Evaluation and Prevention of MAC Layer Misbehaviours in Public Wireless Hotspots

Chaminda Alocious, Hannan Xiao, Bruce Christianson and James Malcolm
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (c.alocious, h.xiao, b.christianson, j.a.malcolm)@herts.ac.uk

***Abstract*—IEEE 802.11 protocol assumes all the nodes in the network cooperate and adhere to the standard. However, nodes may purposefully misbehave in order to obtain extra bandwidth, conserve resources or disrupt network performance. Previously, Kausanaur proposed a Receiver Trusted MAC protocol (REC-TR-MAC) by extending IEEE 802.11 to prevent Medium Access Control (MAC) sender misbehaviours. This protocol trusts the receiving node (Access Point) in a WLAN and enables the Access Point to allocate the MAC protocol random backoff values for wireless clients. Our research investigates MAC layer node misbehaviours in the context of a Public Wireless Hotspot. REC-TR-MAC has been implemented by porting the legacy code-base to the latest ns2. Furthermore, our evaluation has been extended to incorporate several Access Point misbehaviours to simulate the scenario of an untrusted hotspot (misbehaving access point) , which has not been investigated much in the literature. In public wireless hotspot the misbehaving wireless senders could run a malware at the Hotspot to gain the access to alter the MAC protocol operation. The experiment results show that Hotspot misbehaviours significantly affect the network performance, nodes throughput reduced by 50% and misbehaviour detection accuracy by 40%. The results have also been compared with the standard IEEE 802.11 protocol. This evaluation is important to understand the design principles for a reliable MAC protocol which should be resilient against MAC layer misbehaviours. Finally, this paper describes future improvements for detecting and preventing MAC layer misbehaviours in Wi-Fi networks.**

Keywords*—*Wireless Network Security, IEEE 802.11, Wi-Fi Hotspot, Medium Access Control, MAC Layer Misbehaviours

I. Introduction

Public wireless Hotspot uses Wi-Fi technology and acts as an internet Access Point (AP) in public locations. Widespread of public Hotspot making wireless network security important than ever, such networks are more exposed to attackers more than any other network type. Wireless LAN is an infrastructure-based network which is controlled by a centralized AP, which is the receiver of the network of all the connected client nodes. Most of the devices in these networks are running standard IEEE 802.11 protocol. The IEEE 802.11 MAC protocol is used for the coordination and scheduling of transmissions among competing nodes in wireless networks. It assumes that all the nodes in the wireless network ad-here and fully cooperate. However, MAC layer node misbehaviours have been a problematic scenario for WLAN network performance. Due to the vast enhancement of network device adapters' programmability, changing the MAC layer protocol parameters has become easier.

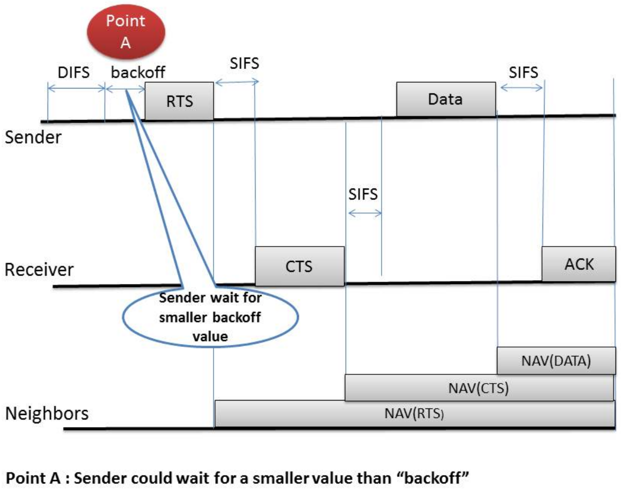
In public wireless hotspot the misbehaving wireless senders could run a malware at the hotspot to gain the access to alter the MAC protocol operations in AP (violating IEEE 802.11 channel access policy), then such a hotspot is untrusted. Our research has implemented an untrusted wireless hotspot in ns2 simulation [1] to evaluate untrusted hotspot communicate with misbehaving clients. This paper investigates the performance effect of misbehaving clients and misbehaving receiver (untrusted hotspot) colluding with misbehaving client nodes in a wireless Wi-Fi environment.

The rest of this paper is organized as follows. The next section elaborates the theoretical aspects of the MAC layer misbehaviours and research background with related work. Section III presents the details of the receiver trusted protocol that will be investigated in detail. Section IV demonstrates and evaluates the receiver-trusted based mechanism with a trusted hotspot with misbehaving senders. Section V evaluates the protocol with an untrusted hotspot with misbehaving senders. Finally, section VI concludes the paper with result conclusion and with a suggested detection mechanism.

II. Research Background

IEEE 802.11 is the most common MAC protocol in wireless networks, which uses the CSMA/CA channel access mechanism to access the shared wireless channel. In this method a node intends to transfer a data packet for a destination 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. The Fig. 1 demonstrates the communication between the sender station and the receiver station while the neighbours listening to the ongoing communication.

In this mechanism a node uses the Distributed Coordination Function (DCF) which is based on the the binary exponential backoff (BEB) mechanism to assign randomly chosen backoff values to each wireless station in the network, aiming to allow each wireless station to get a fair share of the wireless channel. However, misbehaving nodes could manipulate these parameters to their own advantage with the purpose of malicious or selfish. One of the points highlighted in the Fig. 1 is the sender waits for a smaller random backoff value rather protocol defined value. There are other variations of manipulations which are devastating for network performance, such as senders and receivers sets the Network Allocation Vector (NAV) values higher so then the neighbour nodes are waiting longer to access the channel.



Point A : Sender could wait for a smaller value than “backoff”

Fig. 1. Sender and receiver message interaction of CSMA/CA protocol

A. IEEE 802.11 Protocol Misbehaviour

MAC layer misbehaviour, violating IEEE 802.11 channel access policy, is a major security concern for wireless network performance and availability. MAC layer misbehaviour can be classified into selfish misbehaviour and malicious misbehaviour. Selfish misbehaviour intends to get more bandwidth over the performance of other well behaved wireless nodes. Malicious misbehaving nodes want to disrupt the network services so that legitimate wireless nodes cannot access the network services. MAC layer misbehaviours also can be considered as low or moderate level DoS attacks which drain the network throughput for the legitimate users. It is important to evaluate the effect of such important node behaviours in designing MAC protocol. The misbehaving nodes can exploit protocol parameters and mechanism to misbehave by modifying wireless network adaptors. This paper evaluates following misbehaviours which were implemented in ns2 to simulate a Wi-Fi public hotspot.

1) Backoff Value Manipulation: In the IEEE 802.11 MAC protocol some nodes could use smaller back-off values by selecting backoff values from a different distribution. Additionally, selfish nodes could use fixed backoff values instead of random values. This misbehaviour includes nodes that do not double the CW size after a collision. In this investigation the backoff value manipulation has been simulated as the misbehaviour attacks in both hotspot and senders.

2) NAV, DIFS and SIFS Manipulations: In this category of attacks use to launch moderate or higher level DoS attacks which legitimise nodes unable to access the channel. NAV is to configure and communicate that channel is being used by another user for a specified number slots, which they hear from the sender or receiver node (neighbours obtaining this value from the RTS and CTS transmission), if the sender or receiver manipulate this value to be larger then the neighbours will set a higher value which will reduce neighbour nodes deserved channel access. Similarly, nodes might wait for smaller DIFS or SIFS value rather defined in the protocol to complete the transaction early so that node get more frequent channel access.

3) Adaptive Cheating / Smart Misbehaviours: Adaptive cheating or smart misbehaviours, where some nodes are smart enough to adapt their misbehaviour strategy to prevent being caught, such nodes are aware of the detection scheme and adapt their behaviour to mislead the detection. In our evaluation adaptive misbehaviour has been evaluated.

4) Colluding Nodes: In this type of attacks the client device has been able to override the AP configuration which allow client nodes (senders) and the AP to misbehave as a pair. In this case, if there is a scheme that trusts the sender or at least one of the parties, then such misbehaviour could be complicated to detect. We analyses the colluding node misbehaviour by simulation Hotspot colluding with senders in a randomly chosen pattern. The colluding attacks are described to demonstrate a possible AP vulnerabilities which could practically work in public hotspot environment.

B. 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, which could lead to nodes starvation. Their research focused on the affects 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. The RTS/CTS attack is one type of low rate DoS attack which is 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].

In the research proposed by Radosavac et.al. carried out a performance evaluation and trade-offs of optimal back-off misbehaviour detection schemes in wireless networks in the presence of interference [5]. Their approach evaluate the trade-offs that both the adversary and the detector (monitoring entity) face under adaptive different conditions and investigates the performance matrix using a game theoretic framework. They also evaluate the worst-case scenarios under which the given detector can efficiently operate under the predetermined conditions and demonstrate by both mathematical analysis and simulation. In their research they discuss the presence of adaptive intelligent adversaries which changing environment conditions and construct a argument that the adoption of a static detection system is not advisable in such environments and requirement for an adaptive detection system in order to maintain satisfying performance under a wide range of changing network conditions.

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. Furthermore, in [7] has studied DoS attacks and countermeasures in IEEE 802.11 wireless networks. The research in [8] has presented a comprehensive analysis of modern MAC layer misbehaviour detection mechanisms. Therefore, it is important to analyse protocol vulnerabilities experimentally for the security of MAC layer in wireless network. MAC layer misbehaviour attacks evaluation could improve the accuracy and capability of MAC layer selfish and malicious misbehaviour detection mechanisms [9] [10] [5] [11] [12].

III. A Receiver Trusted MAC Protocol(REC-TR-MAC)

MAC layer misbehaviours has become a severe concern for wireless networks, there has been many mac layer misbheaviour detection mechanisms. The researches in [6] have demonstrated a **Receiver-Trusted** MAC layer misbehaviour detection protocol for WLANs which has discussed the issue of selfish wireless nodes waiting for smaller backoff intervals in CSMA/CA based MAC protocol. A wireless station which required to transfer a data packet required to follow the CSMA/CA control packet exchange procedure which involves node required to wait a randomly selected backoff value before start to transmit RTS control packet. However, the problem identified by this research is nodes might not follow this procedure due to misbehaviour intentions which could significantly affect the network performance.

Their research work presents a modification to the IEEE 802.11 protocol, capable of detecting and mitigating MAC layer misbehaviours in a WLAN environment with a trusted AP. In a WLAN, in most cases, it is possible to assume that the AP is trusted in infrastructure-based networks. In their approach the AP act as a monitor entity to observe and allocate backoff values for the senders. Therefore, if the sender deviates from the protocol by waiting for a small backoff value, the AP identifies the sender as a misbehaving node by observing consecutive transmissions. The REC-TR-MAC protocol includes detection scheme, penalty scheme and diagnosis scheme.

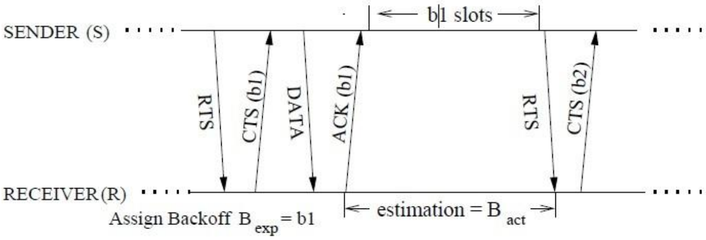


Fig. 2. Sender and receiver protocol CSMA/CA message interaction

The Fig. 2 shows the interaction between the sender and the receiver in the context of MAC layer CSMA/CA message exchange. In CTS control packet the AP sends the backoff value to the sender which sender must use in next transmission.

A. Detection Scheme

Detection scheme is to detect the senders backoff value variations in consecutive transmission. AP decides at the end of a RTS control packet transmission whether the sender has deviated from allocated random backoff value slots or not by (1). The detection scheme is inside the AP which collects the deviated sender backoff timer slots.

$$Deviation(D) = B_{act} - \alpha * B_{exp} \tag{1}$$

Where D is the deviation slots for the sender, (B_{act}) is the observed number of idle slots and (B_{exp}) is the allocated backoff slots for the sender. α is a factor value between 0 to 1. This value can vary based on the channel condition such as channel traffic density and jitter. The sender is designated as deviating from the protocol, if the observed number of idle slots (B_{act}) is smaller than a specified fraction of the assigned backoff value (B_{exp}). However, a deviation does not necessarily indicate that the sender is misbehaving, as the channel conditions seen by the sender and AP may be different. Therefore, detection mechanism required to observe for multiple transmissions and consider means deviation which will be explain in diagnosis scheme. This detection scheme has located inside the AP, this is a centralized detection strategy which works for infrastructure based wireless networks.

B. Penalty Scheme

The penalty scheme works as a misbehaviour prevention and discouraging mechanism, penalty value is calculated by the receiver which was based on the senders previous behaviour. Then the receiver assigning a penalty value for each senders detected backoff value deviation if the AP has identified any deviation in a transmission from the sender, it penalizes the sender by assigning a penalty value based on the magnitude of the perceived deviation for that particular transmission as in (2).

$$P = D + random([0, CW_{min}]) \tag{2}$$

P is the total penalty backoff value assigned by the receiver. The experimental result recognises that penalty for the sender required additional backoff value as represented by $random([0, CW_{min}])$ which is a random function which provides a values between 0 to CW_{min}, where CW_{min} is the minimum contention window value.

C. Diagnosis Scheme

Diagnosis scheme used to diagnose bad clients after defined number of transmission attempts at the receiver (AP). Diagnosis scheme is based on the magnitude of the perceived deviation over multiple transmissions from the sender, the receiver diagnoses whether the sender is indeed misbehaving or not according to (3).

$$T < \sum_{i=0}^{N} D_i \tag{3}$$

T is the number of diagnosing idle threshold slots, i is the number transmission which range from 0 to N. The receiver maintains information about the last N packets received from each sender in the WLAN. The receiver stores the difference of B_{exp} and B_{act}, and then calculate the sum of these differences to check against the detection threshold value (T). If the difference of observed idle slots greater than T over multiple transmission then the sender is diagnosed as ”misbehaving”. Once the detection mechanism detected such nodes, it could decide on such nodes future participation of the network, strict network policies could be implemented to inform upper layers or add the node to a blacklist.

D. Misbehaviour Models

The REC-TR-MAC has implemented two misbehaviour models; the persistent, and the adaptive model. In persistent misbehaviour model nodes are misbehaving to a constant pattern, such as backoff for a smaller backoff value than the allocated backoff value. Wireless nodes in persistent misbehaviour model do not change their misbehaviour strategy to avoid being detected [6]. If the sender has a persistent misbehaviour percentage of 20%, then it only waits for 80% of the actual allocated backoff value. The persistent misbehaviours can cause a lot of damage for the time they are active, but they are easy to detect. The adaptive misbehaviour models are capable of escaping the detection mechanisms by selecting the backoff values based on a smart value selection procedure. In this model a misbehaving node with adaptive misbehaviour, should suitably adjust the magnitude of misbehaviour based on the assigned backoff value by the standard protocol or the detection mechanism.

IV. REC-TR-MAC Evaluation with Trusted Wi-Fi Hotspot

One of the motivation of this research is to apply the client nodes wireless channel access violations at MAC layer and evaluates the performance implications for Wi-Fi hotspot. This section evaluates the REC-TR-MAC protocol with a trusted Wi-Fi hotspot with few misbehaving clients. In this case, the hotspot is trustworthy and operates according to the IEEE 802.11 protocol specification. However, some random clients will try to obtain more throughput over other well behaved nodes by violating IEEE 802.11 channel access policy. Also this section explains the simulation setup and result analysis of REC-TR-MAC protocol, operating in trusted hotspot environment with both persistent and adaptive misbehaviour models.

A. Simulation Configuration and Performance Matrices

The project uses ns2.35 network simulation environment with Linux operating system which consists with Corei7 processor and 24 Gigabytes of RAM. Simulation configuration consists with topology design, traffic configuration and misbehaviour configuration. In Fig. 3, the network topology consists of 8 sender nodes and one single receiver node (AP) that operates as the hotspot in a Wi-Fi environment. Each sender nodes is 150 m away from the AP, forming a circle. The two other extra data flows that distract the transmissions from A to B and C to D (distraction is simulated to provide real network situation where other nodes interfere in CSMA/CA mechanism). The simulations have been designed to investigate effectiveness of the REC-TR-MAC detection mechanism in this environment with misbehaving clients.

In this topology each sender generates a constant bit rate (CBR) traffic flow towards the hotspot according the configuration in Table. I. The sender misbehaviour percentage (SMP) is defined as the ratio of the actual backoff value that sender waited and the expected backoff slots that sender should have waited. The AP or hotspot misbehaviour percentage (HMP) is the ratio of the actual backoff time slots that the Hotspot allocates to a colluding sender node to the expected backoff slots that it should have allocated. The designed WLAN’s CBR traffic flows from each sender (clients nodes) to the Hotspot with a rate of 4 packets per second with each packet size with 512 bytes. The wireless channel bandwidth is 2Mbp/s which is shared between 8 sender nodes and based on the following table each nodes sends 2 Kbytes/s (4x512 bytes per a second) CBR traffic flow towards the Hotspot.

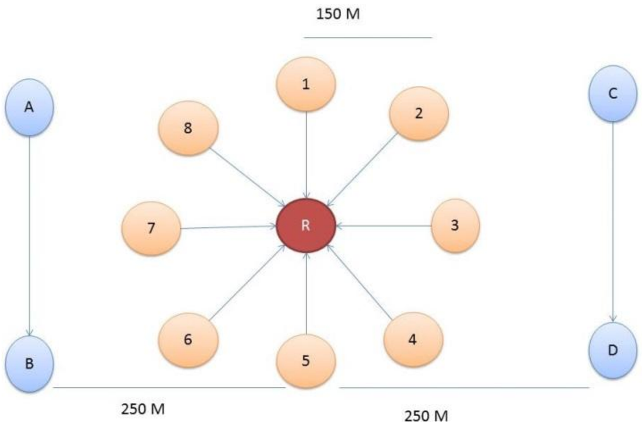


Fig. 3. WLAN Network Topology

Following performance matrix used to evaluate the effect of MAC layer misbehaviours for the network performance. In our evaluation following performance metrics have been consider.

TABLE I. SIMULATION CONFIGURATION IN WIRELESS HOTSPOT

Traffic type	CBR
Packet size	512 bytes
Packet interval	0.25 Seconds
Max no of packets	100000
Max connections	10
Number of total nodes	9
Number of misbehaviour nodes	2
Routing protocol	DSR
X-Dimension	1500 Meters
Y-Dimension	750 Meters
Monitoring Period(W)	5 Packets
Detection deviation threshold slots	20 Slots
Simulation time	500 Seconds
Sender Misbehaviour Percentage (SMP)	(1%-100%)
Hotspot Misbehaviour Percentage (HMP)	(1%-100%)
Simulation time	500 Seconds

- Good Nodes Throughput: This is obtained by dividing the total throughput of good nodes from the number of nodes.
- Misbehaviour Nodes Throughput: This is obtained by dividing the total misbehaviour throughput by the number of misbehaviour nodes. This gives a measurement for a average throughput achieved by a misbehaving node.
- Correct diagnosis percentage: Correct diagnosis is important to measure the accuracy of the detection mechanism , this value is obtained by obtaining the percentage of the ratio value of the correctly predicted packets and the mis-predicted packets for misbehaving nodes.
- Misdiagnosis percentage: The percentage of the ratio value of the total number of mis-predicted and correctly predicted packets for a well-behaved nodes.

B. Trusted Wi-Fi Hotspot Result Analysis

Firstly, the REC-TR-MAC protocol's throughput and detection accuracy results have been compared against the standard IEEE 802.11 protocol. The simulation has run for different seeds numbers (1-5) to obtain an average values for the throughput and diagnosis accuracy. Fig. 4 visualizes the average throughput of well-behaved nodes and misbehaving nodes in the REC-TR-MAC protocol and the IEEE 802.11 standard protocol.

According to the Fig. 4, when the sender's misbehaviour percentage (SMP) changes from 1% to 100%, the gap between the average throughput of the good node and misbehaviour node is narrower in the REC-TR-MAC protocol (blue and purple) than in the standard IEEE 802.11 protocol (red and green). In the REC-TR-MAC protocol, after SMP reaches 50%, the throughput of the misbehaviour nodes increases dramatically with the IEEE 802.11 protocol while the REC-TR-MAC protocol is able to maintain the throughput of the misbehaving nodes. Similarly, well behaving nodes are able to maintain a better throughput in the REC-TR-MAC protocol than in the IEEE 802.11 protocol. Therefore, when the sender misbehaves with persistent misbehaviour model with the REC-TR-MAC shows better resilience.

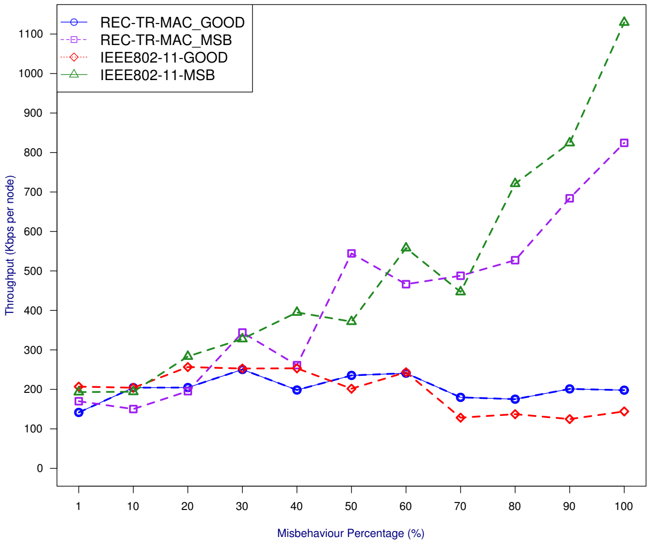


Fig. 4. Throughput vs Misbehaviour (%) in persistent sender misbehaving

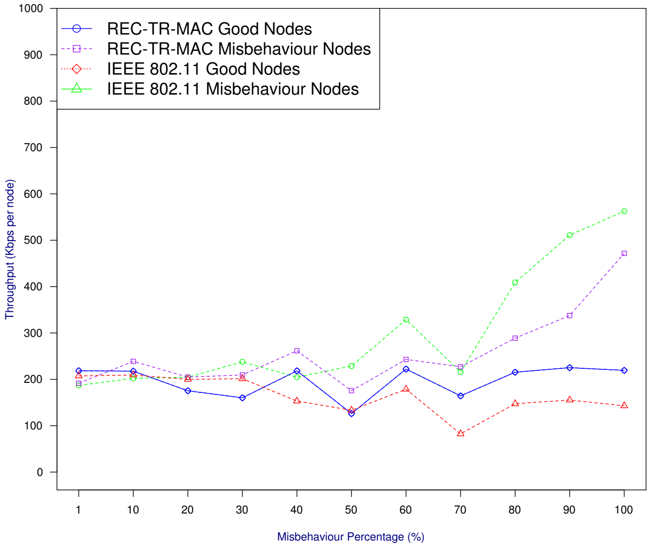


Fig. 5. Throughput Vs Misbehaviour (%) in adaptive misbehaviour sender misbehaving

The results demonstrated in Fig. 5 confirm that the REC-TR-MAC protocol is resilient against the adaptive misbehaviours, when it is compared to the IEEE 802.11 protocol. The REC-TR-MAC does not allow adaptive misbehaving nodes to obtain extra throughput. Furthermore, well behaving nodes are obtaining a better throughput than the standard protocol. However, when both protocols are run under an extreme SMP (90%), it has appeared that most of the good nodes get less throughput and the rest of the nodes get a small portion of the throughput.

Fig. 6 shows the REC-TR-MAC protocol's misbehaviour diagnosis accuracy in the persistent misbehaviour model. According to the results, the detection mechanism shows excellent ability to detect misbehaving nodes when the sender (MP) is high. Therefore, it shows much less false alarms when

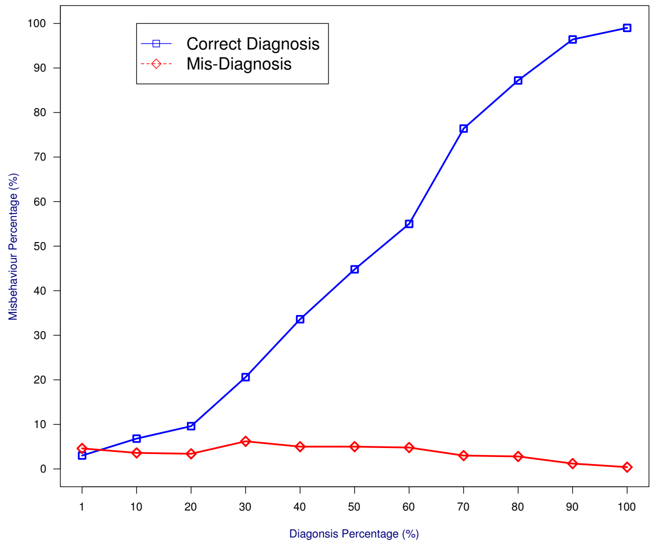


Fig. 6. Diagnosis accuracy of the REC-TR-MAC with persistent sender misbehaviour

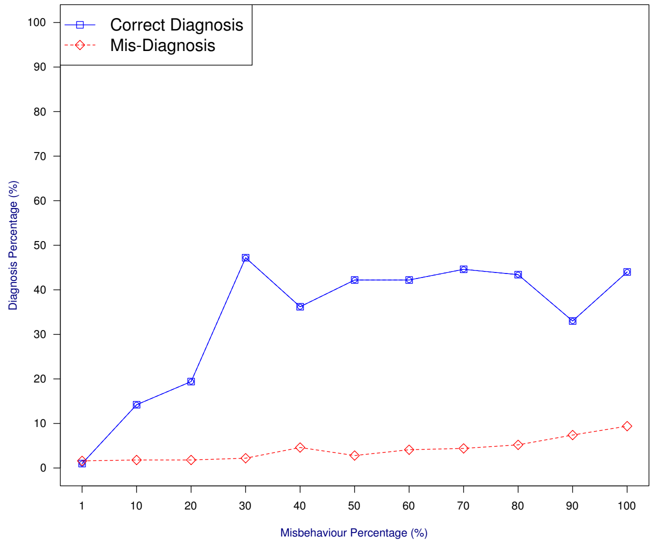


Fig. 7. Diagnosis accuracy of the REC-TR-MAC with adaptive sender misbehaviour

it operates on a trusted hotspot environment. Furthermore, Fig. 7 shows that under the adaptive sender misbehaviour, the detection accuracy of the REC-TR-MAC has dropped dramatically compared to the persistent misbehaviour model detection accuracy (Fig. 6). This result confirms that adaptive misbehaviour is difficult to diagnose with the REC-TR-MAC mechanism. The detection of adaptive or smart misbheaviour required more flexible detection rules and conditions which explore the senders behaving patterns which future MAC protocol designs could include.

V. REC-TR-MAC Evaluation on Untrusted Wi-Fi Hotspot

The REC-TR-MAC protocol has limitations of applying to environments where the Wi-Fi Hotspot is not trusted or it has not been controlled by an certified authority. The REC-TR-MAC protocol does not have the countermeasures for such protocol violation misbehaviours. Our research has identified such protocol violations. AP could ignore allocating a penalty for identified misbehaving senders. According to the message exchange of REC-TR-MAC, the sender is forced to completely trust the AP, even if the AP is corrupted and not functioning as the specification. There is no measurement for the receivers credibility. This section evaluates the applicability of REC-TR-MAC in Wi-Fi untrusted hotspot environment, where the hotspot itself is misbehaving by a fault or by a deployed attack by a third party. Our implementation has been extended to incorporate several hotspot misbehaviour attacks which have not been investigated in literature.

A. *Hotspot Misbehaviour / Attacks Models*

In a misbehaving hotspot, the hotspot may favour some clients in the Wi-Fi network by increasing the client channel access frequency, thereby such clients achieve more throughput. This paper has demonstrated three practically implemented attack models in the hotspot. Firstly, in a given point if the sender misbehaves by 20% (SMP) of the original allocated backoff value, then the hotspot also reduces this value by another 20% (HMP) in the CTS communication in CSMA/CA message exchange when the hotspot allocates backoff values.

Secondly, the hotspot avoids assigning the full penalty value for misbehaving nodes once detected as deviating (penalty values used to discourage misbehaving nodes). If the hotspot ignores the penalty value, the sender can continue misbehaviour without getting caught. Finally, the hotspot can ignore the re-transmission attempt value which used to calculate consecutive backoff values after a collision and AP could misbehave to assign it's own attempt number. This will eventually affect the system's performance by increasing system congestion.

B. *Simulation Configuration*

The simulation topology for the Hotspot Misbehaviour is same as in Fig. 3. In this case there are colluding misbehaving senders which collude with the AP to perform one of the earlier explained hotspot misbehaviour. Therefore, such nodes can increase their channel access ability dramatically. The hotspot misbehaviour has been added to ns2 as a new backoff policy (which simulates this attack model), which can be tested against the REC-TR-MAC protocol.

C. *Hotspot Misbehaviour Result Analysis*

Our research mainly focus on hotspot misbehaviour models and the affect such attacks for the network performance. The Fig. 8 shows the results of the hotspot misbehaviour model which the hotspot is increasing the channel access frequency of randomly selected senders, by reducing senders backoff value by HMP amount from the initial allocated backoff value. Under this misbehaviour the REC-TR-MAC protocol's nodes able to achieve an average throughput. However, it has failed to stop misbehaviour nodes from achieving larger throughput.

Further, the results confirm that the hotspot misbehaviours severely effect the network throughput and the diagnosis accuracy of the detection mechanism. The wireless hotspot misbehaviour strategy allowed the colluding clients to use the channel more frequently, hence achieve more throughput. However, when the HMP is lower, the IEEE 802.11 protocol shows better throughput for well-behaved nodes comparing to the REC-TR-MAC protocol. Furthermore, the REC-TR-MAC misbehaving node's throughput is dramatically increased at the presence of higher HMP. In Fig. 9 the REC-TR-MAC shows a poor ability to detect misbehaving nodes when the hotspot is misbehaving in high percentages.

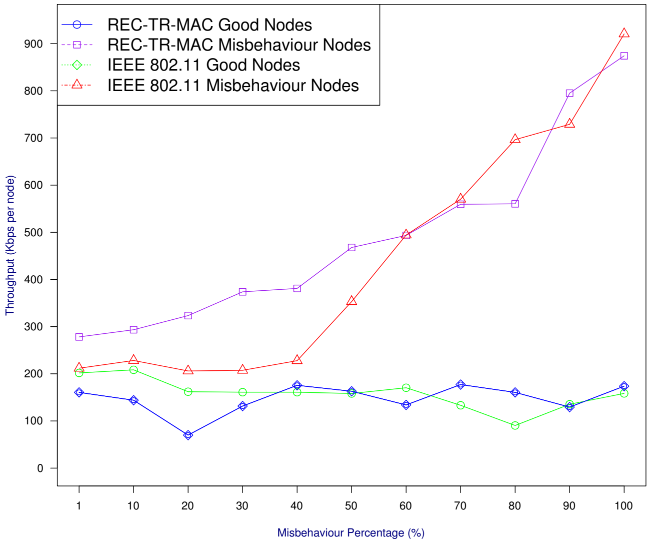


Fig. 8. REC-TR-MAC vs IEEE 802.11 - Throughput vs Misbehaviour (%) - Hotspot misbehaving

VI. Conclusion and Future Work

The experimental results suggest that MAC layer greediness introduced to the public hotspot can have devastating effects with both trusted and untrusted AP. The comprehensive results derive the argument of considering the trustworthiness in the designing of MAC layer misbehaviour detection and prevention systems. Therefore, this research concludes that, the current MAC protocol is not resilient to untrusted hotspot environments. The results show that performance can drop by 50% while the access point misbehave in moderate level, also possibility of the entire network could collapse with higher level of misbehaviour aggressiveness. The presence of adaptive adversaries the detection accuracy of the REC-TR-MAC protocol is around 30% lower, therefore protocol designs such as REC-TR-MAC it will be hard to operate in such adaptive changing network environment. Therefore, the current detection mechanisms require enhancement to detect and penalize untrusted (misbehaving) or faulty hotspots. If the AP is in a more hostile environment such as public wireless hotspot, MAC layer detection mechanisms required more attention towards availability and reliability of the network same as the data confidentiality and integrity.

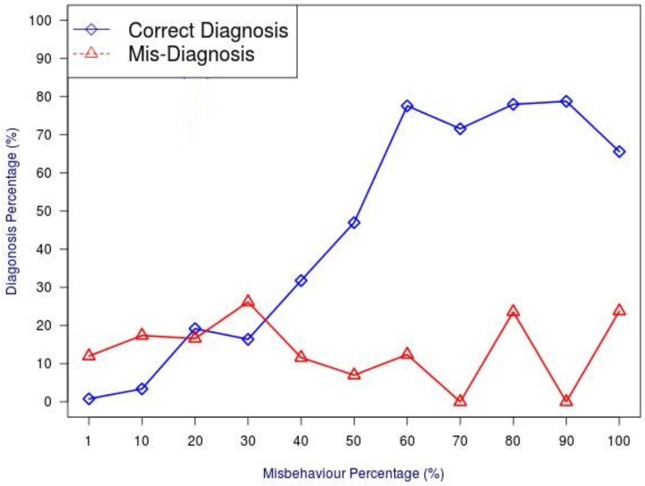


Fig. 9. REC-TR-MAC diagnosis accuracy while Hotspot misbehaviour

Currently, we are working on extending MAC layer detection mechanism to apply with a better trust management between clients and hotspot to detect and prevent MAC layer misbehaviours. Our research has identified that there is a requirement for a transparent backoff value allocation mechanism, which could be integrated to IEEE 802.11 channel sharing function (DCF) whereby nearby nodes can verify that others are not violating the channel access mechanism. Our future research work has focus on involving a more distributed and transparent mechanism to observe MAC layer protocol parameters. The authors in [11] have presented a predictable random backoff (PRB) algorithm to mitigate the effect of the smart MAC layer misbehaviours which requires minor modification to the IEEE 802.11 protocol's Binary Exponential Backoff (BEB) algorithm. This modification forces every node in the network to generate a predictable random backoff value. However, such a mechanism also forces to attacker to predict the backoff value sequence easily, therefore we are currently working on verifiable backoff value generation mechanism which also can keep the randomsness of the protocol.

MAC layer misbehaviour detection in public hotspot required more extended monitoring mechanism which could involve base station set (BSS) and extended basic service set (ESS). The ESS consists of many BSS in the Wi-Fi network. One of the strategies to detect such misbehaviours is to use BSS to track the behaviour of APs under each BSS. In order to monitor AP behaviours, BSS needs to be perform as a monitoring entity and monitor AP communications. The BSS could periodically obtains the backoff value table from each AP and analyse for abnormal backoff values, in this case BSS also should know the deterministic function which AP used to generate backoff values. Furthermore, the research proposed by Rong at el. in [13] explains a statistical and probabilistic model that can be utilized to detect cheating stations. Statistical detection techniques gather the AP transaction data to analyse wireless AP behaviours, and also they can be utilized to detect other abnormal behaviours.

References

[1] K. Liu, "Understanding the implementation of IEEE MAC 802.11 standard in ns-2."

[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, 2013 International Conference on*, Feb 2013, pp. 258–263.

[5] S. Radosavac and J. S. Baras, "Performance evaluation and trade-offs of optimal back-off misbehavior detection schemes in wireless networks in the presence of interference," in *Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools*, ser. ValueTools '08, ICST, Brussels, Belgium, 2008, pp. 31:1–31:10.

[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] 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.

[8] 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.

[9] L. Guang, C. Assi, and A. Benslimane, "Enhancing IEEE 802.11 random backoff in selfish environments," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 3, pp. 1806–1822, May 2008.

[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.

[11] L. Guang and C. Assi, "Mitigating smart selfish MAC layer misbehavior in ad hoc networks," in *Wireless and Mobile Computing, Networking and Communications, 2006. (WiMob'2006). IEEE International Conference on*, June 2006, pp. 116–123.

[12] R. Gunasekaran, V. R. Uthariaraj, U. Yamini, R. Sudharsan, and S. S. Priyadarshini, "A distributed mechanism for handling of adaptive/intelligent selfish misbehaviour at MAC layer in mobile ad hoc networks." *J. Comput. Sci. Technol.*, vol. 24, no. 3, pp. 472–481, 2009.

[13] Y. Rong, S. K. Lee, and H.-A. Choi, "Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis," vol. 2, no. 4, 2006.