Denial of Service Attack in Wireless LAN

∗Tauseef Jamal, ‡∗Pedro Amaral, ±Asifullah Khan, ±Aneela Zameer, ±Kiramat Ullah, ±Shariq Aziz Butt
∗Instituto de Telecomunicações, Lisboa, Portugal.
‡Dept de Eng Electrotecnica, Faculdade de Ciencias e Tecnologia, Universidade Nova de Lisboa, Caparica, Portugal
±DCIS, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan
tauseef.jamal@lx.it.pt, pfa@fct.unl.pt, [asif, aneelaz]@pieas.edu.pk, [shariq2314, kiramat19901]@gmail.com

Abstract—**IEEE 802.11 specifications set the standard for Physical and Medium Access Control (MAC) layer for implementing wireless Local Area Network (LAN). In the wireless network, nodes share media elements with each other. Nodes in wireless network access the media through physical layer using Clear Channel Assessment (CCA) plus Virtual Carrier Sense (VCS) at MAC layer. If VCS timer is not properly handled, there is the possibility of Denial of Service (DoS) attack. In this article, we discuss two scenarios. In the first scenario, DoS attack is launched by increasing the time duration of Clear To Send (CTS) frame. When the CTS frame is received by other nodes, they update their Network Allocation Vector (NAV) for extra time. In prevention step, nodes first detect the malicious duration in the CTS frame and then correct the NAV timer to mitigate the attack. This technique is known as RCD (Re-Evaluation of CTS Duration). In the second scenario, DoS attack is launched by flooding the CTS frame periodically. All other overhearing nodes update their NAV and remain in wait state. To handle such kind of attack, nodes never directly update their NAV after receiving CTS, but after checking the Transmitter Address (TA) and Receiver Address (RA). To increase back the performance of network, blacklisting of malicious node technique is used in both scenarios when a DoS attack is detected.**

Keywords- Virtual Carrier Sense; Medium Access Control; CTS Attack; DoS Attack.

I. INTRODUCTION

Wireless technology is one of the fastest growing industries nowadays. The main reason for this growth is the advantages that only wireless technology has. In wireless communication, there is no need of wires to transmit data from one device to another, which provides flexibility to the network. New devices can be easily added to the network. However, due to the broadcast nature and shared medium of wireless communications, there exist a variety of risks. These risks include packet loss due to distance or mobility, interference, collisions, delay, overhearing, eavesdropping, session hijacking and DoS attacks [1].

In DoS attacks [2], the attacker overloads the network bandwidth with unusual traffic, which makes resources unavailable for others, because other nodes will not be able to send their data after sensing the busy medium. DoS attackers normally exploit the NAV behavior by tempering some of the flags in control frames. In IEEE 802.11 standard, the nodes do not counter check all the flags in control frames, therefore, it is hard to detect such kind of attacks. In this paper, we discuss how DoS attack can be launched when NAV is updated for illegitimate time, by exploiting the duration field of CTS frame in one scenario and exploiting the RA field of CTS frame in the second scenario.

WLANs can be divided into two types: Infrastructure WLANs and Ad-Hoc WLANs. In infrastructure WLAN there is an Access Point (AP) which is surrounded by nodes; AP reserves the media for a node when it has data to send. If one node has data to send to another node, it must pass through AP. In contrast to infrastructure type, the Ad-Hoc WLANs are not centrally connected. In Ad-Hoc mode, the wireless devices are directly connected to each other, handling all communications in distributed fashion.

In Ad-Hoc networks, media is accessed by Distributed Coordinated Function (DCF) with VCS mechanism [3] which includes three-way handshake mechanism before sending data. If a node wants to send data, it sends a Request To Send (RTS) frame to destination. The RTS frame contains reservation duration that is required to complete the data transfer. After receiving an RTS frame by destination, it sends back a CTS frame containing the duration which node requested. According to 802.11 standards all another node when overhear either RTS or CTS must update their NAV and stay quiet until their NAV time reached to zero, NAV is a timer that can uniformly reduce to zero. After all setup, the node sends DATA and waits for ACK, that completes the process. The complete process is shown in Figure 1.

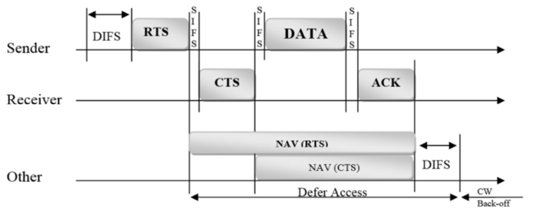

Figure 1. Virtual carrier sensing mechanism [3].

The rest of the paper is structured as follows: In Section 2 we describe related work, while Sections 3 and 4 detaile about DoS attack launching, detection and prevention of two scenarios. Section 5 shows the evaluations of both scenarios. Finally, we concluded the paper in Section 6.

ISBN: 978-1-61208-615-6

II. RELATED WORK

Table I elaborates the related work about DoS attacks.

Table I. DOS ATTACK IN WLAN

Type of Attack	Description	Counter measurement
(ICMP echo) [4]	Fill a network bandwidth with ICMP echo request packets	Rearranging firewall configuration such that it blocks such packets which are not part of the network.
SYN Flood Attack	In SYN flood attacker requests to the target system to provide adequate server resources and network capabilities	Filtering, increasing backlog, reducing SYN-RECEIVED Timer and SYN cache techniques are used as a counter measurement. [5]
DDoS Attack	The main goal of the attacker is launching a large traffic and makes that flow direction towards victim system.	Configuring proper incident response plan before the DDoS attack in the network, checking traffic format and pattern regularly will help out to mitigate such type of attack.[6]
Land Attack (Local Area Network Denial)[6]	The attackers send malicious packets such that it has the same source and destination address.	By enabling both ingress and egress filters in the router to check the source and destination of packets will help out to mitigate the LAND attack.
Authentication request flood	Flood the state table by malicious requests, after the attack there is no space for acceptance from legitimate requests in the state table.	Tracking of client authentication process by wIPS. [7]
Association request flood	Flooding the associate table.	Log the authenticated user and implementation of the tracking system.[7]
RTS /CTS DoS Attack	Sending malicious RTS/CTS back to back.	Using RRD technique protect from such kind of attack. [8]

For better understanding of DoS attacks in WLANs authors in [9] and [10] discussed and analyzed some weaknesses in 802.11 protocols. The cryptographically protection is not effective because MAC spoofing is still vulnerable and DoS attacks are still possible [9]. While exploiting the authentication mechanism [10] leads to additional overhead.

In [11], the authors analyzed Ad-Hoc network, and its vulnerabilities to DoS attack. The malicious node sends control frames to a node which does not exist in the network; while other nodes find it as true communication in the network which leads to DoS attack. However, they did not consider CTS frame. This kind of DoS attack is more prominent when CTS is sent.

In [12], the authors proposed a solution for flood attack using Letter Envelop Protocol (LEP) with Traffic Pattern Filtering (TPF) protocol. They can be used by Central Manager (CM), but if CM is spoofed and maliciously used another mirror of CM, then it will not be effective.

In [12], the authors analyzed the attacks related to VCS. The main focus of the paper is RTS flooding. They analyzed the effects of RTS flood in different conditions. However, they never considered the hidden node problem in all scenarios.

In [13], the authors increased RTS duration and by re-evaluation of the RTS Duration (RRD) technique bring the system performance up. However, this is not efficient either because other nodes already updated their NAV for extra time. Even if RTS duration is found malicious by CTS receiver node, it will not help.

One of the problems with all above solutions is the use of explicit control messages, which increase the overhead as well as they are prone to collisions. Therefore, our solution is based on implicit behavior without any additional control or broadcast messages.

III. FIRST SCENARIO

A. Attack launching

In our first scenario, one node works as receiver. It starts malicious behavior by increasing CTS frame duration to reserve medium more than the time required. CTS duration is increased more than two 2*SIFS+DATA + ACK frames length. Figure 2 shows that other overhearing nodes update their NAV for more than the time required. This leads to DoS attack.

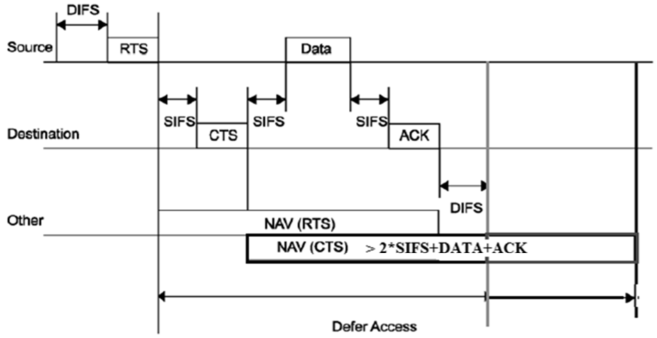

Figure 2. Launching DoS by increasing CTS duration.

B. Detection

We use revalidation technique to detect such kind of attack. In revalidation, there is a comparison between CTS frame duration which is received from receiver node and immediate RTS frame duration which are send by sender node, at lower layer by each node before updating NAV.

In RTS, the duration is set by the sender to keep in view the amount of data. The CTS duration is calculated by receiver node as:

$$\text{RTS\_Duration} - \text{SIFS} - \text{CTS}. \qquad (1)$$

According to IEEE 802.11 standard, when any frame is overheard by a node, it first checks if the frame is destined for it or not. If the frame does not belong to a node, such node just extracts the duration field from the frame and updates its NAV. However, in our proposed detection mechanism all overhearing nodes calculate the CTS duration according to (1), upon reception of RTS. When CTS frame arrives, the overhearing nodes extract the duration field from CTS frame, and compare it to the saved CTS frame (we call it expected CTC duration). Based on the comparison, it decides if the CTS frame is malicious or not. Figure 3 shows the flow diagram of the described mechanism.

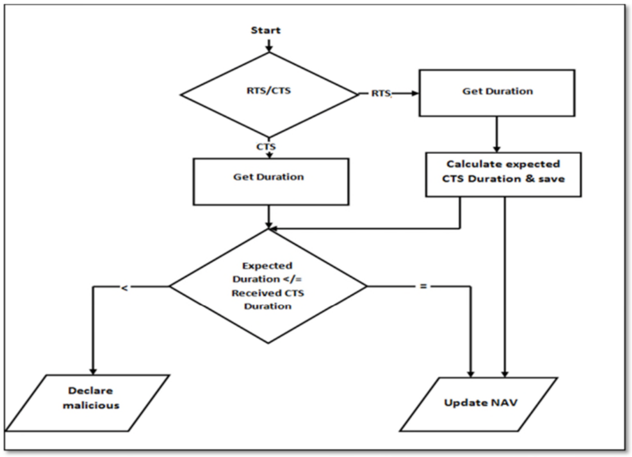
Start
RTS/CTS
RTS
Get Duration
CTS
Get Duration
Calculate expected CTS Duration & save
Expected Duration </= Received CTS Duration
<
=
Declare malicious
Update NAV

Figure 3. Detection mechanism for the first scenario.

C. Prevention

After detecting a malicious node, we need to update the NAV according to the correct value of duration field. Each node will perform three tasks shown in Figure 4.

- Calculates the malicious time interval by subtracting (CTS duration frame duration-immediate RTS). And save in a variable. In non-malicious case, this variable value must be zero.
- Adjust the actual time for NAV by subtracting the malicious time interval from malicious CTS duration.
- Update the NAV timer.

IV. Second Scenario

A. Attack launching

In our second scenario, a malicious node pretends to be receiver of itself, by replacing RA with its own MAC address (Figure 5) and sends malicious CTS periodically.

This way, the channel is occupied by the malicious node while other overhearing nodes update their NAV and remain in quiet state, leading to DoS attack [14].

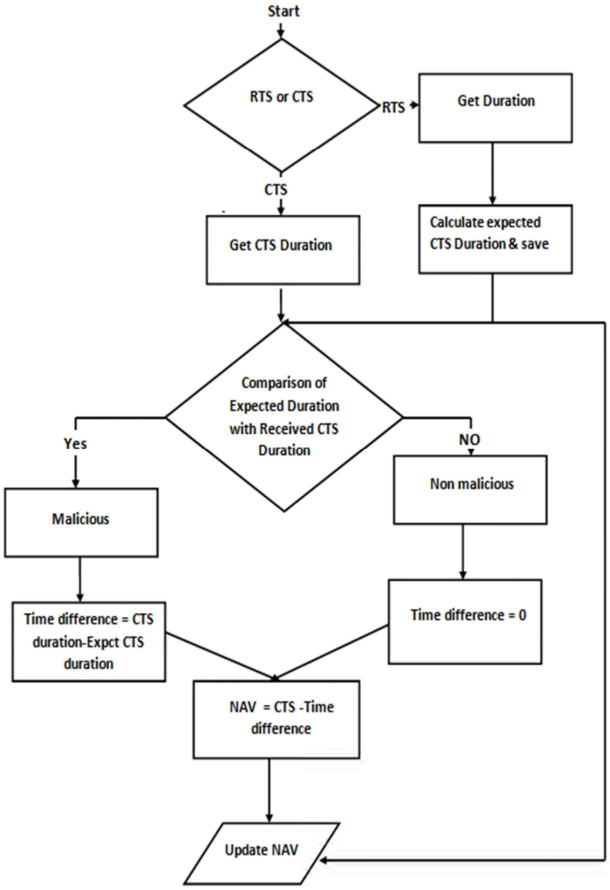
Start
RTS or CTS
RTS
Get Duration
CTS
Get CTS Duration
Calculate expected CTS Duration & save
Comparison of Expected Duration with Received CTS Duration
Yes
NO
Malicious
Non malicious
Time difference = CTS duration-Expct CTS duration
Time difference = 0
NAV = CTS -Time difference
Update NAV

Figure 4. Detection and prevention for the first scenario.

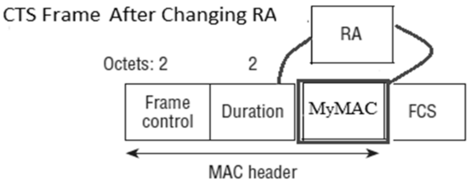

Figure 5. Replacing RA with MyMAC.

There are three kinds of nodes, sender, receiver and others nodes. In case of sender, when malicious CTS is received, it goes to CONTEND state and waits there until the medium is idle for sending the RTS again [15]. In receiver case, when a malicious CTS is received, it goes to QUIET state. The receiver finds that some other nodes are communicating so to avoid a collision it will stay in QUIET state. Other overhearing nodes, just update their NAV (as explained earlier), and most of the time they remain in the QUIET state. Therefore, attack in such a scenario is very critical and hard to detect.

B. *Detection*

This attack is critical because there is no check on receiver address of CTS frame. Other nodes do not know about CTS frame's Sender Address (SA). So, they can not find malicious CTS and would update NAV after receiving malicious CTS. This problem can be detected as follows:

- Since RTS frame includes the receiver address.
- Therefore, as RTS is received by other nodes, they retrieve the RA and save it.
- When CTS is arrived as a consequent of RTS, before updating the NAV, there would be a comparison at two steps:
    - Compare RA to MyMAC
    - Compare SA to RA.
- If SA is same RA, declare it malicious otherwise updated NAV.

Figure 6 describes the flow diagram of detection mechanism.

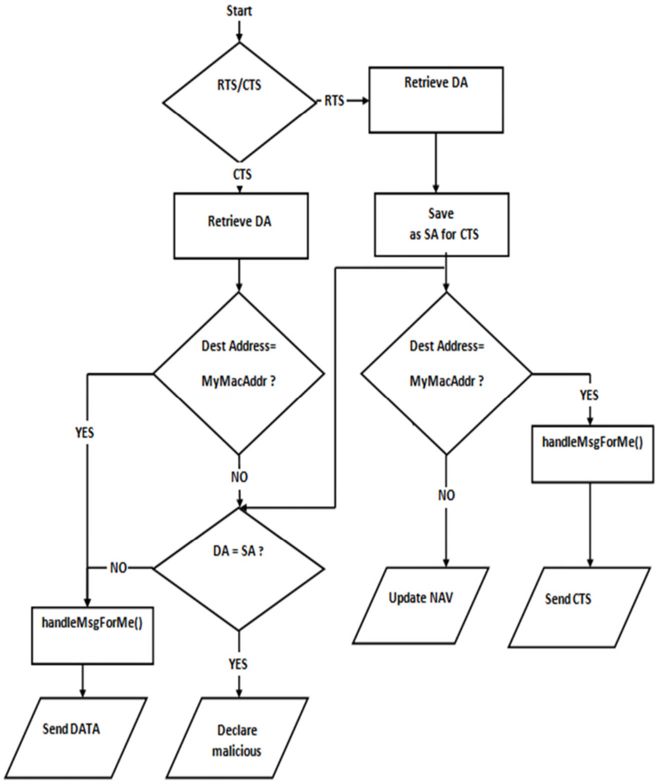

Figure 6. Detection of the second scenario.

C. *Prevention*

The main problem in this scenario is that malicious node will not release the medium. It will send that malicious CTS and other nodes must wait for the end of transmission. The longer the duration mentioned in malicious CTS, the more the network performance would go down. Therefore, in our proposed mechanism, each node maintains a list of MAC addresses. As soon the malicious CTS's originator is detected, its MAC is added to the list.

When a node is detected malicious, three steps are taken by each node: stop updating NAV, update the list and maintain the record of malicious MAC and send a broadcast alert message with malicious MAC to other nodes. So, any node may no longer involve in communication with such malicious node and ignore such CTS in the future. As a result, other nodes would have more chances to utilize the medium, increasing the overall capacity of the network.

V. EVALUATION

In our experimental setup, we used the OMNET++ framework with MIXIM simulator model on window 7 platform. In MIXIM wireless network IEEE 802.11 is implemented. For both scenarios the destination or receiver node is assigned MAC address of 0, while all other nodes are sender nodes. Node-0 sends CTS and behaves maliciously. The number of nodes varies from 3 to 15 nodes. We have performed three kinds of simulations for both scenarios, i.e., without malicious node (which is bench mark), with one malicious node and with our proposed prevention mechanism. We simulated each topology for 300s. We used throughput and latency as performance parameters. Other simulation parameters are listed in Table II.

Table II. SIMULATION PARAMETERS

Parameter	Values
cup-time-limit	300s
playgroundSizeX	500m
playgroundSizeY	500m
playgroundSizeZ	50m
carrier Frequency	2.4e+9Hz
Power	110.11mW
mobility.speed	0 mps
appl.burstSize	1frame
appl.trafficParam	50ms
appl.destAddr	0 node
appl.initializationTime	uniform(60000ms,60050ms)
mac.headerLength	272 bits
mac.queueLength	14 frames
acierate	2E+6bps# in bits/second
phy.useThermalNoise	true

A. *First scenario results*

Latency is the amount of time a message takes to traverse a system; we can observe that latency increases as many nodes increase in a network. We can see in Figure 7 that latency is increased due to the malicious node which means that nodes wait for extra time to send data. Here, our proposal brought the latency as close as possible to normal and decreased the latency up to 35% in case of one malicious node.

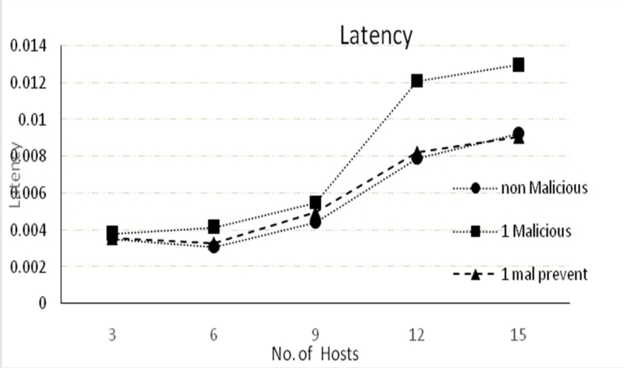

Figure 7. Latency for the first scenario.

Throughput is a measure of how many units of information a system can process in each amount of time. Throughput decreases as network density increases, in Figure 8; the throughput decreases with increase in number of hosts due to increase in latency. As the nodes update their NAV after receiving malicious CTS, the number of packets sent by a node would be less compared to the non-malicious case. Our proposal brought the throughput closer to normal and increased the throughput up to 35% in case of one malicious node.

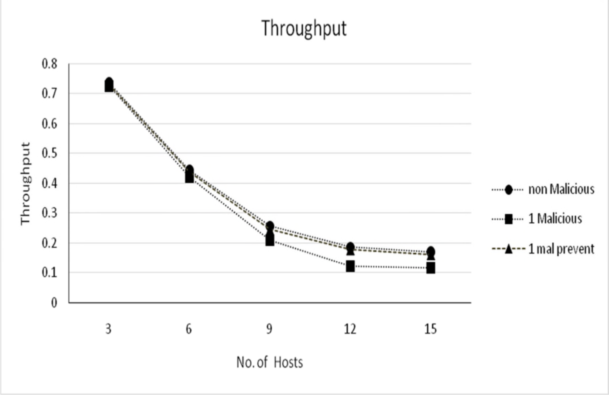

Figure 8. Throughput for the first scenario.

B. *Second scenario results*

In the second scenario, the DoS attack has the worst effect on network performance as compared to the first scenario. As shown in Figure 9, when receiving malicious CTS after the interval, here interval is 3 frames count in the network, sender node sends again RTS frame for sending data and other nodes just only update NAV. Other nodes only send their RTS frame when the first node RTS retries reaches its limit. That decreases throughput abruptly.

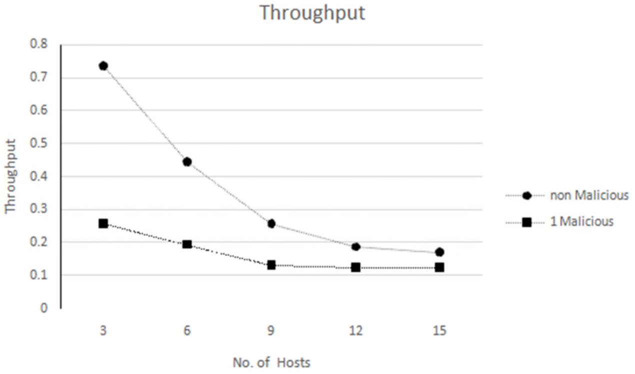

Figure 9. Throughput after malicious CTS for 2nd scenario.

After blacklisting the malicious node, other nodes ignore any kind of frame from the malicious node, the throughput is increased up to 41%, which is 65% increased to normal behavior. It still not reached to normal behavior because there is still a malicious CTS flow in the network. Also, there is slight overhead of broadcast alert, which decreases throughput c.f. Figure 10.

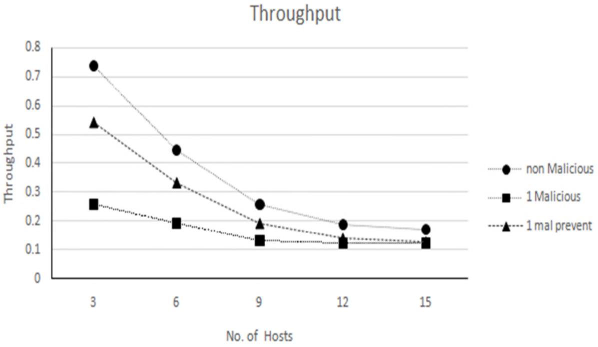

Figure 10. Throughput after prevention for 2nd scenario.

VI. Conclusions and Future Work

In the first scenario, the attacker increase the CTS frame duration field which reserves the media for a node longer than required and other nodes update NAV for the extra time. Nodes are not allowed to sense the media; therefore, we proposed a Re-Evaluate CTS Duration (RCD) technique to detect such behavior and then set back the correct value for NAV as a prevention.

In the second scenario, CTS frame exploits the RA field in CTS frame and sends a CTS frame to itself after a specific interval. In the detection phase, we use the comparison of destination and sender node addresses when CTS is received by any node. During the prevention mechanism, other nodes stop updating NAV and announce the MAC of the malicious node. After that, no other node would communicate with such node.

As a future work, we aim to extend the scenario towards dense network having 100s of highly mobile nodes randomly deployed, to test the proposal against increasing number of malicious nodes. Another extension would be learning the malicious behavior implicitly by other nodes and other nodes would ignore such node (implicitly). In this situation we would use relays to cooperate with [17], using the framework proposed in [18]. The aim is to implement and test in the real scenario.

ACKNOWLEDGMENT

This work is funded by FCT/MEC through national funds and when applicable co-funded by FEDER – PT2020 partnership agreement under the project UID/EEA/50008/2013.

REFERENCES

[1] SA Butt, T. Jamal, “Study of Black Hole Attack in AODV”, in Proc of International Journal of Future Generation Communication and Networking, Vol.10, No.9 (2017), pp.37-48.

[2] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection,” International Journal on Advances in Networks and Services, vol. 05, no. 2, pp. 116–127, Jun. 2012.

[3] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks,” in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[4] B. John and S. Stefan. “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions.” Proceedings of the USENIX Security Symposium, August 2003.

[5] D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Neworks,” International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[6] H.Deng, W.Li and D.P.Agrawal, “Routing Security in Wireless Ad Hoc Networks,” University of Cincinnati, IEEE Communication Magzine, Oct, 2002.

[7] C. Liu and J. Yu, “A Solution to WLAN Authentication and Association DoS Attacks,” IAENG Int. J. Comput. Sci., vol. 34, no. 1, pp. 31–36, 2007.

[8] P. M. D. Nagarjun, V. A. Kumar, C. A. Kumar, and A. Ravi, “Simulation and analysis of RTS/CTS DoS attack variants in 802.11 networks,” in 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, 2013, pp. 258–263.

[9] K. Bicakci and B. Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks,” Comput. Stand. Interfaces, vol. 31, no. 5, pp. 931–941, Sep. 2009.

[10] J. Heo and C. S. Hong, “An Efficient and Secured Media Access Mechanism Using the Intelligent Coordinator in Low-Rate WPAN Environment,” Springer, Berlin, Heidelberg, 2005, pp. 470–476.

[11] T. Jamal, P. Mendes, and A. Zúquete, “RelaySpot: A Framework for Opportunistic Cooperative Relaying,” in Proc. of IARIA ACCESS, Luxembourg, Jun. 2011.

[12] A. L., V. B., S. S., and P. A., “A Solution to Prevent Resource Flooding Attacks in 802.11 WLAN,” Springer, Berlin, Heidelberg, 2012, pp. 607–616.

[13] T. Jamal, M. Alam, and M. M. Umair, “Detection and prevention against RTS attacks in wireless LANs,” in 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), 2017, pp. 152–156.

[14] T. Jamal and P. Mendes, “802.11 Medium Access Control In MiXiM,” Copelabs Technical Report, 2013.

[15] T. Jamal and P. Mendes, “Cooperative Relaying in Dynamic Wireless Networks under Interference Conditions (2014)”, in: IEEE Communication Magazine, Special issue on User-centric Networking and Services.

[16] Y. Ohsita, S. Ata, and M. Murata, “Deployable overlay network for defense against distributed SYN flood attacks,” IEICE Trans. Commun., vol. E91–B, no. 8, pp. 2618–2630, Aug. 2008.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection,” in Proc. of ACM CoNEXT, Tokyo, Japan, Dec. 2011.

[18] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network,” in Proc. of IEEE IFIP NTMS, Istanbul, Turkey, May 2012.