ARQ scheme. However, at higher SNR values, the throughput from GBN converge to the throughput values in SR as the BER will be very low in high SNR, and consequently, the requirement for retransmission will be substantially reduced. Therefore, at high SNRs, the GBN ARQ scheme performs similar to the SR ARQ scheme.

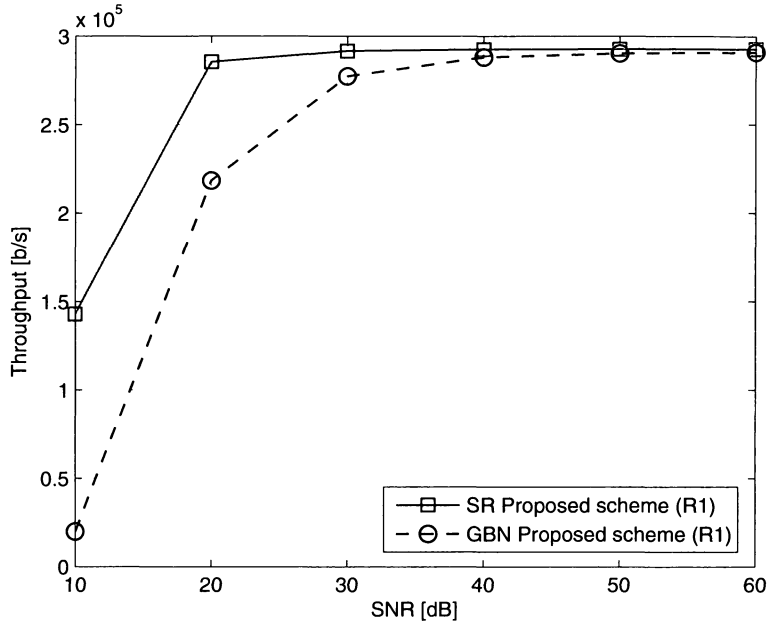

Figure 4.17: Comparison of Selective Repeat and Go-Back-N retransmission schemes with S_{packet} of 128 bytes.

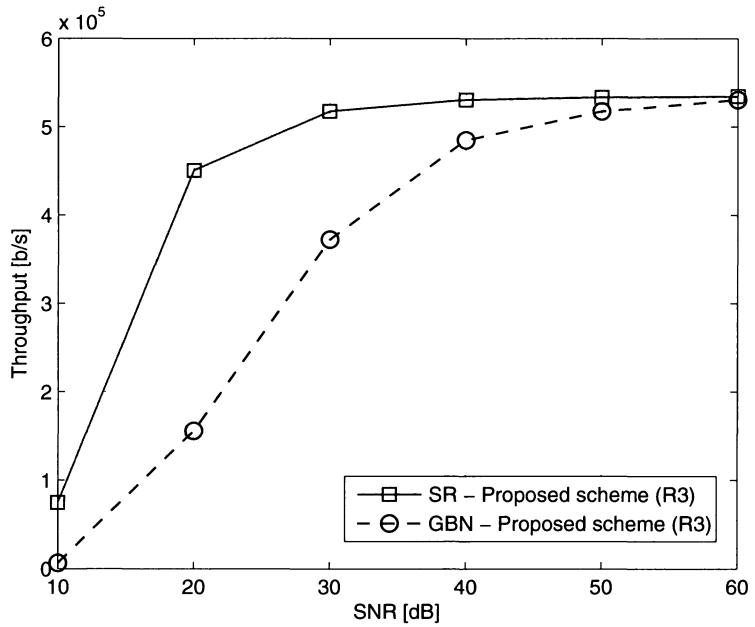

Figure 4.18: Comparison of Selective Repeat and Go-Back-N retransmission schemes with S_{packet} of 256 bytes.

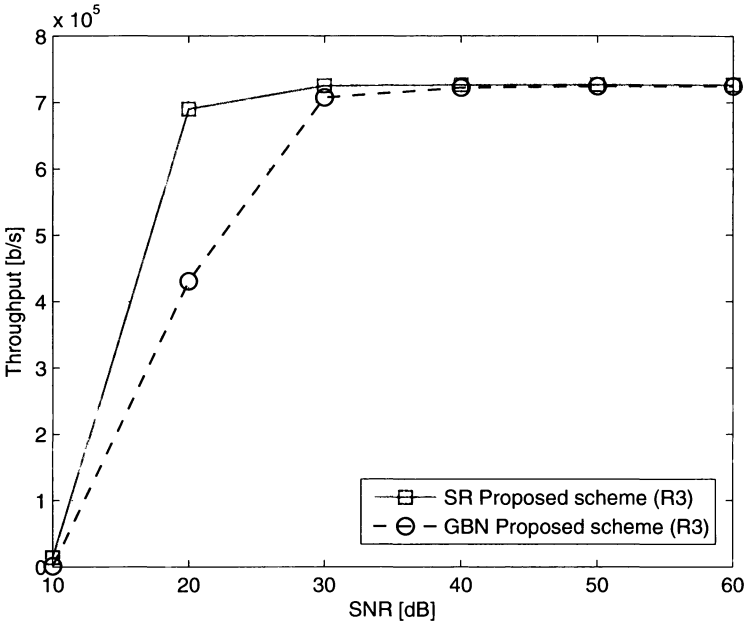

Figure 4.19: Comparison of Selective Repeat and Go-Back-N retransmission schemes with S_{packet} of 512 bytes.

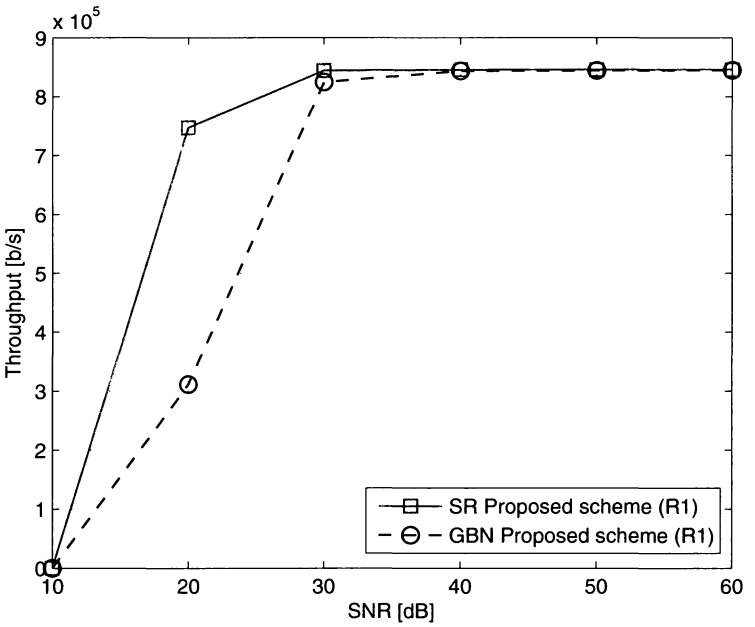

Figure 4.20: Comparison of Selective Repeat and Go-Back-N retransmission schemes with S_{packet} of 1024 bytes.

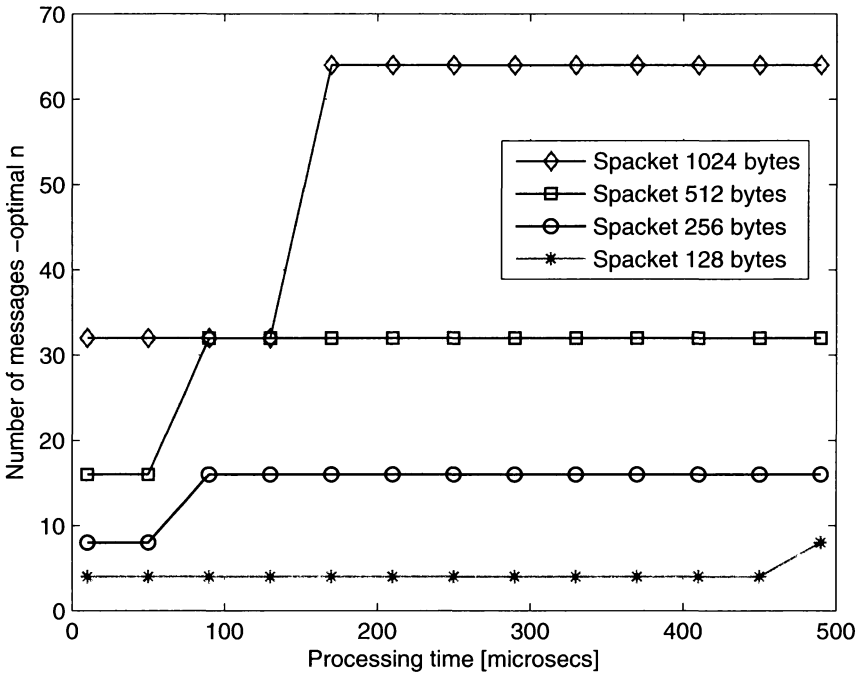

Figure 4.21: Change in optimal n for different processing times.

4.4 Effect of Processing Time on the Optimal n Value

We also considered the effect of processing time on the optimal number of messages (optimal n) and the result is presented in Figure 4.21. Since there are often heterogeneous wireless devices in a wireless network with different processing capabilities (e.g., different CPUs and memories), the processing time for security services will be different which impacts on the selection of the optimal number of messages in the Merkle tree. In Figure 4.21, we observe that if the processing time is increased, the optimal n value changes for all packet sizes (S_{packet}). Therefore, the optimal n value will be different for each scenario and has to be calculated for each specific case to obtain the highest throughput.

4.5 Summary

In this chapter, we provided the simulation results that serve as vindication of JAQS. We show that the optimal n value provides the highest throughput in comparison with other n values, and that it has to be calculated for each specific case scenario. The above simulation experiments also show that the relay selected under JAQS offers better throughput performance in comparison with the relay selected under the existing scheme, which is based on outage capacity and does not consider security aspects. This improvement in performance is due to the fact that the relay selected under JAQS has the lowest BER and consequently a higher throughput in comparison with the other relays. It is possible in some cases that both the schemes might potentially select the same relay as the best relay, but this can only be a random occurrence on account of the differing channel state information generated from the arbitrary topology arrangement.

The simulation illustrates the effectiveness of the proposed security enabled relay selection scheme considering authentication and throughput QoS in cooperative communication networks. The proposed JAQS enables the nodes to confirm that the messages and the acknowledgments received are authenticated, complete and have not been tampered with. We provide our conclusions in the next chapter.

Chapter 5

Conclusions and Future work

In this thesis, we propose a *prevention*-based technique, joint authentication and QoS scheme (JAQS), for proactive secure relay selection in cooperative communication taking into consideration authentication and QoS optimization. We make use of a combination of hash chains and Merkle trees to provide both end-to-end and hop-by-hop authentication and integrity protection in the cooperative communicative framework. Cooperative communication is vulnerable as the communication approach is dependent upon the integrity of the relays to ensure the authenticity and integrity of the messages they handle. For this purpose, the best relay has to be selected among the multitude of intermediate nodes that are available between the source and the destination. Furthermore, the destination and the relays have to confirm the identity of the source and verify that the message is complete and has not been tampered with. JAQS prevents the above vulnerabilities and selects the best relay on the basis of security-enabled throughput QoS performance. We provide the theoretical framework of JAQS and derive closed-form secured throughput equations. We further describe the implementation process and show that the proposed JAQS can jointly optimize the number of leaves or data chunks in the Merkle tree, corresponding to the number of S_2 packets, and perform secure proactive relay selection

in cooperative communication networks. Simulation results show that the proposed relay selection scheme, which provides authentication and integrity protection, selects a better relay outperforming the relay selected on the basis of the existing relay selection schemes derived from outage capacity that do not consider security.

In the future, it will be worthwhile to implement the cooperative communication framework in MANETs, and consider network topology control using JAQS. As indicated in Chapter 2.2, MANET shares many similar characteristics with cooperative communication including the absence of centralized control, frequent topology changes, resource constraints, etc. As MANET uses multi-hop network communication, it requires security in terms of both end-to-end and hop-by-hop authentication and message integrity. In addition, an inherent feature of MANET is its dynamic topology wherein the nodes constantly move and change according to the signal transmission and reception parameters, which ultimately affects the throughput QoS. Although many studies have been done on security and topology control in MANETs, our understanding is that they have been studied separately and no integrated approach has been attempted. However, it is apparent that these two issues are interrelated as any security scheme consumes network resources and again decreases the throughput QoS. Furthermore, the existing topology schemes assumes that the nature of the wireless channel is well known in advance, while in reality, the channel conditions change dynamically and it is not possible to have prior knowledge on the channel quality.

Therefore, the intention would be to evaluate how our proposed two-hop JAQS model could be adapted for the multi-hop MANET taking into consideration scalability with the increasing number of relay nodes and use it to effectively provide both end-to-end and hop-by-hop authentication and confirm that the messages have not been tampered with. As JAQS estimates the channel quality for each time slot on

a dynamic basis with no requirement to have any prior knowledge on the condition of the wireless channel, it could be well suited for the requirements in MANETs. By integrating with a proper topology control approach, malicious nodes could also be excluded furthermore increasing network security in MANETs. All these are proposed to be studied and addressed in our future work.

List of References

[1] M. Dohler, D.-E. Meddour, S.-M. Senouci, and A. Saadani, "Cooperation in 4G - hype or ripe?," *IEEE Technology and Society Magazine*, vol. 27, pp. 13–17, Spring 2008.

[2] M. Dohler and Y. Li, *Cooperative communications: Hardware, Channel & PHY.* U.K.: John Wiley & Sons, 2010.

[3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. on Information Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[4] E. Erkip, A. Sendonaris, A. Stefanov, and B. Aazhang, "Cooperative communication in wireless systems," in *In advances in network information theory* (P. Gupta, G. Kramer, and A. J. van Wijngaarden, eds.), USA: AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 2004.

[5] G. D. Menghwar and C. F. Mecklenbräuker, "Cooperative versus non-cooperative communications," in *Proc. 2nd IEEE International Conference on Computer, Control and Communication. IC4'09*, (Karachi, Pakistan), Feb. 2009.

[6] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Magazine*, vol. 42, pp. 74–80, Oct. 2004.

[7] Y. L. Sun and Z. Han, "Trusted cooperative transmissions: turning a security weakness into a security enhancement," in *Securing wireless communications at the physical layer* (R. Liu and W. Trappe, eds.), USA: Springer, 2010.

[8] Y. Hong, W. Huang, F. Chiu, and C.-C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Processing Magazine*, vol. 24, pp. 47–57, May 2007.

[9] E. Beres and R. Adve, "Relay selection in cooperative networks," in *Cooperative communications for improved wireless network transmission: Framework for virtual antenna array applications* (M. Uysal, ed.), USA: Information Science Reference, 2010.

[10] A. Bletsas, "Orthogonal opportunistic relaying for cooperative wireless communications," in *Cooperative wireless communications* (Y. Zhang, H. Chen, and M. Guizani, eds.), USA: Auerbach Publications, 2009.

[11] T. M. Cover and A. A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Information Theory*, vol. 25, pp. 572–584, Sep. 1979.

[12] E. C. V. D. Meulen, "Three terminals communication channels," *Advances in Applied Probability*, vol. 3, pp. 120–154, Spring 1971.

[13] A. Sendonaris, E. Erkip, and B. Aazhang, "Increasing uplink capacity via user cooperation diversity," in *Proc. of IEEE International Symposium on Information Theory*, (Cambridge, USA), Aug. 1998.

[14] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - Part I: System description," *IEEE Trans. on Commun.*, vol. 51, pp. 1927–1938, Nov. 2003.

[15] J. Laneman and G. Wornell, "Energy-efficient antenna sharing and relaying for wireless networks," in *Proc. of IEEE Wireless Communication and Networking Conference. WCNC'00*, Sep. 2000.

[16] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Cooperative communications," in *Cooperation in wireless networks: Principles and applications* (F. H. P. Fitzek and M. D. Katz, eds.), USA: Springer, 2006.

[17] Y. Li, B. Vucetic, Z. Chen, and J. Yuan, "An improved relay selection scheme with hybrid relaying protocols," in *Proc. of IEEE Global Telecommunications Conference. GLOBECOM'07*, (Washington DC, USA), Nov. 2007.

[18] K. Chen and R. Prasad, *Cognitive radio networks.* U.K.: John Wiley & Sons, 2009.

[19] M. Dohler, D.-E. Meddour, S.-M. Senouci, and H. Moustafa, "Cooperative communication system architectures for cellular networks," in *Cooperative communications for improved wireless network transmission: Framework for virtual*

antenna array applications (M. Uysal, ed.), USA: Information Science Reference, 2010.

[20] K. Hwang, Y. Ko, and M. Alouini, "A study of multi-hop cooperative diversity system," in *Proc. Asia-Pacific Conference on Communications. APCC'06*, (Busan, Korea), Aug. 2006.

[21] R. U. Nabar, H. Bölcskei, and F. W. Kneubühler, "Fading relay channels: Performance limits and space-time signal design," *IEEE Journal on Selected Areas in Commun.*, vol. 22, pp. 1099–1109, Aug. 2004.

[22] A. Avestimehr and D. Tse, "Outage capacity of the fading relay channel in the low-SNR regime," *IEEE Trans. on Information Theory*, vol. 53, pp. 1401–1415, Apr. 2007.

[23] J. Hu and N. Beaulieu, "Closed-form expressions for the outage and error probabilities of decode-and-forward relaying in dissimilar rayleigh fading channels," in *IEEE International Conference on Communication. ICC'07*, (Glasgow, U.K.), June 2007.

[24] Y. Zhao, R. Adve, and T. Lim, "Outage probability at arbitrary SNR with cooperative diversity," *IEEE Commun. Letters*, vol. 9, pp. 700–702, Aug. 2005.

[25] J. Hu and N. Beaulieui, "Performance analysis of decode-and-forward relaying with selection combining," *IEEE Commun. Letters*, vol. 11, pp. 489–491, June 2007.

[26] K. Hwang, Y. Ko, and M. Alouini, "Performance analysis of incremental relaying with relay selection and adaptive modulation over non-identically distributed cooperative paths," in *Proc. of IEEE International Symposium on Information Theory*, (Toronto, Canada), July 2008.

[27] S. Ikki and M. Ahmed, "Performance analysis of incremental relaying cooperative diversity networks over rayleigh fading channels,"

[28] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. on Wireless Commun.*, vol. 6, pp. 3450–3460, Sep. 2007.

[29] Z. Ding, Y. Gong, T. Ratnarajah, and C. F. N. Cowan, "Opportunistic cooperative diversity protocols for wireless networks," in *Proc. of IEEE Workshop on Information Theory for Wireless Networks*, (Solstrand, Norway), July 2007.

[30] A. Bletsas, H. Shin, M. Z. Win, and A. Lippman, "To relay or not to relay? cooperative diversity with opportunistic relaying," in *Proc. of IEEE Wireless Communications and Networking Conference. WCNC'06*, (Las Vegas, USA), Apr. 2006.

[31] W. Ni, G. Shen, S. Jin, T. Fahldieck, and R. Muenzner, "Cooperative relay in IEEE 802.16j MMR," Tech. Rep. IEEE C802.16j-06_006r1, Alcatel, http://ieee802.org/16/relay/contrib/C80216j-06_006r1.pdf, May 2006.

[32] P. H. J. Chong, F. Adachi, S. Hamalainen, and V. Leung, "Technologies in multihop cellular network," *IEEE Commun. Magazine*, vol. 45, pp. 64–65, Sep. 2007.

[33] Q. Zhang, Q. Chen, F. Yang, X. Shen, and Z. Niu, "Cooperative and opportunistic transmission for wireless ad hoc networks," *IEEE Network*, vol. 21, pp. 14–20, Jan./Feb. 2007.

[34] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[35] V. Stankovic, A. Host-Madsen, and Z. Xiong, "Cooperative diversity for wireless ad hoc networks," *IEEE Signal Processing Magazine*, vol. 23, pp. 37–49, Sep. 2006.

[36] A. Scaglione and Y. Hong, "Opportunistic large arrays: Cooperative transmission in wireless multihop ad hoc networks to reach far distances," *IEEE Trans. on Signal Processing*, vol. 51, Aug. 2003.

[37] I. Krikidis and J. S. Thompson, "Overview of amplify-and-forward relaying," in *Cooperative communications for improved wireless network transmission: Framework for virtual antenna array applications* (M. Uysal, ed.), USA: Information Science Reference, 2010.

[38] A. Scaglione, D. L. Goeckel, and J. N. Laneman, "Cooperative communications in mobile ad hoc networks: Rethinking the link abstraction," in *Distributed antenna systems: Open architecture for future wireless communications* (H. Yu, Y. Zhang, and J. Luo, eds.), USA: Auerbach Publications, 2007.

[39] A. Scaglione, D. Goeckel, and J. N. Laneman, "Cooperative communications in mobile ad hoc networks," *IEEE Signal Processing Magazine*, vol. 23, pp. 18–20, Sep. 2006.

[40] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal Selected Areas in Commun.*, vol. 24, pp. 659–672, Mar. 2006.

[41] A. S. Ibrahim, A. K. Sadek, W. Su, and K. J. R. Liu, "Cooperative communications with relay-selection: When to cooperate and whom to cooperate with?," *IEEE Trans. on Wireless Commun.*, vol. 7, pp. 2814–2827, July 2008.

[42] K. Woradit, T. Q. S. Quek, W. Suwansantisuk, H. Wymeersch, L. Wuttisittikulkij, and M. Z. Win, "Outage behavior of selective relaying schemes," *IEEE Trans. on Wireless Commun.*, vol. 8, pp. 3890–3895, Aug. 2009.

[43] E. Beres and R. Adve, "Selection cooperation in multi-source cooperative networks," *IEEE Trans. on Wireless Commun.*, vol. 7, pp. 118–127, Jan. 2008.

[44] H. Shan, W. Zhuang, and Z. Wang, "Distributed cooperative MAC for multihop wireless networks," *IEEE Commun. Magazine*, vol. 47, pp. 126–133, Feb. 2009.

[45] T. C.-Y. Ng and W. Yu, "Joint optimization of relay strategies and resource allocations in cooperative cellular networks," *IEEE Journal on Selected Areas in Commun.*, vol. 25, pp. 328–339, Feb. 2007.

[46] J. Cai, X. Shen, J. W. Mark, and A. S. Alfa, "Semi-distributed user relaying algorithm for amplify-and-forward wireless relay networks," *IEEE Trans. on Wireless Commun.*, vol. 7, pp. 1348–1357, Apr. 2008.

[47] A. S. Ibrahim, A. K. Sadek, W. Su, and K. J. R. Liu, "Relay selection in multi-node cooperative communications: When to cooperate and whom to cooperate with?," in *Proc. of IEEE Global Telecommunications Conference. GLOBECOM'06*, (San Francisco, USA), Nov. 2006.

[48] A. Bletsas, A. Lippman, and D. P. Reed, "A simple distributed method for relay selection in cooperative diversity wireless networks, based on reciprocity and channel measurements," in *Proc. of 61st IEEE Vehicular Technology Conference. VTC'05*, (Stockholm, Sweden), May 2005.

[49] Y. Zou, B. Zheng, W. Zhu, and J. Cui, "An optimal relay selection scheme for cooperative diversity," in *Proc. of 9th IEEE Conference on Signal Processing. ICSP'08*, (Beijing, China), Oct. 2008.

[50] J. Luo, R. S. Blum, L. Cimini, L. Greenstein, and A. Haimovich, "Power allocation in a transmit diversity system with mean channel gain information," *IEEE Commun. Letters*, vol. 9, pp. 2415–2525, July 2005.

[51] J. Luo, R. S. Blum, L. J. Cimini, L. J. Greenstein, and A. M. Haimovich, "Link-failure probabilities for practical cooperative relay networks," in *Proc. of 61st IEEE Vehicular Technology Conference. VTC'05*, (Stockholm, Sweden), May 2005.

[52] V. Sreng, H. Yanikomeroglu, and D. Falconer, "Relayer selection strategies in cellular networks with peer-to-peer relaying," in *Proc. of 58th IEEE Vehicular Technology Conference. VTC'03*, (Florida, USA), Oct. 2003.

[53] B. Zhao and M. C. Valenti, "Practical relay networks: A generalization of hybrid-ARQ," *IEEE Journal on Selected Areas in Commun.*, vol. 23, pp. 7–18, Jan. 2005.

[54] M. Zorzi and R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: multihop performance," *IEEE Trans. on Mobile Computing*, vol. 2, pp. 337–348, Oct./Dec. 2003.

[55] M. Zorzi and R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," *IEEE Trans. on Mobile Computing*, vol. 2, pp. 349–365, Oct./Dec. 2003.

[56] A. Ibrahim, A. Sadek, W. Su, and K. Liu, "Cooperative communications with partial channel state information: when to cooperate?," in *Proc. of IEEE Global Telecommunications Conference. GLOBECOM'05*, (St.Louis, USA), Nov. 2005.

[57] J. Luo, R. S. Blum, L. J. Cimini, L. J. Greenstein, and A. M. Haimovich, "New approaches for cooperative use of multiple antennas in ad hoc wireless networks," in *Proc. of 60th IEEE Vehicular Technology Conference. VTC'04*, (Los Angeles, USA), Sep. 2004.

[58] J. Yuan, Y. Li, and L. Chu, "Differential modulation and relay selection with detect-and-forward cooperative relaying," *IEEE Trans. on Vehicular Technology*, vol. 59, pp. 261–268, Jan. 2010.

[59] Y. Zhao, R. Adve, and T. Lim, "Improving amplify-and-forward relay networks: optimal power allocation versus selection," *IEEE Trans. on Wireless Commun.*, vol. 6, p. 31143123, Aug. 2007.

[60] E. Beres and R. Adve, "On selection cooperation in distributed networks," in *Proc. 40th Annual Conference on Information Sciences and Systems. CISS'06*, (Princeton, USA), Mar. 2006.

[61] E. Beres and R. Adve, "Cooperation and routing in multi-hop networks," in *Proc. of IEEE International Conference on Communication. ICC'07*, (Glasgow, U.K.), June 2007.

[62] L. Zhang and L. Cimini, "Cooperative network coding in selective decode-and-forward networks with multiple source-destination pairs," in *Proc. 42nd Annual Conference on Information Sciences and Systems. CISS08*, (Princeton, USA), Mar. 2008.

[63] E. Beres and R. Adve, "Outage probability of selection cooperation in the low to medium SNR regime," *IEEE Commun. Letters*, vol. 11, pp. 589–597, July 2007.

[64] M. Yuksel and E. Erkip, "Information theoretical limits on cooperative communications," in *Cooperative communications for improved wireless network transmission: Framework for virtual antenna array applications* (M. Uysal, ed.), USA: Information Science Reference, 2010.

[65] B. A. Forouzan, *Cryptography and network security.* USA: McGraw-Hill, 2008.

[66] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless network security* (Y. Xiao, X. Shen, and D. Du, eds.), USA: Springer - Signals and Communication Technology, 2007.

[67] G. Schäfer, *Security in fixed and wireless networks - An introduction to securing data networks.* U.K.: John Wiley & Sons, 2003.

[68] Y. Mao and M. Wu, "Security issues in cooperative communications: Tracing adversarial relays," in *Proc. of IEEE International Conference on Acoustic, Speech, and Signal Processing. ICASSP'06*, (Toulouse, France), May 2006.

[69] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. on Information Forensics and Security*, vol. 2, pp. 198–212, June 2007.

[70] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.

[71] L. Lai and H. E. Gamal, "Cooperative secrecy: The relay-eavesdropper channel," in *IEEE International Symposium on Information Theory. ISIT'07*, (Nice, France), June 2007.

[72] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of 6th ACM International Conference on Mobile Computing and Networking*, (Boston, USA), Aug. 2000.

[73] S. Buchegger and J. Le Boudec, "Performance analysis of the confidant protocol," in *Proc. of 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing*, (Lausanne, Switzerland), June 2002.

[74] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Sustaining cooperation in multi-hop wireless networks," in *Proc. of 2nd ACM Conference on Symposium on Networked Systems Design & Implementation*, (Boston, USA), May 2005.

[75] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: a case for cooperative jamming," in *Proc. of IEEE Global Telecommunications Conference. GLOBECOM'08*, (New Orleans, USA), Dec. 2008.

[76] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing. ICASSP'09*, (Dallas, USA), Mar. 2009.

[77] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in *Proc. of 46th Annual Allerton Conference on Communication, Control and Computing*, (Monticello, USA), Sep. 2008.

[78] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. of IEEE Workshop on Statistical Signal Processing. SSP'09*, (Cardiff, U.K.), Aug. 2009.

[79] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Processing*, vol. 58, pp. 1875–1888, Mar. 2010.

[80] S. Makda, A. Choudhary, N. Raman, T. Korakis, Z. Tao, and S. Panwar, "Security implications of cooperative communications in wireless networks," in *Proc. IEEE Sarnoff Symposium*, (Princeton, USA), Apr. 2008.

[81] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *Proc. of 28th IEEE Conference on Computer Communications. INFOCOM'09*, (Rio de Janeiro, Brazil), Apr. 2009.

[82] S. Dehnie, H. T. Sencar, and N. Memon, "Detecting malicious behavior in cooperative diversity," in *Proc. Conference on Information Sciences and Systems. CISS'07*, (Baltimore, USA), Mar. 2007.

[83] Z. Han and Y. L. Sun, "Self-learning cooperative transmission - coping with unreliability due to mobility, channel estimation errors, and untrustworthy nodes," in *Proc. of IEEE Global Communications Conference. GLOBECOM'07*, (Washington DC, USA), Dec. 2007.

[84] Z. Han and Y. Sun, "Securing cooperative transmission in wireless communications," in *Proc. of the ACM MobiQuitous Conference.*, (Philadelphia, USA), Aug. 2007.

[85] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. on Wireless Commun.*, vol. 8, pp. 806–815, Feb. 2009.

[86] N. Aboudagga, M. Refaei, M. Eltoweissy, L. DaSilva, and J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," in *Proc. of the 1st ACM international workshop on Quality of Service & Security in Wireless and Mobile Networks. Q2SWinet'05*, (Montreal, Canada), Oct. 2005.

[87] H. Tang, M. Salmanian, and C. Chang, "Strong authentication for tactical mobile ad hoc networks," *Technical Memorandum, Defence Research & Development Canada*, July 2007.

[88] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770–772, Nov. 1981.

[89] R. C. Merkle, "A certified digital signature," 1979.

[90] T. Heer, S. Götz, O. G. Morchon, and K. Wehrle, "ALPHA: an adaptive and lightweight protocol for hop-by-hop authentication," in *Proc. of the ACM CoNEXT Conference*, (Madrid, Spain), Dec. 2008.

[91] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, Summer 2002.

[92] R. Akbani, T. Korkmaz, and G. Raju, "HEAP: Hop-by-hop efficient authentication protocol for mobile ad-hoc networks," in *Proc. ACM 10th Communications and Networking Simulation Symposium. CNS'07*, (Norfolk, USA), Mar. 2007.

[93] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *Proc. of 23rd International Conference on Distributed Computing Systems Workshops. ICDCSW'03*, (Rhode Island, USA), May 2003.

[94] B. Lu and U. Pooch, "A lightweight authentication protocol for mobile ad hoc networks," in *Proc. of International Conference on Information Technology, Coding and Computing. ITCC'05*, (Las Vegas, USA), April 2005.

[95] G. Raju and R. Akbani, "Mobile ad hoc networks security," in *Proc. of Annual Review of Communications. IEC*, Oct. 2005.

[96] G. Raju and R. Akbani, "Authentication in wireless networks," in *Proc. of 40th Hawaii International Conference on System Sciences. HICSS'07*, Jan. 2007.

[97] P. G. Bradford and O. V. Gavrylyako, "Foundations of security for hash chains in ad hoc networks," in *Proc. of 23rd International Conference on Distributed Computing Systems Workshops. ICDCSW03*, (Rhode Island, USA), May 2003.

[98] S. Lee, H. Kim, and K. Chung, "Hash-based secure sensor network programming method without public key cryptography," in *Proc. of the Workshop on World-Sensor-Web at International Conference on Embedded Networked Sensor Systems. SenSys06*, (Colorado, USA), Oct. 2006.

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

[100] S. Lin, D. J. Costello, and M. J. Miller, "Automatic repeat request error control schemes," *IEEE Commun. Magazine*, vol. 22, pp. 5–17, Dec. 1984.

Appendix A

Simuation Programs

```
%Sample of the matlab program used for simulation
%This script generates four nodes randomly, calculates the outage capacity,
%BER, throughput (for selective repeat retransmission) for all the relays for a given
    packet size using the %optimal no of packets by varying the SNR

SNR_dB = 10:10:60; % transmit SNR in the range of 10-60 dB
SNR=10.^(SNR_dB./10);
size_snr = size(SNR,2);

% randomly generates the coordinates of four relay nodes
X = zeros(1,4);
Y = zeros(1,4);
i=1;
while i<5
   X(i) = randi([0 1000],1,1);
   Y(i) = randi([0 300],1,1);
   if (X(i)==0 & Y(i)==0) |(X(i)==1000 & Y(i)==0)
      i =i;
   else
      i=i+1;
   end
end

number_relay = size(X,2);
dist_SD = 1000;
pathloss = 3.5;

% Calculating the distance of each relay from the source and the destination
SD_N=(dist_SD/dist_SD)^pathloss;
for i = 1 : number_relay
   SR(i) = sqrt((0 - X(i))^2 + (0 - Y(i))^2);
   RD(i) = sqrt((1000 - X(i))^2 + (0 - Y(i))^2);
end
```

```
SR_N1 = (SR./dist_SD); % normalised distance for tput calcn
RD_N1 = (RD./dist_SD);
SR_N = SR_N1.^pathloss;
RD_N = RD_N1.^pathloss;

% calculating the outage capacity, BER for each relay for different SNR
% values
Cap_ssdf = zeros(4,size_snr);
for l =1:4
   for k = 1: size_snr
      [Cap_ssdf(l,k),Cap_DC(k) BER(l,k) Pe_SD(k)]= error_SSDF(SD_N,SR_N(l),RD_N(l),
          SNR(k));
    end
end
[max_cap, relay]= max(Cap_ssdf) % determines which relay has maximum outage
    capacity
spack = 512; % packet size
n =16; % optimal no of packets in the merkle tree

% calculating the throughput for each relay at different snr using
% selective repeat retransmission
[RT] = tput_varyn(SR_N1,RD_N1,BER,spack,n);
[max_RT, relay]= max(RT) %determines which relay has maximum throughput

% This function calculates the outage capacity and BER for each relay for
% different SNR values
% Inputs:
% SD_N: Normalized distance between source and destination
% SR_N: Normalized distance between source and relay
% RD_N: Normalized distance between relay and destination
% SNR: Signal to Noise Ratio
% Outputs:
% Cap_ssdf: Outage capacity for each relay
% Cap_dc: Outage capacity for Direct Communication
% BER: Bit Error Rate for all relays
% Pe_SD: Bit Error Rate for Direct Communication

function [Cap_ssdf Cap_dc BER Pe_SD]= error_SSDF(SD_N,SR_N,RD_N,SNR)
EPS = 0.01; % outage probability
% calculating outage probability 'result'
vMAX = 1;
vMIN = 0;
while vMIN < vMAX
   vmid = (vMAX + vMIN) / 2;
   w = exp(2 * log(vmid) - (log(vmid)^2)*SNR);
   result = 1 - vmid + (w^(SR_N + RD_N) *(vmid^(1-RD_N)-1))/(1-RD_N);

   if abs(EPS - result)<(EPS * 0.001)
      result;
      break
```

```
    end
    if result > EPS
       vMIN = vmid;
    else
       vMAX = vmid;
    end
 end
 vEPS = vmid;

% outage capacity Cap_ssdf for relays

Cap_ssdf = log2(1+ SNR*log(1/vEPS));
Cap_dc = log2(1+ SNR*log(1/(1-EPS))); % outage capacity for direct communication

% calculating BER for cooperative transmission 'BER'

Y_SD = SNR/SD_N;
Y_SR = SNR/SR_N;
Y_1 = SNR/SD_N;
Y_2 = (SNR/RD_N) ;
 Pe_SD = 0.5 * ( 1 - sqrt(Y_SD/(1+Y_SD))); % BER for DC 'Pe_SD'
 Pout_SR = 1 - exp(-1*((2)^(2* Cap_ssdf)-1)/Y_SR);
 Pe_MRC = 0.5 * ( 1 + 1/(Y_2 - Y_1) * (Y_1/sqrt(1 + (1/Y_1)) - Y_2/sqrt(1 + (1/
     Y_2))));
 BER = (Pout_SR * Pe_SD) + ((1 - Pout_SR) * Pe_MRC);

% This function calculates the throughput for each relay using selective
% repeat retransmission.
% Inputs:
% SR_N1: Normalized distance between source and relay
% RD_N1: Normalized distance between relay and destination
% BER: Bit Error Rate
% Spacket: Packet Size
% n: Number of S2 packets
% Outputs:
% RT: Throughput for all relays for different SNRs

function [RT]=tput_varyn(SR_N1, RD_N1,BER,Spacket,n)
HASHSIZE = 20; % # of bytes in a hash
Sh = HASHSIZE; % SHA-1 hash
S1 = 2 * HASHSIZE;
A1 = 2 * HASHSIZE;
RCOUNTS = 4;
relays = zeros(2,RCOUNTS);
relays(1,:)=SR_N1;
relays(2,:)=RD_N1;
RELAYS = transpose(relays);
Tproc = 10e-6; % 10 micro secs Processing time for S1 A1 S2 A2
SMT = 10e-6; % Time required to build the Merkle Tree in Source
DMT = 10e-6; % Time required to build the Merkle Tree in the destination
```

```
iter = 1;
SNR_dB = 10:10:60;
SNR=10.^(SNR_dB./10);
size_snr = size(SNR,2);

for x=1:size(SNR,2)
  fprintf('Computing for SNR %d\n', SNR_dB(x));
   S2 = Spacket;
   A2 = (1 + (ceil(log2(n)))) * HASHSIZE;
   PAYLOAD = (n * (Spacket - Sh * (ceil(log2(n)) + 1))) * 8;
   MaxR = 0;
   MaxThroughput = 0;

   for i = 1:1:RCOUNTS
   % time taken for the exchange of S1(TS1) and A1(TA1)packet
      TS1 = SMT + ...
            prop_delay_test(RELAYS(i, 1)) + ...
            packet_delay_test(S1) + ...
            prop_delay_test(RELAYS(i, 2)) + ...
            packet_delay_test(S1) + ...
            Tproc; % Processing time for S1 in destination
      fprintf('TS1 for Relay %d: %f\n', i, TS1);
      TA1 = DMT + ...
            prop_delay_test(RELAYS(i, 2)) + ... % From D to R
            packet_delay_test(A1) + ...
            prop_delay_test(RELAYS(i, 1)) + ... % From R to S
            packet_delay_test(A1) + ...
            Tproc;
      fprintf('TA1 for Relay %d: %f\n', i, TA1);
   % time taken for the exchange of S2(TS2) and A2(TA2)packet
      TS2 = prop_delay_test(RELAYS(i, 1)) + ...
            packet_delay_test(Spacket * n) + ...
            prop_delay_test(RELAYS(i, 2)) + ...
            packet_delay_test(Spacket) + ...
            Tproc;
      fprintf('TS2 for Relay %d: %f\n', i, TS2);
      TA2 = prop_delay_test(RELAYS(i, 2)) + ...
            packet_delay_test(A2) + ...
            prop_delay_test(RELAYS(i, 1)) + ...
            packet_delay_test(A2) + ...
            2 * Tproc;
      fprintf('TA2 for Relay %d: %f\n', i, TA2);
      SUM = TS1 + TA1 + TS2 + TA2;
      fprintf('Total time for Relay %d: %f\n', i, SUM);

 % Calculating selective repeat throughput
      THROUGHPUT = PAYLOAD * ((1 - BER(i,x)) ^ (Spacket * 8)) / SUM;
      fprintf('Throughput for Relay %d: %f\n', i, THROUGHPUT);
      if MaxR == 0
         MaxR = i;
```

```
        MaxThroughput = THROUGHPUT;
      elseif MaxThroughput < THROUGHPUT
        MaxR = i;
        MaxThroughput = THROUGHPUT;
      end
      RT(i, iter) = THROUGHPUT;
      fprintf('********\n');
    end
  Ns(iter) = SNR_dB(x);
  iter = iter + 1;
  fprintf('Maximum throughput is for relay %d: %f\n', MaxR, MaxThroughput);
end

% This function calulates the packet delay for different packe size
% psize: number of bytes in the packet

function [del] = packet_delay_test(psize)
  DATA_RATE = 1e6;
  del = (psize * 8) / DATA_RATE;
end

% This function calculates the propagation delay between two points
% distance: distance between two points in meters

function [del] = prop_delay_test(distance)
  SPEED_OF_LIGHT = 3 * 1e8;
  del = distance / SPEED_OF_LIGHT;
end
```

```
% This script generates four nodes randomly, calculates the outage capacity,
% BER, throughput for selective repeat retransmission for all the relays for a
%given packet size, SNR and estimate the optimal number of packets

SNR_dB = 10:10:60;
SNR=10.^(SNR_dB./10);
size_snr = size(SNR,2);

% randomly generates the coordinates of four relay nodes
X = zeros(1,4);
Y = zeros(1,4);
i=1;
while i<5
  X(i) = randi([0 1000],1,1);
  Y(i) = randi([0 300],1,1);
  if (X(i)==0 & Y(i)==0) |(X(i)==1000 & Y(i)==0)
    i =i;
  else
    i=i+1;
  end
end
```

```
number_relay = size(X,2);
dist_SD = 1000;
pathloss = 3.5;
% Calculating the distance of each relay from the source and the
% destination
for i = 1 : number_relay
   SR(i) = sqrt((0 - X(i))^2 + (0 - Y(i))^2);
   RD(i) = sqrt((1000 - X(i))^2 + (0 - Y(i))^2);
end
size(RD);
SR_N1 = (SR./dist_SD);
RD_N1 = (RD./dist_SD);
SD_N1 = dist_SD/dist_SD;
SD_N=(dist_SD/dist_SD)^pathloss;
SR_N = SR_N1.^pathloss;
RD_N = RD_N1.^pathloss;

% calculating the outage capacity, BER for each relay for different SNR
% values
Cap_ssdf = zeros(4,size_snr);

for l =1:4
   for k = 1: size_snr
      [Cap_ssdf(l,k),Cap_DC(k) BER(l,k) Pe_SD(k)]= error_SSDF(SD_N,SR_N(l),RD_N(l),
          SNR(k));
    end
end

BER1 = BER(:,3);% selects the BER for SNR 30

% calculating the optimum number of data chunks and the corresponding throughput
%for each relay at given fixed snr using selective repeat retransmission
for i = 1:4 % for different packet sizes 128, 256, 512, 1024
   n=i+6;
   spack = 2^n;
   [Ns, RT,opt_n(i)] = tput_vpack(SR_N1,RD_N1,BER1,spack);
end

% This function returns the optimum no of data chunks and maximum
% throughput of the relay for a given packet size and SNR
% Inputs:
% SR_N1: Normalized distance between source and relay
% RD_N1: Normalized distance between relay and destination
% BER: Bit Error Rate
% Spacket: Packet Size
% n: Number of S2 packets
% Outputs:
% RT: Throughput for all relays for different SNRs
%opt_n: optimum no of data chunks
```

```
function [Ns, RT, opt_n]=tput_vpack(SR_N1,RD_N1,BER,Spacket)

HASHSIZE = 20; % # of bytes in a hash
Sh = HASHSIZE; % SHA-1 hash
S1 = 2 * HASHSIZE;
A1 = 2 * HASHSIZE;

RCOUNTS = 4;
relays = zeros(2,RCOUNTS);
relays(1,:)=SR_N1;
relays(2,:)=RD_N1;
RELAYS = transpose(relays);

Tproc = 100e-6; % 10 micro secs Processing time for S1 A1 S2 A2
SMT = 100e-6; % Time required to build the Merkle Tree in Source
DMT = 100e-6; % Time required to build the Merkle Tree in the destination

 n = 1; % initializing the no of data chunks
iter = 1;

while (n < 2^24)
    n = n * 2;
  fprintf('Computing for n = %d\n', n);

   S2 = Spacket;
   A2 = (1 + (ceil(log2(n)))) * HASHSIZE;

   PAYLOAD = (n * (Spacket - Sh * (ceil(log2(n)) + 1))) * 8;

   MaxR = 0;
   MaxThroughput = 0;

   for i = 1:1:RCOUNTS
      % For S1, there is no processing in the relay node. so there is no
      % processing delay.
      TS1 = SMT + ...
            prop_delay_test(RELAYS(i, 1)) + ...
            packet_delay_test(S1) + ...
            prop_delay_test(RELAYS(i, 2)) + ...
            packet_delay_test(S1) + ...
            Tproc; % Processing time for S1 in destination
      fprintf('TS1 for Relay %d: %f\n', i, TS1);

      TA1 = DMT + ...
            prop_delay_test(RELAYS(i, 2)) + ... % From D to R
            packet_delay_test(A1) + ...
            prop_delay_test(RELAYS(i, 1)) + ... % From R to S
            packet_delay_test(A1) + ...
            Tproc;
```

```
        fprintf('TA1_for_Relay_%d:_%f\n', i, TA1);

        TS2 = prop_delay_test(RELAYS(i, 1)) + ...
              packet_delay_test(Spacket * n) + ...
              prop_delay_test(RELAYS(i, 2)) + ...
              packet_delay_test(Spacket) + ...
              Tproc;
        fprintf('TS2_for_Relay_%d:_%f\n', i, TS2);

        TA2 = prop_delay_test(RELAYS(i, 2)) + ...
              packet_delay_test(A2) + ...
              prop_delay_test(RELAYS(i, 1)) + ...
              packet_delay_test(A2) + ...
              2 * Tproc;
        fprintf('TA2_for_Relay_%d:_%f\n', i, TA2);

        SUM = TS1 + TA1 + TS2 + TA2;
        fprintf('Total_time_for_Relay_%d:_%f\n', i, SUM);

         THROUGHPUT = PAYLOAD * ((1 - BER(i)) ^ (Spacket * 8)) / SUM;
        fprintf('Throughput_for_Relay_%d:_%f\n', i, THROUGHPUT);

        if MaxR == 0
           MaxR = i;
           MaxThroughput = THROUGHPUT;
        elseif MaxThroughput < THROUGHPUT
           MaxR = i;
           MaxThroughput = THROUGHPUT;
        end

        RT(i, iter) = THROUGHPUT;
        fprintf('********\n');
     end

    Ns(iter) = n;
    iter = iter + 1;
    fprintf('Maximum_throughput_is_for_relay_%d:_%f\n', MaxR, MaxThroughput);
end

for i =1:4
    [val, maxn(i)]= max(RT(i,:));
end

maxn = 2.^maxn;
opt_n = maxn(1);
```

%This script generates four nodes randomly, calculates the outage capacity, %BER, throughput (for selective repeat retransmission) for all the relays for a given packet size using the %optimal no of packets by varying the SNR

```
SNR_dB = 10:10:60; % transmit SNR in the range of 10−60 dB
SNR=10.^(SNR_dB./10);
size_snr = size(SNR,2);

% randomly generates the coordinates of four relay nodes
X = zeros(1,4);
Y = zeros(1,4);
i=1;
while i<5
   X(i) = randi([0 1000],1,1);
   Y(i) = randi([0 300],1,1);
   if (X(i)==0 & Y(i)==0) |(X(i)==1000 & Y(i)==0)
      i =i;
   else
      i=i+1;
   end
end

number_relay = size(X,2);
dist_SD = 1000;
pathloss = 3.5;

% Calculating the distance of each relay from the source and the destination
SD_N=(dist_SD/dist_SD)^pathloss;
for i = 1 : number_relay
   SR(i) = sqrt((0 − X(i))^2 + (0 − Y(i))^2);
   RD(i) = sqrt((1000 − X(i))^2 + (0 − Y(i))^2);
end
SR_N1 = (SR./dist_SD); % normalised distance for tput calcn
RD_N1 = (RD./dist_SD);
SR_N = SR_N1.^pathloss;
RD_N = RD_N1.^pathloss;

% calculating the outage capacity, BER for each relay for different SNR
% values
 Cap_ssdf = zeros(4,size_snr);
 for l =1:4
   for k = 1: size_snr
      [Cap_ssdf(l,k),Cap_DC(k) BER(l,k) Pe_SD(k)]= error_SSDF(SD_N,SR_N(l),RD_N(l),
          SNR(k));
    end
 end
[max_cap, relay]= max(Cap_ssdf) % determines which relay has maximum outage
    capacity
spack = 512; % packet size
n =16; % optimal no of packets in the merkle tree

% calculating the throughput for each relay at different snr using
% go back n retransmission
 [RT] = thput_rand_gbn(SR_N1,RD_N1,BER,spack,n);
```

```
[max_RT, relay]= max(RT) %determines which relay has maximum throughput

% This function calculates the throughput for each relay using go back n retransmission
% Inputs:
% SR_N1: Normalized distance between source and relay
% RD_N1: Normalized distance between relay and destination
% BER: Bit Error Rate
% Spacket: Packet Size
% n: Number of S2 packets
% Outputs:
% RT: Throughput for all relays for different SNRs

function [THROUGHPUT]=thput_rand_gbn(SR_N1, RD_N1,BER,Spacket,n)
HASHSIZE = 20; % # of bytes in a hash

% Spacket = 1024; % fixed-size packets
Sh = HASHSIZE; % SHA-1 hash
S1 = 2 * HASHSIZE; % Should this be 2 * HASHSIZE? -- Yes
A1 = 2 * HASHSIZE; % And this one too?
RCOUNTS = 1;
relays = zeros(2,RCOUNTS);
relays(1,:)=SR_N1;
relays(2,:)=RD_N1;
RELAYS = transpose(relays);

DATA_RATE = 1e6;
Tproc = 10e-6; % 10 micro secs Processing time for S1 A1 S2 A2
SMT = 10e-6; % Time required to build the Merkle Tree in Source
DMT = 10e-6; % Time required to build the Merkle Tree in the destination

S2 = Spacket;
A2 = (1 + (ceil(log2(n)))) * HASHSIZE;
PAYLOAD = (n * (Spacket - Sh * (ceil(log2(n)) + 1))) * 8;

    TS1 = SMT + ...
        prop_delay_test(SR_N1) + ...
        packet_delay_test(S1) + ...
        prop_delay_test(RD_N1) + ...
        packet_delay_test(S1) + ...
        Tproc; % Processing time for S1 in destination
    fprintf('TS1_for_Relay_%f\n', TS1);

    TA1 = DMT + ...
        prop_delay_test(RD_N1) + ... % From D to R
        packet_delay_test(A1) + ...
        prop_delay_test(SR_N1) + ... % From R to S
        packet_delay_test(A1) + ...
        Tproc;
    fprintf('TA1_for_Relay_%f\n', TA1);
```

```
        TS2 = prop_delay_test(SR_N1) + ...
              packet_delay_test(Spacket * n) + ...
              prop_delay_test(RD_N1) + ...
              packet_delay_test(Spacket) + ...
              Tproc;
        fprintf('TS2_for_Relay_%f\n',TS2);

        TA2 = prop_delay_test(RD_N1) + ...
              packet_delay_test(A2) + ...
              prop_delay_test(SR_N1) + ...
              packet_delay_test(A2) + ...
              2 * Tproc;
        fprintf('TA2_for_Relay_%f\n',TA2);

        SUM = TS1 + TA1 + TS2 + TA2;
        fprintf('Total_time_for_Relay_%f\n',SUM);


SNR_dB = 10:10:60;
SNR=10.^(SNR_dB./10);
size_snr = size(SNR,2);
  % Calculating go back n throughput
for x=1:size(SNR,2)

        Pc(x) = ((1 - BER(x)) ^ (Spacket * 8));

        L = 2 *(prop_delay_test(SR_N1) + prop_delay_test(RD_N1) + Tproc + ((Spacket*
            8)/DATA_RATE) + ((A2*8)/DATA_RATE))* DATA_RATE / (Spacket * 8)

        WS = round(L + 1)

       THROUGHPUT = (PAYLOAD * Pc(x)) / (SUM * (Pc(x) + (1-Pc(x)) * WS));

end

%calculates the throughput of each relay at different packet sizes by varying the no of data
      chunks for a fixed snr

BER = BER(:,2);
spack = [128, 256,512, 1024];
n =[4, 8, 16, 32];

for i=1:4
   for j=1:4
      [RT] = tput_varyn(SR_N1,RD_N1,BER,spack(j),n(i));
      [max_RT, relay]= max(RT);
      thru(i,j)=max_RT;
   end
end
```

```
plot(spack, thru(1, :),'-r*',spack, thru(2, :),'-rd',spack,thru(3, :),'-bs',spack, thru(4, :),'
    -ko');
legend('n=4','n=8','n=16','n=32');
grid on;
xlabel('Spacket [bytes]');
ylabel('Throughput [b/s]');
```