Assessing RoQ Attacks on MANETs over Aware and Unaware TPC Techniques

Urlan Barros,* **Mathieu Bouet**†, **Aldri Santos*** and **Michele Nogueira***
* Department of Informatics, Federal University of Paraná, Brazil
† Thales Communications, France
{urlan, aldri, michele}@inf.ufpr.br, mathieu.bouet@fr.thalesgroup.com

***Abstract*—Adaptation mechanisms, such as transmission power control (TPC) techniques, cognitive radio technology and intelligent antenna, have been applied to efficiently manage the use of resources on wireless ad hoc networks. However, these mechanisms open doors for Reduction of Quality (RoQ) attacks. Those attacks damage network services exploiting adaptation capability and they can be easily launched on mobile ad hoc networks (MANETs). This paper assesses the influence of RoQ attacks on MANETs, aiming to provide insights and lead the design of control access mechanisms able to prevent or mitigate them. We evaluate MANETs supported by a modified IEEE 802.11 using unaware and aware TPC techniques. We analyze the impact of three types of RoQ attacks by simulations, and we show their effect over more dynamic aware TPC techniques.**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) comprise different devices (nodes) communicating among them in a wireless multi-hop way and with no control infrastructure. These characteristics result in constant changes on network topology, conditions and environment, requiring fast adaptation of essential services as connectivity.Thus, several adaptation mechanisms have been applied to efficiently manage the use of resources on MANETs, such as transmission power control techniques [1], cognitive radio technology [2] and intelligent antenna [3].

Transmission power control (TPC) techniques enable to save energy and reduce interference on wireless networks. They improve the performance of IEEE 802.11, particularly, the network throughput by the spatial reuse of the medium [4]. TPC allows transmitter nodes to send frames to the medium using power levels defined dynamically, saving energy and ensuring that destination nodes can decode frames [1]. By TPC techniques, nodes can transmit at the same time, increasing their lifetime by the reduction of energy consumption.

MANETs are vulnerable to different security issues due to their characteristics [5]. Wireless communication, for instance, is prone to interferences and interceptions, being susceptible to attacks against hop-to-hop connectivity. The network autonomy makes easy the participation of malicious or selfish nodes in network operations, resulting in damage to multi-hop or end-to-end communications. Further, network adapters are becoming *reprogrammable*, making easy the modification of their behavior by users [2], [3].

Adaptation mechanisms, like TPC techniques, open doors for Reduction of Quality (RoQ) attacks on all layers of the protocol stack [6]. RoQ attacks exploit adaptation capability on communication mechanisms inducing oscillations between overload and underload states [7]. RoQ attacks aim at depriving nodes of their capacity by degrading network services. These attacks are an instance of Denial of Service (DoS) attacks [8], differentiating from them by sustaining no attack traffic to make network services unresponsive. Such characteristics make RoQ attacks detection a demanding task.

In this paper, we assess the influence of RoQ attacks on the end-to-end communication and connectivity of MANETs employing IEEE 802.11. The main goal lies in providing insights and leading the design of control access mechanisms able to prevent or mitigate RoQ attacks. We consider MANETs using a modified IEEE 802.11 that employs TPC techniques. Particularly, we evaluate the impact of RoQ attacks over dynamic aware AEWMA TPC techniques, which intend to be aware of channel state and link performance. We analyze the influence of three RoQ attack types, flooding, round-robin and self-whisper [5], that establish asymmetric links.

Simulation results show that RoQ attacks affect significantly MANETs employing 802.11 or the modified 802.11 using TPC techniques. RoQ attacks yield a higher impact on dynamic aware TPC techniques. Further, self-whisper and round-robin attacks are the most powerful, decreasing network performance and increasing the consumption of energy.

This paper proceeds as follows. Section II gives a brief overview of TPC techniques. Section III details the investigated RoQ attacks. Section IV describes the methodology used to evaluate the implications of RoQ attacks and shows results. Finally, Section V presents conclusions and future works.

II. TPC TECHNIQUES

By default, nodes that use the standard IEEE 802.11 (called only 802.11) do not employ TPC techniques. They transmit all frames using the maximum transmission power allowed by their transceivers, wasting energy and decreasing nodes' lifetime. Thus, TPC techniques have been proposed to save energy and decrease interference on the medium.

A TPC technique calculates the minimum transmission power, $P_{TX_{min}}$, according to attenuations suffered by the transmitted signal [9]. Thus, in order to determine the amount of attenuation suffered by the signal, whenever an incoming frame arrives at the transceiver, nodes compare the value of the power used by the sender node to transmit the frame, called transmission power, with the power perceived at the

receiver node, called reception power. The transmission power value is added to the frame at the sender node, allowing that comparison. Aware of the signal attenuation, sender nodes adjust their transmission power in a way that the reception power will be the minimum required to correctly decode frames at receiver nodes.

In general, TPC techniques must satisfy the following requirements to calculate $P_{TX_{min}}$ [1]:

- The calculated transmission power must lie within the nominal limits of the transceiver. $P_{TX_{lower}}$ and $P_{TX_{upper}}$ are the lowest and the highest power of transceiver, respectively.
- Receiver nodes must consider the signal attenuation, also called *gain*, $G_{i \to j}$, being this value inferred by the transmission power P_{TX} and the reception power P_{RX}.
- The transmission power must balance the attenuation imposed by the medium, guaranteeing that received signal strength is higher than received sensitivity threshold of the radio RX_{thresh}.
- The minimum transmission power $P_{TX_{min}}$ must tolerate the thermal noise N_j observed in the medium and the attenuation $G_{i \to j}$ suffered by the signal. Further, the observed signal-to-noise plus interference ratio (SNIR) for the transmission must be higher than the minimum SNIR threshold $SNIR_{thresh}$.

Next, we present two TPC techniques, Attenuation and AEWMA (Atennuation with Exponentially Weighted Moving-Average), classified as unaware techniques. We also describe aware AEWMA's instances intending to be more adapted to MANET's dynamism and aware of channel state and link performance.

A. Unaware TPC techniques

1) Attenuation: It is a TPC technique initially developed to wireless sensor network [4]. In the attenuation technique, nodes periodically sample the signal strength when no transmissions occur to determine the thermal noise, N_j. Supposing that node i wishes to communicate with node j, it verifies in the table of neighbors if there is the value of the transmission power to j. If there is a value, i inserts it in the RTS and sends the frame using that power level; otherwise, it is transmitted in maximum transmission power. When node j receives RTS from i, it sends CTS frame using the same power level that i used to transmit RTS. This procedure is performed to mitigate asymmetric links and avoid collisions.

Hence, node i transmits data frame using the same power previously used to send RTS. When node j receives data frame, it determines the reception power P_{RX} and calculates the ideal transmission power $P_{TX_{ideal}}$ from node i to j using Eq. 1. Next, j inserts the calculated transmission power in the ACK frame and sends it using the same transmission power indicated in the data. Lastly, i receives ACK and stores the $P_{TX_{ideal}}$ in the table of neighbors. Node i will transmit subsequent frames to node j using this new power level.

$$P_{TX_{ideal}} = \max\left(\frac{RX_{thresh}}{G_{i \to j}}, \frac{SNIR_{thresh} \times N_j}{G_{i \to j}}\right) \quad (1)$$

Unfortunately, the Attenuation technique suffers of fluctuation on the calculated transmission power. Such drawback can increase the rate of dropped frames, caused by the variations on the input parameters, such as average noise, battery voltage and dynamic noise in environment [4].

2) AEWMA: Intending to solve issues on the Attenuation technique, signal filters were applied resulting in the AEWMA TPC technique. Filters are mathematical functions used to make output signals behave more smoothly, considering the past behavior of the signal and its current value in order to produce a more stable output signal. AEWMA uses a filter based on the EWMA (Exponentially Weighted Moving Average) and solves fluctuations on the calculation of transmission power. This filter has been chosen because of its low cost on calculations. AEWMA technique performs four-way handshake like Attenuation.

B. Aware AEWMA

AEWMA technique solves the fluctuation of the calculated transmission power of Attenuation. However, filter EWMA uses a static factor α that can decrease the performance of AEWMA due to the dynamism of MANETs. α can be calculated in accordance with network conditions in order to avoid this problem. Approaches that dynamically calculate the value of α in accordance with network conditions are called, in this work, dynamic AEWMA or aware AEWMA. Since links often experience attenuation of signal and also performance degradation, the dynamic AEWMA can be aware of channel state, link performance, or both of them. Hence, three instances are possible for aware AEWMA: CS-AEWMA (CS), LP-AEWMA (LP) and Hybrid-AEWMA (H).

CS-AEWMA considers the attenuation suffered by signal between sender and receiver nodes. This attenuation is calculated according transmission and reception power at the same frame. Thus, α is calculated by the *gain* in order to make AEWMA aware of variations on channel state.

LP-AEWMA uses virtual carrier sense rate *(VCSR)* and data rate *(DR)* to quantify the amount of frames received by the destination node and the performance degradation of the link. A node i starts the transmission sending a RTS frame to the receiver node j. Next, j transmits a CTS to i. In order to know the number of CTS frames arriving at node i, node j measures the $VCSR$ according to Eq. 2. $SC_{j \to i}$ is *the number of CTS frames sent by j to i*, whereas $LC_{j \to i}$ is *the number of CTS frames sent by j to i, but that were lost*. When CTS doesn't achieve i, it will retransmit a RTS setting the flag *retry* to 1. Hence, j will know that the previous CTS was lost.

$$VCSR_{i \to j} = \frac{SC_{j \to i} - LC_{j \to i}}{SC_{j \to i}} \quad (2)$$

Upon receiving CTS, node i sends the data frame to node j and, thus, j transmits ACK to i. Hence, node j calculates DR

according to Eq. 3, in which $SA_{j\rightarrow i}$ is the number of ACKs sent by j to i, whereas $LA_{j\rightarrow i}$ is the number of ACK sent by j to i, but lost. When ACK doesn't reach i, j retransmits the data frame setting the flag *retry* to 1.

$$DR_{i\rightarrow j} = \frac{SA_{j\rightarrow i} - LA_{j\rightarrow i}}{LA_{j\rightarrow i}} \quad (3)$$

Hence, α is calculated following Eq. 4.

$$\alpha = \frac{VCSR_{i\rightarrow j} + DR_{i\rightarrow j}}{2} \quad (4)$$

H-AEWMA combines both information, CS and LP, to calculate a new value for α. It aims at making AEWMA aware of the variations suffered by the channel state and the performance degradation of the link. Hence, a hybrid approach satisfies adaptability and dynamism required for MANETs. Receiver node j can calculate the new value of α following Eq. 5.

$$\alpha = \frac{VCSR_{i\rightarrow j} + DR_{i\rightarrow j} + G_{i\rightarrow j}}{3} \quad (5)$$

III. Reduction of Quality (RoQ) Attack Model

This section describes RoQ attack models. These attacks are performed by malicious nodes (attackers) that take advantage of the dynamic medium virtual reserve. Attackers create a disorder in the network making the medium virtual reserve in an arbitrary manner. To avoid detection, they randomly choose the power levels for sending frames. A RoQ attacker sends control frames RTS/CTS using lower level of transmission power. Next, it sends data and ACK frames considering a higher level of transmission power. An attacker always chooses a higher level of the transmission power for sending data and ACK frames in order to create asymmetric links [10].

Thus, all neighboring nodes receive data frames, even if they have not received control frames. In this case, if other transmissions are occurring, there is high probability of collision in the receiver node because of attacker's frames. In this paper, RoQ attacks present three variations, *round-robin*, *flooding* and *self-whisper*. These attacks create asymmetric links and have as target a specific network traffic.

On **round-robin attack**, an attacker node, neighbor of a specific traffic, chooses randomly a victim node that is not participating of the traffic. In order to create collision in receiver nodes of the traffic, attackers make virtual carrier sense using different power levels.

On **flooding attack**, an attacker node chooses randomly a victim node that can be the source or the destination of a data traffic between two no attacker nodes. Attacker nodes make virtual carrier sense in a arbitrary manner by sending a RTS frame using a lower transmission power. After receiving a CTS, the attacker node sends data frames to the victim node.

On **self-whisper attack**, multiple attacker nodes, neighbors of a specific traffic, establish communication among them to create a malicious traffic in the network. When the medium is arbitrarily reserved with lower transmission power, two attacker nodes send data and ACK frames with higher transmission power in order to damage traffic between no attacker nodes.

IV. Evaluation and Results

The impact of RoQ attacks on IEEE 802.11 using unaware and aware TPC techniques is evaluated using the Network Simulator (NS) version 2.31. A physical and MAC layers model, called dei80211mr [11], is employed to provide more realistic simulations. It models the packet error and verifies if a frame is received correctly calculating SNIR *(Signal-to-Noise plus Interference Ratio)*, defined by RSSI *(Received Signal Strength Indication)*, noise and interference generated by other nodes. The interference is calculated according to a Gaussian model that checks transmissions arriving at receivers.

We simulate a MANET with 50 nodes randomly scattered in an area of 500 x 500 meters. Nodes use IEEE 802.11b radios that possess a Cisco Aironet 1250 interface with a radio providing nine different power levels, being 0.0007 W the minimum, and 0.2 W the maximum power transmission.

An UDP-based victim flow simulates voice or video traffic at a rate of $0.3Mbps$. They follow an exponential distribution with a burst time and idle time of $0.01ms$ and $0.04ms$, respectively, starting in $2\ s$ and stopping in $250\ s$ of simulation. Attacking flows, also UDP based, occur in the neighborhood of victim flow and follow a exponential distribution with a burst time chosen randomly between $0.05ms$ and $0.15ms$, and an idle time of $0.004ms$. Attacking flows start in $5\ s$ and stops in $200s$ of simulation, having a rate of $1.0Mbps$. The impact of RoQ attacks, *flooding* (**F**), *round-robin* (**RR**) and *self-whisper* (**SW**), is analyzed under 10%, 30% and 50% of attacker nodes, respectively. Each scenario is executed 35 times, using different seeds for the random number generator. Results are presented with a 95% confidence interval.

We investigate the impact of RoQ attacks under AEWMA and aware TPC techniques. Four performance metrics are used: the average of number of **COLlisions** (**COL**) occurred in the source and destination nodes; **Packet Delivery Ratio** (**PDR**) - it is the rate of packets sent by the source node and received by the destination node; **Average Transmission Power** (**ATP**) - it is the average of transmission power used to send frames by end nodes of victim flows.

A. Aware approaches

Figure 1 shows the number of frames that suffered collisions on AEWMA and aware approaches. With no attacker nodes in the network, all approaches yielded COL close to zero, and, hence, these results are not presented. Under 10% of attacker nodes, Flooding attack resulted in 4871, 6632, 10707 and 11637 of collided frames on AEWMA, CS, LP and H. RR attack produced 12061, 6965, 10707 and 12858 of collisions on AEWMA, CS, LP and H. SW attack caused 14506, 8680, 14210 and 13781 of collided frames on AEWMA, CS, LP and H. Under 30% of attacker nodes, F attack generated 19145, 27602, 18492 and 20528 collisions on AEWMA, CS, LP and

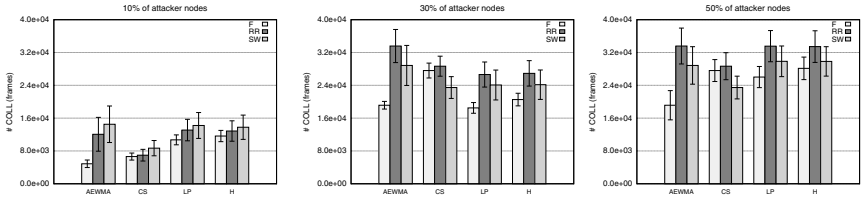

Fig. 1. Comparing collisions generated by RoQ attacks over AEWMA and aware TPC techniques

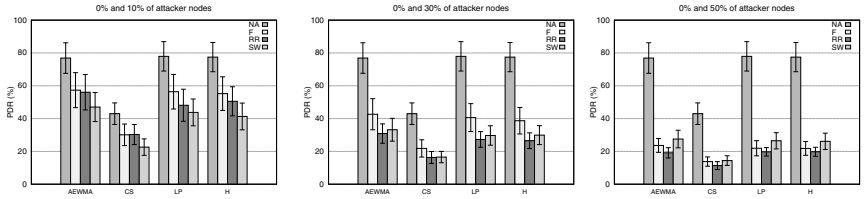

Fig. 2. Examining PDR resulted from AEWMA and aware TPC techniques under RoQ attacks

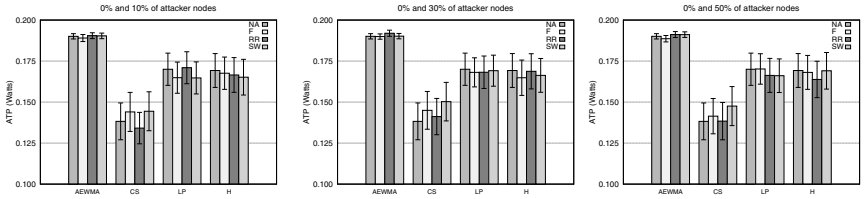

Fig. 3. Analyzing ATP resulted from AEWMA and aware TPC techniques under RoQ attacks

H. RR attackers produced 33580, 28661, 26631 and 26917 of collided frames on AEWMA, CS, LP and H. SW attack resulted in 28849, 23460, 24078 and 24152 collisions on AEWMA, CS, LP and H.

Figure 2 presents the PDR yielded by aware approaches in comparison with AEWMA. Without attacker nodes, AEWMA yielded a PDR of 76.9%, while CS, LP and H, obtained 43%, 77.9% and 77.5%. Under 10% of attacker nodes, the difference of the PDR resulted by aware approaches under F attack ranged around 1% (LP). Under RR attack, the difference ranged around 3% (LP). On 30% of F attacker nodes, AEWMA yielded a PDR of 42.7%, while CS resulted in 21.8%. Under RR attack, AEWMA, CS, LP and H yielded, respectively, 30.9%, 16.3%, 27.3% and 26.5%. Under SW attack, AEWMA yielded a PDR of 33.2%, while CS resulted in 16.5% and H produced 29.9%.

Figure 3 compares the ATP used by AEWMA and aware approaches. AEWMA consumed an ATP of 0.190 W to send one frame. CS consumed 0.138 W, while LP and H consumed 0.170 W. Exposing the network to 10% of attacker nodes, LP consumed 0.171 W under RR attack. Under 30% of attacker nodes, H consumed 0.164 W under F attack, H consumed 0.169 W under RR attack, and LP consumed 0.169 W under SW attack. Under 50% of attacker nodes, H consumed 0.168 and 0.169 W under F and SW attack, and LP consumed 0.166 W under RR attackers.

Discussion - The presence of RoQ attacks has resulted in a significant amount of collisions. We observed that for aware approaches, as LP and H, the amount of collisions was higher than for aware approaches that consider few aspects for transmission power control, as CS. As expected, higher the percentage of attacks on the network, higher is the number of collisions. Under lower percentage of attackers, SW attack is the most powerful, whereas under higher percentage of attackers, the RR attack is the most powerful. Further, LP and H under attacks presented almost the same number of collisions resulted by AEWMA. RoQ attacks affect PDR. Higher is the percentage of attacker nodes, lower is the PDR produced by AEWMA, CS, LP and H. In terms of percentage, aware techniques, as LP and H, have been the most affected by RoQ attacks. In general, the ATP has not been influenced by RoQ attacks, remaining with values similar than those found without attacks on the network.

V. Conclusion

This work quantified the impact of three types of Reduction of Quality (RoQ) attacks on MANETs. Analyses considered RoQ attacks on a modified 802.11 using unaware and aware transmission power control (TPC) techniques. Aware TPC are more dynamic and take into account the performance and network conditions to determine transmission power. Results showed that RoQ attacks, mainly round-robin and self-whisper, affect considerably MANET's performance. Further, those attacks have been more powerful over aware TPC techniques that consider many aspects to define transmission power used by nodes. Since round-robin attacks are more powerful under high percentage of attacker nodes, whereas self-whisper attacks are more effective under low percentage of attacker nodes.

REFERENCES

[1] J. P. Monks, V. Bharghavan, and W. mei W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *IEEE INFOCOM*, 2001, pp. 219–228.

[2] I. Akyildiz, L. Won-Yeol, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, 2008.

[3] H. Singh and S. Singh, "Smart-802.11b MAC protocol for use with smart antennas," in *IEEE ICC*, 2004, pp. 3684–3688.

[4] L. H. A. Correia, D. F. Macedo, D. A. C. Silva, A. L. dos Santos, A. A. Loureiro, and J. M. Nogueira, "Transmission power control in MAC protocols for wireless sensor networks," in *ACM MSWiM*, 2005, pp. 282–289.

[5] W. Ren, D. yan Yeung, H. Jin, and M. Yang, "Pulsing RoQ DDoS attack and defense scheme in mobile ad hoc networks," *International Journal of Network Security*, vol. 4, no. 2, pp. 227–234, 2007.

[6] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," in *IEEE INFOCOM*, 2005, pp. 1362–1372.

[7] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the transients of adaptation for RoQ attacks on internet resources," in *IEEE ICNP*, 2004, pp. 184–195.

[8] X. Luo, E. W. W. Chan, and R. K. C. Chang, "Vanguard: A New Detection Scheme for a Class of TCP-targeted Denial-of-Service Attacks," in *Network Operations and Management Symposium (NOMS 2006)*, 2006, pp. 507–518.

[9] L. H. A. Correia, D. F. Macedo, A. L. D. Santos, A. A. F. Loureiro, and J. M. S. Nogueira, "Transmission power control techniques for wireless sensor networks," *Computer Networks*, vol. 51, pp. 4765–4779, 2007.

[10] V. P. Mhatre, K. Papagiannaki, and F. Baccelli, "Interference mitigation through power control in high density 802.11 WLANs," in *IEEE INFOCOM*, 2007, pp. 535–543.

[11] N. Baldo, F. Maguolo, M. Miozzo, M. Rossi, and M. Zorzi, "ns2-MIRACLE: a modular framework for multi-technology and cross-layer support in network simulator 2," in *ICST ValueTools*, 2007.