Security Issues In A Relay Based Network

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. 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)**[1].

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. It is a promising technique which enables efficient utilization of communication resources and mitigates signal fading in wireless networks[2].

Cooperative communication has two phases

- Relay Selection [3]
- Data Forwarding [4]

There are various relay selection mechanisms such as proactive relay selection, reactive relay selection, opportunistic relay selection etc. [5]

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

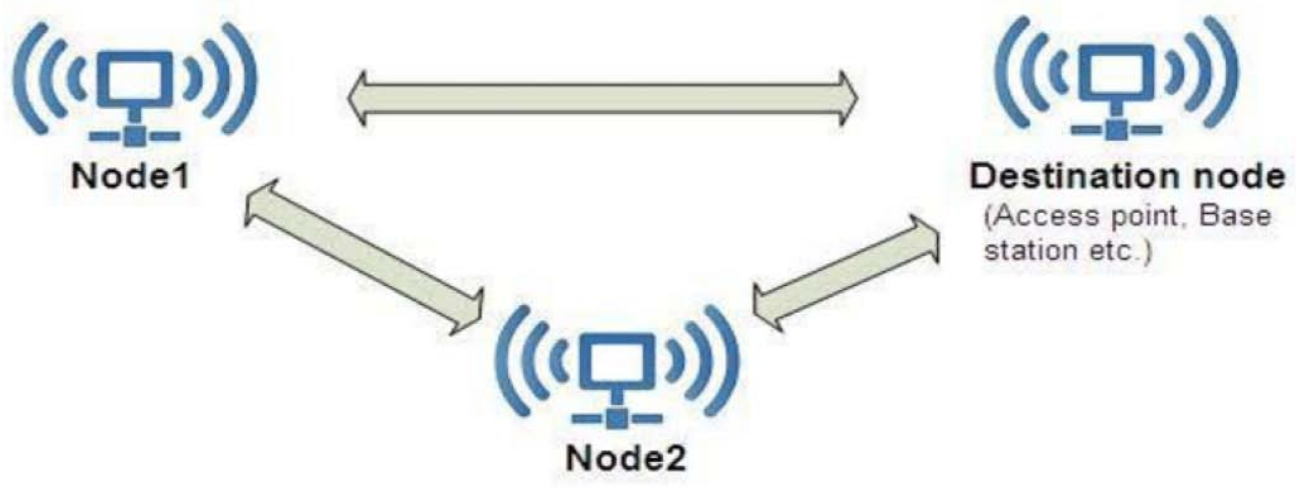


Figure 1

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. In this way, the data rate is improved and medium is released sooner. [5] 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 [8].

Figure 2 - IEEE 802.11 Association sequence

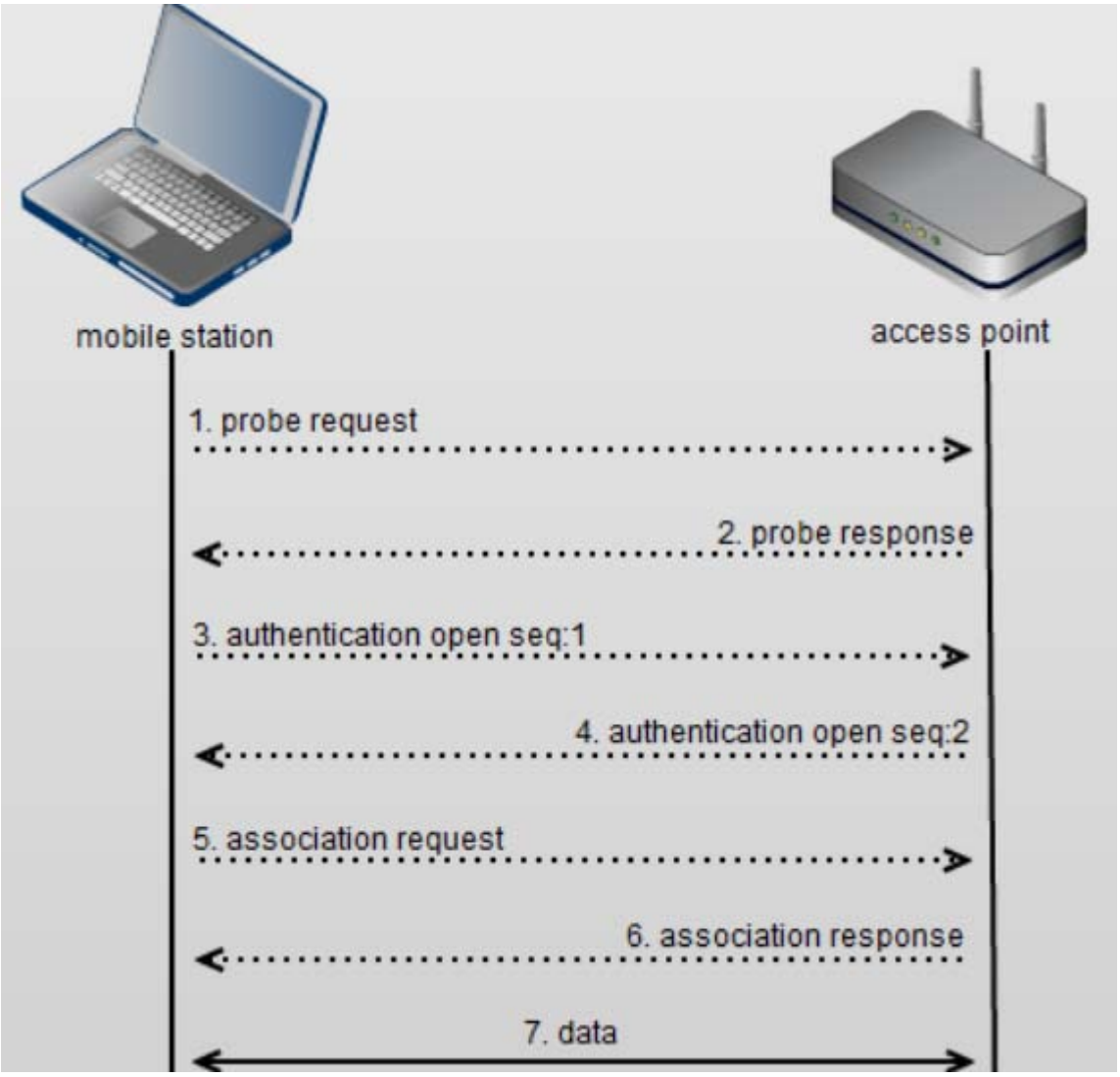


Figure 2 shows 802.11 standard process to develop a connection between two wireless devices in a network.

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. [6]

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

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

A. ***Packet dropping****[9]*

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. [7]

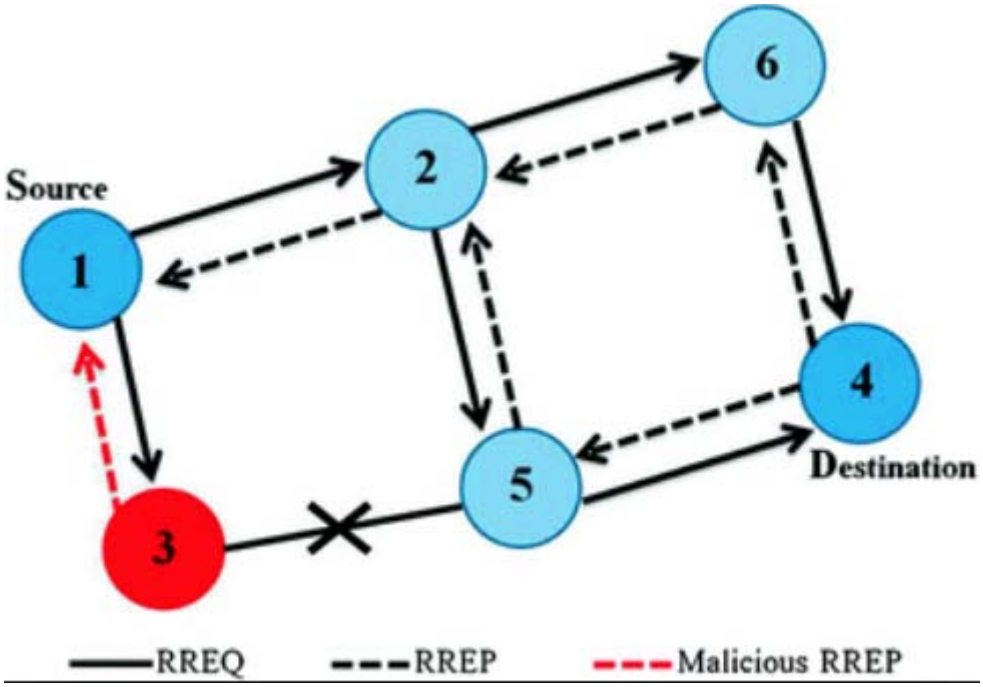


Figure 3 Packet dropping at relay 3

Consider a wireless mobile network where node 1 is source and node 4 is destination while all the other nodes are acting as relays. In figure above, node 3 is a malicious node and sends a malicious RREP to source while dropping the packets received.

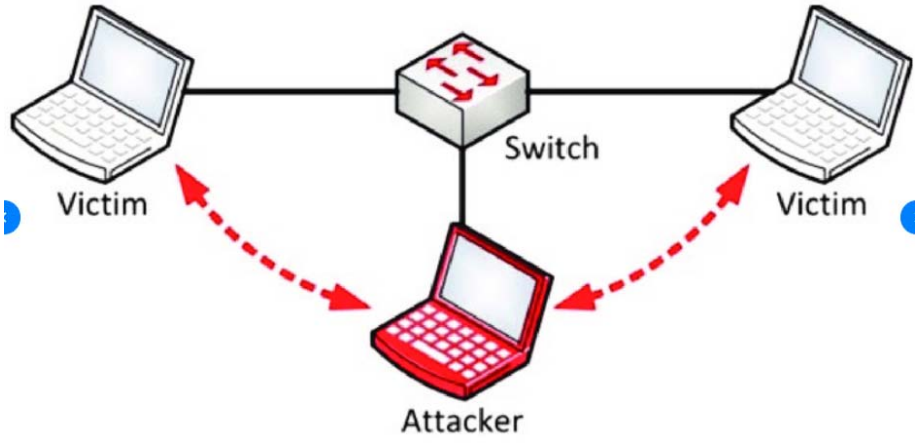
Solution: [13]

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.

B. ***Spoofing*** *[12]*

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 [15].

Figure 4 - Spoofing attack



In Figure 3, a network of laptop computers, which are connected to a switch, is shown. The attaker node disturbs the communication of the other 2 nodes by acting as a malicious relay [18].

Solution:

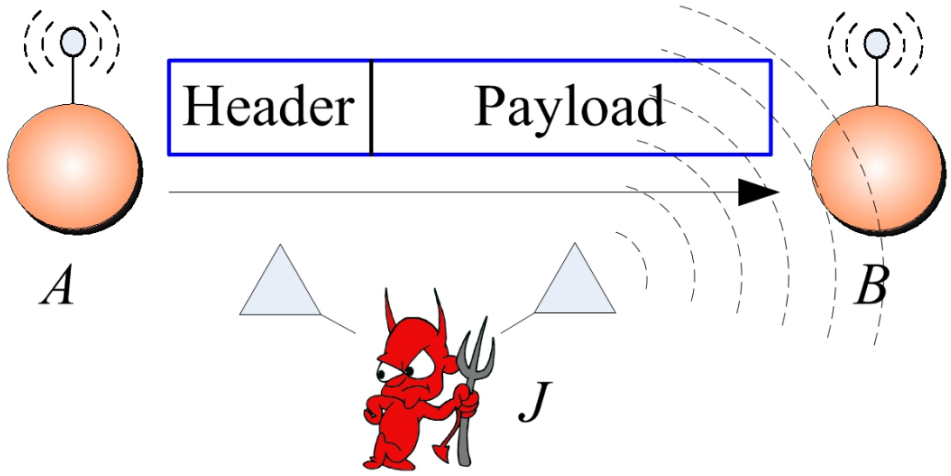
Cooperative networking may use a kind of RTS/CTS scheme to combat this issue [19]. This means that the destination sends the CTS, and is aware that it is an intended recipient of the future frame. Thus, if it does not receive this frame in an allocated NAV period (due to the fact that the helper didn't 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 [20].

C. Payload modification

Another issue is a scenario where the relay modifies the payload and then forwards it. The receiver will typically not come to know of this, so it may end up voluntarily replying with privileged information, 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. [10]

Figure 5 - Payload modification attack [11]



Here, node J is acting as relay between A and B yet modifying the payload and forwarding packets in a longer time than is required [14]

Solution:

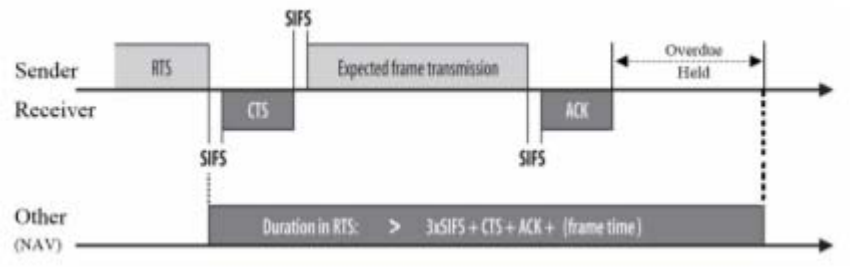
Such an attack cannot be easily avoided unless the transmitter and receiver can themselves find that there is an unusually large delay in the received packets, which will be due to the calculation of the CRC etc., at the relay. However, if we implement a protocol which requires the retransmission of the packet by the relay in a SIFS interval. This type of attack will not be possible then unless relay knows the exact key, as SIFS duration is very small to perform any kind of complex calculations and manipulation the packet [16].

D. RTS Attack

RTS attack is type of DoS attack where the sender of RTS sends RTS either to flood or to reserve the medium for undue amount of time [17]

In IEEE 802.11 standard the Medium Access Control (MAC) layer defines the channel access mechanism. It includes optional RTS/CTC handshake mechanism to avoid collision and hidden node problems. When the sender finds medium free it sends RTS frame after Distributed Inter Frame Space (DIFS) amount of time. DIFS is normally 50 micro seconds, and have considered the same in our evaluation. RTS frame includes 2 Bytes duration field to insert the duration of channel reservation for data transfer. This allows the overhearing nodes to remain in Quiet state for reservation duration. All other nodes will access the channel after expiration of this time. In case of malicious node, the duration field in RTS is filled to undue amount of time such as maximum allowed time, causing the RTS attack.

Figure 6 - Behaviour of RTS attack

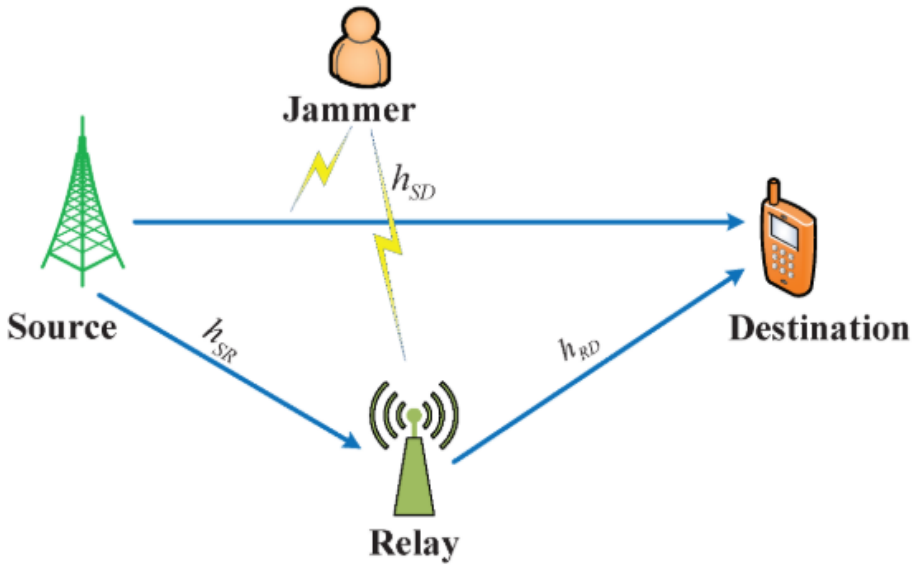


A node with malicious intent can modify the RTS control frame's set duration operation and replace it with a larger value to pretend that it needs large duration to communicate [21], to held the channel unnecessarily for overdue time and reduce the bandwidth utilization with increase in latency for other communications (Figure 6)

E. Jamming Attack

A cooperative communication network is particularly vulnerable to malicious attacks in the physical layer. Moreover, jamming is one of the most serious attacks that greatly degrade network performance. It is a physical layer attack where a jammer tries to block the data communication between the source and the destination. An energy-constrained relay is able to assist the source to forward the data to the destination even when the jammer tries to block the direct link. In jamming attacks, a jammer attempts to prevent users from accessing wireless network resources and reduces network availability by generating interference signals on the channels (Figure 7). This exhausts the energy of the nodes in the network. In order to tackle the jamming attacks, frequency hopping spread spectrum and direct sequence spread spectrum are widely utilized [22]. However, the same sequence can be used by the jammer to attack its target if the hopping sequence is exposed. Thus, the random rendezvous and the uncoordinated frequency hopping is used to safely share the hopping sequence. Nevertheless, these techniques result in the time waste for the communications. Therefore, other secret sharing protocols are proposed such as public key cryptography, certificate and authentication protocol but they also cause large overheads [23].

Figure 7: Jamming attack



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 [24].

Cooperative diversity has some drawbacks and challenges including resource over-utilization, additional delay, implementation complexity, unavailability of cooperating nodes and security threats [25]. it should be emphasized that the implementation of cooperative diversity is shown to be challenging due to the various complexity issues.

Reduced-complexity algorithms and protocols are needed to simplify the [26] 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.

The work is currently in progress and we hope to see the cooperative diversity based networks in future. It is expected to revolutionize the mobile communications and all the wireless networks [27].

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

[1] T. JAMAL, P. AMARAL, A. KHAN, SAB, AND KIRAMAT, "DENIAL OF SERVICE ATTACK IN WIRELESS LAN", IN PROC. OF IARIA 12TH ICDS, ROME ITALY, MAR. 2018.

[2] T. JAMAL AND P. MENDES, "RELAY SELECTION APPROACHES FOR WIRELESS COOPERATIVE NETWORKS", IN PROC. OF IEEE WIMOB, NIAGARA FALLS, CANADA, OCT. 2010.

[3] T. JAMAL, P. MENDES, AND A. ZÚQUETE, "OPPORTUNISTIC RELAY SELECTION FOR WIRELESS COOPERATIVE NETWORK", IN PROC. OF IEEE IFIP NTMS, ISTANBUL TURKEY, MAY 2012.

[4] T. JAMAL AND P. MENDES, "COOPERATIVE RELAYING IN USER-CENTRIC NETWORKING UNDER INTERFERENCE CONDITIONS", IN PROC. OF IEEE COMMUNICATIONS MAGAZINE, VOL. 52, NO. 12, PP. 18–24, DEC 2014.

[5] P. MENDES, W. MOREIRA, T. JAMAL, AND HUILING ZHU, "COOPERATIVE NETWORKING IN USER-CENTRIC WIRELESS NETWORKS", IN: ALDINI A., BOGLIOLO A. (EDS) USER-CENTRIC NETWORKING. LECTURE NOTES IN SOCIAL NETWORKS. SPRINGER, CHAM, ISBN 978-3-319- 05217-5, MAY 2014.

[6] T. JAMAL, P. MENDES, AND A. ZÚQUETE, "RELAYSPOT: A FRAMEWORK FOR OPPORTUNISTIC COOPERATIVE RELAYING", IN PROC. OF IARIA ACCESS, LUXEMBOURG, JUNE 2011.

[7] T. JAMAL, AND SA BUTT, "MALICIOUS NODE ANALYSIS IN MANETS", IN PROC. OF INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY, PP. 1-9, SPRINGER PUBLISHER, APR. 2018.

[8] T. JAMAL, AND P. MENDES, "COOPERATIVE RELAYING FOR DYNAMIC NETWORKS", EU PATENT, (EP13182366.8), AUG. 2013.

[9] T. JAMAL, AND P. MENDES, "802.11 MEDIUM ACCESS CONTROL IN MIXIM", IN PROC. OF TECH REP. SITILABS-TR-13-02, UNIVERSITY LUSÓFONA, LISBON PORTUGAL, MAR. 2013.

[10] T JAMAL, M ALAM, AND MM UMAIR, "DETECTION AND PREVENTION AGAINST RTS ATTACKS IN WIRELESS LANS", IN PROC. OF IEEE C-CODE, ISLAMABAD PAKISTAN, MAR. 2017.

[11] L. LOPES, T. JAMAL, AND P. MENDES, "TOWARDS IMPLEMENTING COOPERATIVE RELAYING", IN PROC. OF TECHNICAL REPORT COPE-TR-13-06, COPELABS UNIVERSITY LUSOFONA PORTUGAL, JAN 2013.

[12] T. JAMAL, P. MENDES, AND A. ZÚQUETE, "INTERFERENCE-AWARE OPPORTUNISTIC RELAY SELECTION", IN PROC. OF ACM CONEXT STUDENT WORKSHOP, TOKYO, JAPAN, DEC. 2011.

[13] T. JAMAL, "COOPERATIVE MAC FOR WIRELESS NETWORK", IN PROC. OF 1ST MAP TELE WORKSHOP, PORTO, PORTUGAL, 2010.

[14] T. JAMAL AND P. MENDES, "ANALYSIS OF HYBRID RELAYING IN COOPERATIVE WLAN", IN PROC. OF IEEE IFIP WIRELESS DAYS (WD), VALENCIA, SPAIN, NOVEMBER 2013.

[15] T. JAMAL, AND P. MENDES, "COOPERATIVE RELAYING FOR WIRELESS LOCAL AREA NETWORKS", IN: GANCHEV I., CURADO M., KASSLER A. (EDS) WIRELESS NETWORKING FOR MOVING OBJECTS. LECTURE NOTES IN COMPUTER SCIENCE, VOL 8611. SPRINGER, CHAM, (WINEMO), AUG. 2014.

[16] T. JAMAL, AND SA BUTT, "COOPERATIVE CLOUDLET FOR PERVASIVE NETWORKS", IN PROC. OF ASIA PACIFIC JOURNAL OF MULTIDISCIPLINARY RESEARCH, VOL. 5, NO. 3, PP. 42-26, AUG 2017.

[17] T. JAMAL, P. MENDES, AND A. ZÚQUETE, "WIRELESS COOPERATIVE RELAYING BASED ON OPPORTUNISTIC RELAY SELECTION", IN PROC. OF INTERNATIONAL JOURNAL ON ADVANCES IN NETWORKS AND SERVICES, VOL. 5, NO. 2, PP. 116-127, JUN. 2012.

[18] T. JAMAL, P. MENDES, AND A. ZÚQUETE, "DESIGN AND PERFORMANCE OF WIRELESS COOPERATIVE RELAYING", PHD THESIS MAP-TELE, UNIVERSITY OF AVEIRO, OCT. 2013.

[19] T. JAMAL, AND P. AMARAL, "FLOW TABLE CONGESTION IN SOFTWARE DEFINED NETWORKS", IN PROC. OF IARIA 12TH ICDS, ROME ITALY, MAR. 2018.

[20] R. SOFIA, P. MENDES, W. MOREIRA, A. RIBEIRO, S. QUEIROZ, A. JUNIOR, T. JAMAL, N. CHAMA, AND L. CARVALHO, "UPNS: USER PROVIDED NETWORKS, TECHNICAL REPORT: LIVING-EXAMPLES, CHALLENGES, ADVANTAGES", TECH. REP. SITI-TR-11-03, RESEARCH UNIT IN INFORMATICS SYSTEMS AND TECHNOLOGIES (SITI), UNIVERSITY LUSOFONA, LISBON PORTUGAL, MAR. 2011.

[21] T. JAMAL, AND P. MENDES, "COOPERATIVE RELAYING IN WIRELESS USER-CENTRIC NETWORKS", BOOK CHAPTER IN: ALDINI, A., BOGLIOLO, A. (EDS.) USER CENTRIC NETWORKING. LECTURE NOTES IN SOCIAL NETWORKS, SPRINGER, CHAM, PP. 171–195, 2014.

[22] SA BUTT, AND T. JAMAL, "FREQUENT CHANGE REQUEST FROM USER TO HANDLE COST ON PROJECT IN AGILE MODEL", IN PROC. OF ASIA PACIFIC JOURNAL OF MULTIDISCIPLINARY RESEARCH 5 (2), 26-42, 2017.

[23] T. JAMAL, P. MENDES, AND A. ZUQUETE, "RELAYSPOT: COOPERATIVE WIRELESS RELAYING", IN PROC. OF MAP-TELE WORKSHOP, AVEIRO, PORTUGAL, MAY 2011.

[24] T. JAMAL, AND P. MENDES, "COOPERATIVE WIRELESS RELAYING, KEY FACTORS FOR RELAY SELECTION", IN PROC. OF MAP-TELE WORKSHOP, PORTO, PORTUGAL, DEC. 2009.

[25] SA BUTT, AND T. JAMAL, "STUDY OF BLACK HOLE ATTACK IN AODV", IN PROC. OF INTERNATIONAL JOURNAL OF FUTURE GENERATION COMMUNICATION AND NETWORKING, VOL. 10, NO.9, PP. 37-48, 2017.

[26] T. JAMAL, AND SA BUTT, "LOW-ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH) ENHANCEMENT FOR MILITARY SECURITY OPERATIONS", IN PROC. OF JOURNAL OF BASIC AND APPLIED SCIENTIFIC RESEARCH, ISSN 2090-4304, 2017.

[27] T. JAMAL, AND P. MENDES, "RELAYSPOT, OMNET++ MODULE", SOFTWARE SIMULATOR EXTENSION IN PROC. OF COPE-SW-13-05, 2013.