Diversity In Wireless Networks
Tooba Maryam, Amna Shamshad, Narmeen Falak, Maham Saeed

Abstract- This document is about techniques in which the performance and reliability of a wireless network can be improved. We will discuss the cooperative communication system, how it operates and its security issues. Also, the future of the diversity in wireless networks will be analysed [1]. In cooperative networks, the data is transmitted from sender to receiver via intermediate nodes called relays. The main objective is to consider the pros and cons of relaying techniques in order to improve wireless local area networks (WLANs) [2].

Keywords- Relaying; cooperative communication system; wireless networks

I. INTRODUCTION

The conventional wireless networks face issues such as interference, signal loss, signal fading and denial of service attacks. The cooperative networking uses cooperation among the involved nodes to achieve significant improvement in terms of the overall system capacity and performance[3]. It is a promising technique which enables efficient utilization of communication resources and mitigates signal fading in wireless networks [4].

Cooperative communication has two phases [5]

- Relay Selection
- Data Forwarding

There are various relay selection mechanisms such as proactive relay selection, reactive relay selection, opportunistic relay selection etc [6].

In proactive relay selections, the relays are selected prior to transmission, while in reactive relaying the relays are selected when needed. Reactive relaying is beneficial when there is failed transmission. In case of opportunistic relay selections, the relays are selected on demand.

II. OPERATION

Basic mechanism of cooperative communication is shown in figure 1

Figure 1 [7]

Cooperation can be used to achieve better data rates. In above figure, we suppose that node 1 is at a larger distance from destination. Since 802.11 rate adaptation allows the stations to adopt different rates based on distance and Signal to Noise Ratio (SNR). So, if node 1 establishes direct link with destination, the data rate will be very low. Conventionally, if an intermediate node with faster bit rate overhears data, it is obliged to drop it. Rather in cooperation, node 1 sends the data to destination via node 2 which is lies in between [8]. In this way, the data rate is improved and medium is released sooner. Simulation results as well as real implementations show that the cooperative communication system boosts the performance of the networks up to 5 times comparing with the exiting technology of IEEE 802.11.

A. Specifications of CoopNet

In CoopNet, cooperation among peers compliments traditional client-server communication. Specifically, CoopNet
addresses the problem cases of client-server communication. It plays its role only when needed and acts normally when direct links are working just fine. CoopNet, unlike other peer-to-peer systems, does not assume that helper nodes will be available all the time. For instance, helper nodes may only be willing to cooperate for a few minutes. Hence, network cannot solely depend on peer-to-peer communication [9].

In cooperative network, each wireless user is assumed to transmit its own data as well as act as a cooperative agent for another user. One might think this reduces the data rate of nodes. However, the spectral efficiency of each user improves, traffic jams are avoided and hence the overall system performance gets better.

### III. Security Issues in a Relay Based Network

Following are some of the security issues associated with cooperative networking and their proposed possible solutions.

**A. Packet dropping**

One potential security issue is associated with the relay deliberately not forwarding frames received from the source. Here, relay node denies service to the source by simply dropping the packets it receives [10].

**Solution:**

It is then up to the source to realize that this node is malicious and choose another one. If another relay does not exist, it can then transmit directly to the destination, albeit at a lower rate. The source could detect the responsiveness of a relay by imposing a timeout, after which if no acknowledgement from destination is received, it would blacklist that relay [22].

**B. Spoofing [24]**

A malicious node may deny service to sender by failing to forward data and spoofing an ACK on behalf of the destination, thereby making the source think that the data was received [11].

**Solution [25]:**

Cooperative networking may use a kind of RTS/CTS scheme to combat this issue. This means that the destination sends the CTS, and is aware that it is an intended recipient of the future frame. Thus, if it does not receive this frame in an allocated NAV period (due to the fact that the helper didn’t send it and spoofed an ACK to the sender), destination node can send a NACK or negative acknowledgement alerting the source that it didn’t receive the frame [12].

**C. Payload modification [26]**

Another issue is a scenario where the relay modifies the payload and then forwards it [23]. The receiver will typically not come to know of this, so it may end up voluntarily replying with privileged information [20], such as passwords and usernames. This type of an attack is possible when the change in the payload will not lead to the corruption of the packet, i.e. when no wireless encryption scheme is used, so that no mechanism exists to detect the alteration of the payload [13].

**Solution [27]:**

Such an attack cannot be easily avoided unless the transmitter and receiver can themselves find that there is an unusually large delay in the received packets, which will be due to the calculation of the CRC etc., at the relay. However, if we implement a protocol which requires the retransmission of the packet by the relay in a SIFS interval. This type of attack will not be possible then unless relay knows the exact key [21], as SIFS duration is very small to perform any kind of complex calculations and manipulation the packet [14].

### IV. Future of Cooperative Networking

It has been shown that cooperative diversity brings several benefits including better signal quality, reduced transmission power, better coverage and higher capacity [15].

Cooperative diversity has some drawbacks and challenges including resource over-utilization, additional delay, implementation complexity, unavailability of cooperating nodes and security threats. It should be emphasized that the implementation of cooperative diversity is shown to be challenging due to the various complexity issues [16].

Reduced-complexity algorithms and protocols are needed to simplify the implementation of cooperative diversity in order to be able to harvest the benefits of cooperative diversity. Effective measures and schemes are required to increase users’ motivation for cooperation and to enhance information security and service authenticity in cooperative diversity [17].

The work is currently in progress and we hope to see the cooperative diversity based networks in future [18]. It is
expected to revolutionize the mobile communications and all the wireless networks [19].

V. GLOSSARY

Payload  the actual information or message in transmitted data, as opposed to automatically generated metadata.

CRC  A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices in order to detect accidental changes to raw data.

SIFS  In IEEE 802.11 networks, SIFS is a short interframe spacing prior to transmission of an acknowledgment, a Clear To Send (CTS) frame.

ACK  The control character used in the Transmission Control Protocol to acknowledge receipt of a packet.

RTS / CTS  Request to Send / Clear to Send is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem.

REFERENCES


