Analysis of DoS Attacks at MAC Layer in Mobile Adhoc Networks

Chaminda Alocious
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: c.alocious@herts.ac.uk

Hannan Xiao
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: h.xiao@herts.ac.uk

Bruce Christianson
School of Computer Science
University of Hertfordshire,
United Kingdom
Email: b.christianson@herts.ac.uk

***Abstract*—Wireless network security has received tremendous attention due to the vulnerabilities exposed in the open communication medium. The most common wireless Medium Access Control (MAC) protocol is IEEE 802.11, which assumes all the nodes in the network are cooperative. However, nodes may purposefully misbehave in order to disrupt network performance, obtain extra bandwidth and conserve resources. These MAC layer misbehaviours can lead to Denial of Service (DoS) attacks which can disrupt the network operation. There is a lack of comprehensive analysis of MAC layer misbehaviour driven DoS attacks for the IEEE 802.11 protocol. This research studied possible MAC layer DoS attack strategies that are driven by the MAC layer malicious/selfish nodes and investigates the performance of the IEEE 802.11 protocol. Such DoS attacks caused by malicious and selfish nodes violating backoff timers associated with the protocol. The experimental and analytical approach evaluates several practical MAC layer backoff value manipulation and the impact of such attacks on the network performance and stability in MANETs. The simulation results show that introducing DoS attacks at MAC layer could significantly affect the network throughput and data packet collision rate. This paper concludes that DoS attacks with selfish/malicious intend can obtain a larger throughput by denying well-behaved nodes to obtain deserved throughput, also DoS attacks with the intend of complete destruction of the network can succeed.**

***Index Terms*—Wireless Network Security, IEEE 802.11, Medium Access Control, Denial of Service, MAC Layer Misbehaviours**

I. Introduction

MANETs are self-organized networks, which could change the topology dynamically without a centralized control. MANETs have many applications in different domains such as tactical networks in military communication for automated battlefield and disaster recovery planning. The wireless nodes in a MANET communicate by forwarding packets on behalf of other nodes by working as routers in multi-hop communication channel. Therefore, MANETs need to contain the basic security requirements such as availability, fairness, data confidentiality and integrity. MANET based wireless networks using the IEEE 802.11 protocol as the MAC layer protocol; this standard assumes that all the nodes in the wireless network adhere to the protocol, and fully cooperates with the protocol. However, selfish or malicious mobile stations may not adhere the IEEE 802.11 protocol rules when sharing the wireless channel. In IEEE 802.11 based ad hoc networks, MAC protocol related misbehaviours such as backoff timer and differ timer manipulation can drastically reduced network performance. Our research investigates such violations which could cause a network unfairness also could drive to Denial-of-Service (DoS) attacks. Experiment results show that it could be devastating in MANET environment due to its strict bandwidth constraints. MAC layer misbehaviour attacks evaluation could improve the accuracy and capability of MAC layer selfish and malicious misbehaviour detection mechanisms [5].

MAC layer malicious misbehaviour can be divided into link layer jamming and DoS attacks. DoS attacks can be single adversary attacks (SSA) or colluding adversary attacks (CAA). The SAA attacks inject enormous amounts of Request to Send (RTS) packets to the network. CAA attacks could deplete the channel bandwidth in their vicinity in order to disturb the communication. Although, these attacks are easy to execute, given their nature they are easy detect [1]. However, in our research, we consider low/moderate/higher rate DoS attacks which selfish or malicious misbehaviour nodes could launch at MAC layer by manipulating IEEE 802.11 backoff timers. These DoS attacks are relatively new variants of DoS attacks and difficult to detect since they are not sending a stream of traffic such as conventional jamming attacks (SAA and CAA). Because countermeasures used to handle the jamming DoS attacks are not suitable for these types of attacks. The rest of the paper has organized as follows: the next section elaborates the related work of MAC layer misbehaviour analysis. Section III investigates the theoretical aspects of the MAC protocol operation and provides a summary of the MAC layer misbehaviour which can cause low to high rate DoS attacks. Section IV analyses the DoS attack's impact. Section V discusses the outcome of the research experiments in detail. Finally, the paper concludes with a summary of contributions and detection mechanism suggestion.

A. Research Contribution

MAC layer DoS attacks caused by the MAC layer selfish and malicious misbehaviours are not particularly discussed in detail in the literature. We simulate new attacks and their behaviour in ns2 simulation environment to demonstrate the attack feasibility, as well as the potential impact of these

978-1-4799-5344-8/15/$31.00 © 2015 IEEE

attacks to 802.11 based networks. This research demonstrates that low/moderate/higher level selfishness can lead to DoS attacks which can affect the network throughput and even network collapses in practically. The experimental results contribute to extend the IEEE 802.11 protocol to prevent and detect similar MAC layer DoS attacks. Case studies are chosen to demonstrate the vulnerabilities in standard protocols which gives provision to design a resilient MAC protocol for such backoff value violation attacks. Finally, the research suggest a trust management based detection mechanism for MANET.

II. Related Work

In recent years, several researchers have evaluated MAC layer misbehaviours in the IEEE 802.11 protocol. The research done by [2] [3] has conducted a similar evaluation for greedy receiver misbehaviour in IEEE 802.11 Hotspots. Their research was motivated by the observation that many hotspot users receive more traffic than they send. The research in [3] identifies a range of greedy receiver misbehaviours, and quantify their damage using both simulation and testbed experiments. The results show that greedy receivers can result in very serious damage, including completely shutting off the competing traffic including starvation. Their research focuses on the effects of greedy receivers in fixed rate environments. However, they have also explored attacks under adaptive rate. Under adaptive rate the damage of faking ACKs can be reduced. In contrast, the damage of spoofing ACKs can increase and incur significant performance degradation, which may benefit the greedy receiver.

In [4] the authors have analysed and simulated the RTS/CTS DoS attack variants in 802.11 networks which is one type of low rate DoS attack that capable to exploit the medium reservation mechanism of IEEE 802.11 networks through duration field. Their research proposing a RTS/CTS attack which changes the Network Allocation Vector(NAV) value in RTS/CTS control packet. The attacker could set the maximum value for the NAV duration field, and if the attacker uses a data rate of 30 frames/s then the attacker can prevent genuine nodes from accessing the channel [4]. The research done by P. Kyasanaur et al. [6] have proposed a modification to the existing standard IEEE 802.11 MAC protocol in order to address the problem of sender backoff manipulation in WLANs. In their approach, the receiver is trustworthy and assigns backoff value to the sender and the receiver monitors the sender, by checking whether the sender deviates from the protocol. However, such detection mechanism is not capable to handle receivers backoff manipulation. In [7] authors have proposed a detection mechanism for MANET which is capable of detecting several selfish misbehaviours. However, this method also needs to trust at least one party in a communication which is not a valid assumption in adhoc networks. Furthermore, in [8] has studied DoS attacks and countermeasures in IEEE 802.11 wireless networks. The research in [9] has presented a comprehensive analysis of modern MAC layer misbehaviour detection mechanisms. Therefore, it is important to analyse protocol vulnerabilities experimentally for better design of MAC protocols. [10].

III. MAC Layer Misbehaviour Driven DoS Attacks

MAC layer misbehaviour driven DoS attacks are the main focus of this research. These misbehaviour nodes initial intend may be to achieve higher channel access frequency (selfish) by manipulating backoff value timers. However, with the greediness increases of such nodes, the network starts to suffer with low/moderate/high level DoS attacks (malicious). This section explains the IEEE 802.11 channel sharing operation using Distributed Coordination Function (DCF) and newly proposed MAC layer backoff timer violations.

A. IEEE 802.11 with DCF

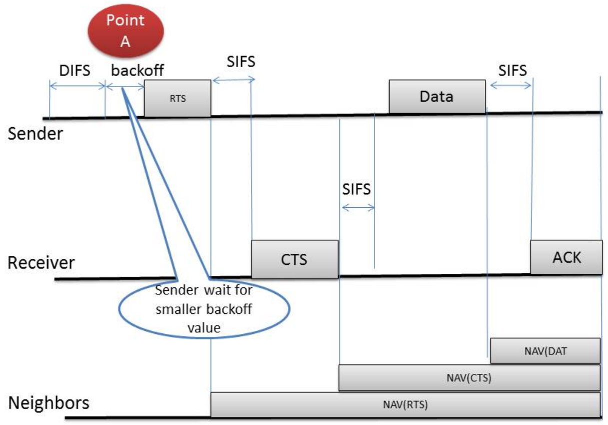
DCF uses the BEB mechanism to assign backoff values to each wireless station in the network, aiming to allow each wireless station to get a fair share of the wireless channel. When a wireless node wants to transmit data, firstly it senses the channel status. If the channel is busy it waits for distributed inter frame space (DIFS) time. Then the node enters the Contention Window (CW) time scale where the node calculates the random backoff value. Next, if the medium becomes idle after additional DIFS time, the node starts to decrement backoff counter until the channel becomes busy or counter reaches zero. If the channel becomes busy before the counter becomes zero, then the node freezes its timer. This process continues until backoff counter reaches zero. Then the node starts to send the first control packet Request to Send (RTS), the receiver then responds after a small inter frame space (SIFS) with a Clear to Send (CTS) packet. After another SIFS time the sender transmits the DATA packet. Finally, the receiver acknowledges the data by sending an ACK packet. Occasionally, two nodes can reach zero in the same time, in which case collision will happen and the node has to recalculate the backoff value.

B. Denial of Service Attacks

In our research, we exploit the DCF backoff time interval to achieve low/moderate/high DoS attacks. The CTS control packet has been used by the malicious/selfish receivers to favour colluded senders which wants to access the channel more frequently. These misbehaviours could also use to disrupt the network services hence legitimate wireless nodes cannot access the network services. The first case study is the sender bakoff value manipulation to start DoS attack by capturing the channel more frequently, which will lead other legitimize nodes to wait longer to access the channel. The second misbehaviour case study is the misbehaving receivers misconducts the CTS control transmission to override selected sender's backoff value policy by allowing to transmit more frequently. Case studies are chosen to demonstrate the vulnerabilities in standard protocol which gives provision to design a resilient MAC protocol to detect and prevent such attacks.

- Case Study 1: Sender Generating DoS Attacks

The primary intention of this case study is to demonstrate the MAC layer backoff timers manipulation by the sender with malicious or selfish purpose. The misbehaving senders select small backoff values (different backoff value policy) instead of randomly selected backoff value, or ignore to increment the attempt number after a collision which is used to calculate the CW value eventually backoff value. The Fig. 1 demonstrates the DoS attack which can be initiated from such senders while their greediness increases to higher level, then network will deny the services for good nodes. In this backoff value violation model, if a sender has a greediness of 20% (misbehaviour percentage), then the sender only waits for 80% of the actual allocated backoff value by the IEEE 802.11 protocol. In such scenario, these senders can act as a source for a DoS attack.



Pont A : Sender could wait for a smaller value than "backoff" also in this point the sender calculate the backoff value for next transmission,

Fig. 1. Sender manipulates its backoff value to access the channel more frequently

- Case Study 2: Receiver Generating DoS Attacks

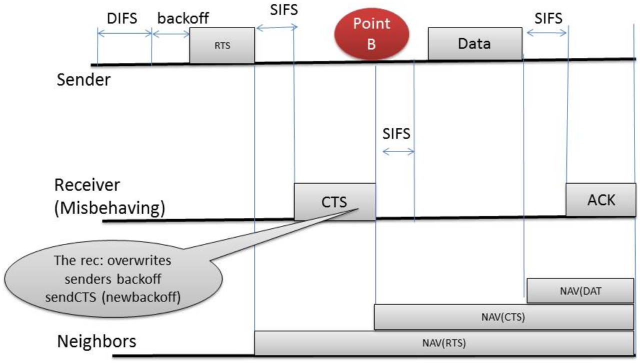
In the IEEE 802.11 protocol the receiver misbehaviours can be in different forms such as, changing backoff values of selected senders, change NAV of neighbours and dropping CTS packets intentionally. Such behaviours can be seen as selfish or malicious purpose which could be leading to a DoS attacks. This research, demonstrates a receiver misbehaviour based on a CTS modification where the receiver uses CTS transmission to modify the senders' backoff value selection policy. The receiver updates the selected senders backoff selection policy value to increase/decrease the sender's backoff value. In the Fig. 2 and the following code, if the receiver tries to favour a selected sender, then the receiver will reduce the sender's backoff value or increase otherwise. The malicious receiver could also manipulates the CTS time-out value in the CTS transmission to mislead genuine nodes who trying to send data packets.

```
Mac_IEEE_802_11::sendCTS(senderID,RTS duration) {
.........................................
/*The receiver obtain the backoff value of sender*/
 senderBackoff = getbackoff(senderID)
/*The misbehaving attacker updating senders
backoff value selection policy in CTS transmission with
different CW distribution */
ReceiverUpdateBackoffPolicy(senderID,newbackoffpolicy);
 ..................................
}
```

The following code segment shows the modification required for the backoff timer class to follow different backoff policy.

```
BackoffTimer::start(int backoff, double difs){
..........
/*Calculate the backoff based on the policy selected
,backoff policy can be as below executed by sender or
recvr*/
switch(backoff_policy) {
//Normal 802.11 scheme
case 0:
        rslots=backoff;
        break;
//Sender misbehaving, set backoff to misb_perc always
case 1:
        rslots = MISB_PERC;
        break;
//Sender misbehaving,set backoff-backoff*MISB_PERC/100
case 2:
        rslots=backoff-(backoff * MISB_PERC/100);
        break;
//Receiver Misbehaviour with REC_MIS% value,
case 3:
        rslots= (backoff - (backoff*(REC_MIS/100));
        break;
}
..........
```

In the simulation script nodes are set to follow certain misbehaviour policy with a certain misbehaviour percentage.



Point B : The receiver overwrites senders backoff value in CTS, the IEEE 802.11 implementation allow receiver to access backoff value of sender

Fig. 2. The receiver manipulate senders backoff value in the CTS

IV. Simulations Configuration

The protocols, selfish and malicious misbehaviour driven DoS attacks, network topologies and required C++ modifications, simulation scripts have been simulated in ns2 2.35 network simulator. The Table I presents the wireless nodes CBR traffic and simulation configuration parameters. The simulation configures a sender misbehaviour percentage (SMP) which represents the percentage of the backoff value slots that the sender reduces from the originally assigned backoff value, which has also been referred as selfish nodes' greediness. The receive misbehaviour percentage (RMP) is configures, such a way that the receiver is misbehaving by colluding with senders randomly. In our study, the receiver identifies the sender to collude in the network and then reduces its backoff values slots by an RMP. Initially, the purpose of such a attack could be selfish(frequent channel access), however, in good nodes point of view, it is a moderate or higher rate DoS attack.

TABLE I
SIMULATION CONFIGURATION

Simulation Configuration	
Network Model	ADHOC
Simulation Area	1500x750 m
Routing protocol	DSR
Simulation time	500 s
Simulation Runs	10x11x5
Total nodes	11
misbehaviour nodes	(3 - 9)
Max moving speed	10 m/s
Average moving speed	3.82 m/s
Route changes	123
CBR Traffic Configuration	
Traffic type	CBR
Packet size	512 bytes
Packet interval	0.25 S
Max no of packets	100000

A. *Performance Metrics*

Performance metrics are considered to measure the DoS attack impact on the network performance, such as well-behaving node throughput, selfish/malicious node throughput and packet collision rate (CR). The well-behaving node's throughput is important to identify the effect of the DoS attack for good wireless nodes. This value is obtained by dividing the total throughput achieved by good nodes by the number of good nodes. The average throughput of selfish/malicious nodes gives a clear measurement for the overall network performance degradation and the advantage achieved by the misbehaviour nodes. This is obtained by dividing the total misbehaviour nodes' throughput by the number of total misbehaving nodes. The CR is calculated by the equation (1) the divides the total collided packets of each node by the total packets transmitted in the network, where collided packets are denoted by $colPktNum$ and total packets by denoted by the sum of $colPktNum$ and $nonColPktNum$.

$$CR = \frac{\sum_{i=0}^{N-1} colPktNum[i]}{\sum_{i=0}^{N-1}(colPktNum[i] + nonColPktNum[i])} \quad (1)$$

V. RESULTS AND ANALYSIS

Simulation results have been obtained with performance metrics for each MAC layer misbehaviour driven DoS attack scenarios, different mobility patterns, topologies and traffic rates.

A. *Sender Generated DoS Attack Result Analysis*

This section analyses the simulation results of different sender bakcoff value manipulation scenarios by focussing the impact on nodes' throughput and data packet CR. Furthermore, sender misbehaviour simulations have been extended to study the effect of increasing the selfish nodes greediness, the number of misbehaving nodes and CBR traffic rate.

1) Increase Misbehaviour Greediness: Increasing the greediness means allow misbehaviour nodes to access the wireless channel more frequently. Figure. 3 shows the average throughput of good nodes and misbehaving nodes when the sender greediness increases from 10% to 90% (SMP). Other parameters such as the CBR traffic rate, total number of nodes (11) and the number of misbehaving nodes are constant as shown in Table I. It is clear that misbehaving nodes achieve higher throughput with higher SMP. Similarly, good nodes are suffering from lower throughput. For example, when the greediness percentage (SMP) is 50%, misbehaviour nodes' throughput dramatically increases to more than 3 times of good node (from about 500kbps to about 1500kbps). After 50% SMP the network acts as a low rate DoS for good nodes while misbehaving nodes having access to the channel more frequently. Furthermore, Fig. 3 shows that misbehaving nodes achieve higher average throughput than good nodes under all SMP from 10% to 90%. The misbehaving nodes' average throughput increase gradually and the good nodes' decreases gradually, making the gap between the average throughputs of both groups bigger. The CR analysis is important to demonstrate the effect of misbehaviours for the network stability. The result in Fig. 4 shows the effect of increasing the aggressiveness of the DoS attack for the network CR. The CR has increased more than 5 times (from 0.5% to nearly 2.5%).

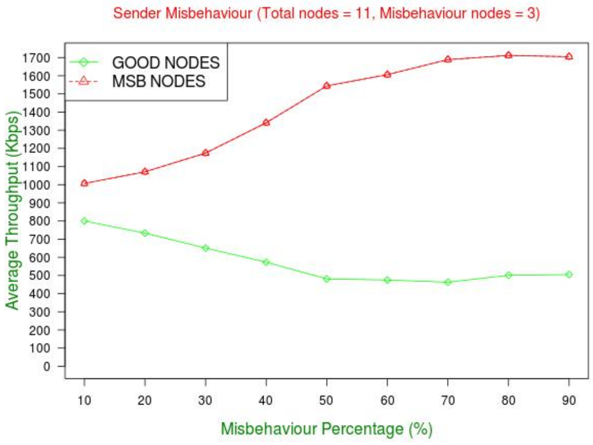


Fig. 3. Throughput with increasing senders misbehaviour percentage(SMP)

2) Increase Misbehaviour Nodes: Figure. 5 demonstrates the simulation results obtained with increasing number of misbehaving nodes, but keeping the total nodes (11), SMP (40%) and traffic rate constant. According to the graph, this can cause

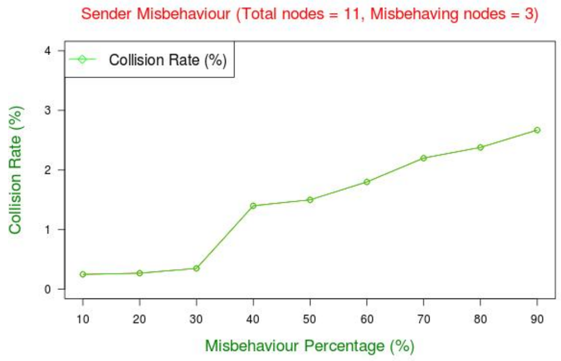


Fig. 4. CR with increasing senders misbehaviour percentage(SMP)

severe harm to the network performance due to the DoS attack generating by misbehaviour nodes. The good nodes' average throughput gradually decreases to a lower range with higher number of misbehaving nodes in the network. Furthermore, initially misbehaviour node's throughput start to rise with less number of misbehaving nodes because many misbehaving nodes compete each other for the channel access. Then, misbehaviour nodes' throughput gradually goes down with higher number of misbehaving nodes. This result suggests that increasing the number of misbehaving nodes doesn't really help for misbehaving nodes to maintain a higher throughput, but it helps to disrupt the network services. When the network has reached a state even misbehaving nodes can not gain more throughput. This graph behaviour can be explained in different point of view. Firstly, The increase the number of DoS attack launching misbehaving nodes (Fig. 6) can cause the network data packet CR to increase in considerable margins (from 0.3% to nearly 3.0%). Secondly, selfish nodes start to compete each other for optimal throughput and this can lead to increased CR thus lower throughput. Eventually, competitive selfish misbehaviours causes a perfect DoS attack situation for the network.

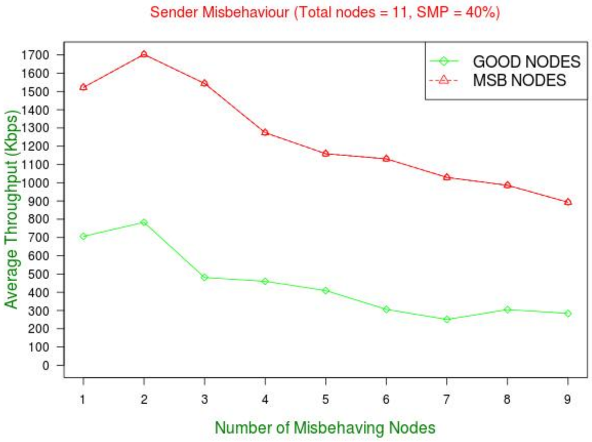


Fig. 5. Throughput with Increasing number of DoS attack launching senders

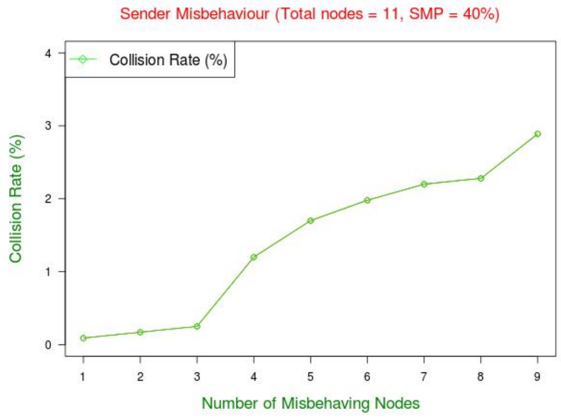


Fig. 6. CR with increasing number of DoS attack launching sender

3) Increase Network CBR Traffic: CBR traffic has changed from 1 packet per second to 16 packets per second to observe the throughput of the network. This means that DoS attack source traffic generating speed increases to moderate to high. The results show bad nodes have achieved the best throughput when the packet rate is moderate (4 packets/second) and then dramatically goes down when packet rates increases in the DoS situation in the network. The Fig. 7 shows that the increasing network traffic rate will severely affect the good node throughput as the DoS attack nodes deny the access to the good nodes. Good nodes throughput dramatically decreases after the packet rate increases more than 4 packets per second. The main reason is while backoff value manipulation helps malicious or selfish nodes to access the channel more frequently, the CR increase for good nodes. Therefore, the higher traffic rates will help the attacker to launch the DoS attack more successfully.

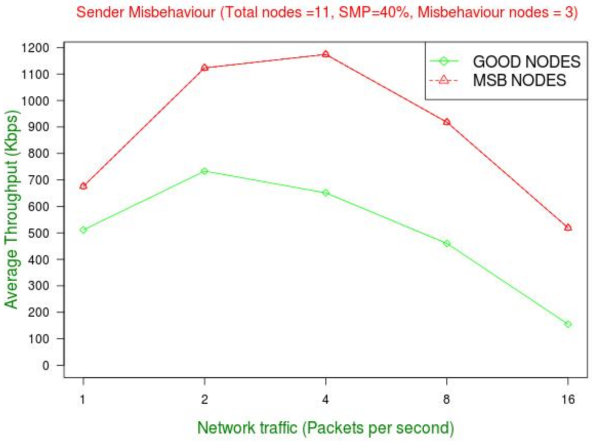


Fig. 7. Nodes throughput while increasing network CBR traffic rate

B. Receiver Generated DoS Attack Result Analysis

In MANETs receivers can be non-cooperative, and could misbehave by changing selected sender's random backoff value in CTS transmission. Greedy or malicious intended receivers could result in higher rate DoS attacks. These receivers favour misbehaving senders to increase their channel access possibility, and also increases the malicious or selfish traffic generation. The graph presented in Fig. 8 shows that well-behaving nodes have dramatically reduced throughput due to higher throughput achieved by misbehaving nodes. Furthermore, good nodes hardly get any throughput when malicious receiver attacking rate increases (RMP). Therefore, increase of RMP will cause good nodes to wait longer times to access the channel and can be a possible network collapse. The Fig. 9 demonstrates the scenario of the CR of the network when malicious/selfish senders collude with bad receivers to launch the DoS attack. In this case network suffered with a large number of collisions resulted increase of CR range (from 0.1% to 3.5%). DoS attack has been the reason for the performance degradation explained in Fig. 8. So colluded receivers can really shutdown the network with the support of senders who are already launching moderate level DoS attack.

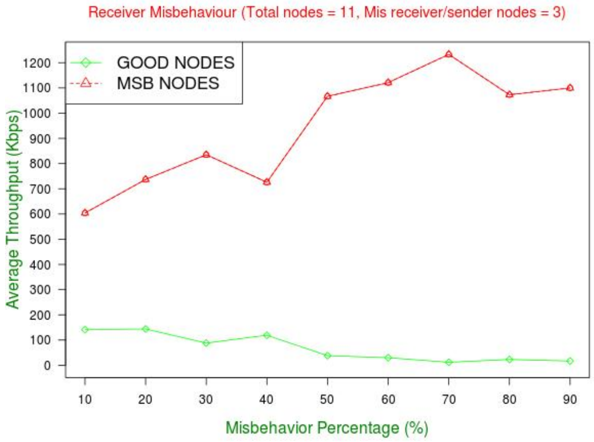


Fig. 8. Throughput with increasing number of DoS attack launching receiver aggressiveness (RMP)

VI. Prevention Mechanism and Conclusion

This paper has analysed MAC layer misbehaviour driven DoS attacks with IEEE 802.11 in MANET environment. The research has successfully performed analysis of standard IEEE 802.11 MAC protocol's sender and receiver backoff value violations which lead to partial and severe DoS attacks. The results show the effect of such DoS attacks for the network throughput and data packet CR. Therefore, IEEE 802.11 MAC protocol is not resilient against the MAC layer DoS attacks generated by backoff value policy violation at MAC layer.These practical investigations help to design resilient MAC layer protocols for MANETs. IEEE 802.11 protocol requires enhancements for detecting and penalizing the DoS attacks at MAC layer. MANETs are unique networks with unique characteristics which could lead such DoS attacks to be very effective. Such designs need to consider that MANET has no centralized management to deploy mechanism to detect such attacks. We suggest decentralized detection mechanism at MAC layer to apply with a better trust management mechanism. Also, there is a requirement for a transparent backoff value allocation and monitoring. A novel trust management mechanism among the nodes could help the network nodes to be aware of such protocol violations, thus nodes knows which nodes to trust in their communication.

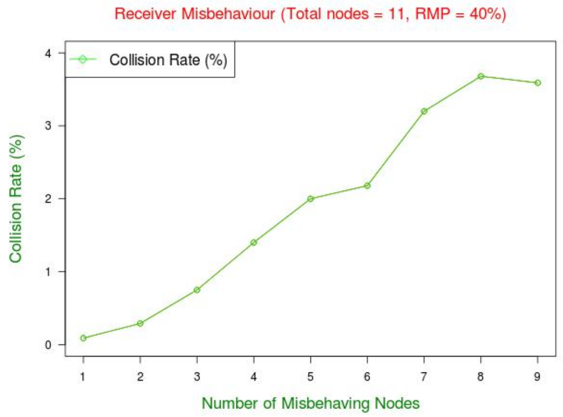


Fig. 9. CR with increasing number of DoS attack launching sender and receivers

References

[1] Y. Kim and G. Hwang, "Design and analysis of medium access protocol: Throughput and short-term fairness perspective," *Networking, IEEE/ACM Transactions on*, vol. PP, no. 99, pp. 1–14, 2014.

[2] H. Diwanji and J. Shah, "Effect of mac layer protocol in building trust and reputation scheme in mobile ad hoc network," in *Engineering (NUiCONE), 2013 Nirma University International Conference on*, Nov 2013, pp. 1–3.

[3] M. K. Han and L. Qiu, "Greedy receivers in IEEE 802.11 hotspots: Impacts and detection," *Dependable and Secure Computing, IEEE Transactions on*, vol. 7, no. 4, pp. 410–423, Oct 2010.

[4] P. Nagarjun, V. Kumar, C. Kumar, and A. Ravi, "Simulation and analysis of rts/cts dos attack variants in 802.11 networks," in *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on*, Feb 2013, pp. 258–263.

[5] F. Shi, J. Baek, J. Song, and W. Liu, "A novel scheme to prevent mac layer misbehavior in IEEE 802.11 ad hoc networks," *Telecommunication Systems*, vol. 52, no. 4, pp. 2397–2406, 2013.

[6] P. Kyasanur and N. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 4, no. 5, pp. 502–516, Sept 2005.

[7] S. Radosavac, A. A. Cárdenas, J. S. Baras, and G. V. Moustakides, "Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers," *Journal of Computer Security*, vol. 15, no. 1, pp. 103–128, 2007.

[8] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 931 – 941, 2009, specification, Standards and Information Management for Distributed Systems.

[9] A. S. A. Balador and D. Kanellopoulos, "Mac layer misbehavior in manets," *IETE TECHNICAL REVIEW*, vol. 30, no. 4, pp. 410–423, JUL-AUG 2013.

[10] S. Djahel, Z. Zhang, F. Nait-Abdesselam, and J. Murphy, "Fast and efficient countermeasure for MAC layer misbehavior in manets," *Wireless Communications Letters, IEEE*, vol. 1, no. 5, pp. 540–543, October 2012.