Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

DENIAL OF SERVICE RESISTANT MAC FOR WIRELESS MESH NETWORKS

BOTEZATU, N[icolae] A[lexandru] & STAN, A[ndrei]

Abstract: *The wide use of IEEE 802.11 wireless networks enables most of everyday ubiquitous Internet access. One drawback of such networks is the vulnerability to Denial-of-Service attacks. Due to the use of an unsecure communication medium, the disruption of communication services can be achieved even with standard off-the-shelf equipment. In this paper we present an adaptive power control method applied to the IEEE 802.11 MAC and we show by simulation its superior resistance to DoS attacks compared to the standard MAC.*

Key words: *IEEE 802.11 MAC, denial of service, power control, wireless security*

1. INTRODUCTION

The most commonly used MAC protocol for wireless networks is based on the IEEE 802.11 standard. Unfortunately, it cannot cope with the general vulnerability of wireless networks: due to a shared communication environment, data transmission is subjected to radio interference. Because most wireless technologies use the ISM frequency bands, in environments where the device density is high, the availability of such networks becomes a problem.

More, wireless networks are prone to Denial-of-Service attacks because of the broadcast nature of the communications and because they can be conducted with the use of commercial equipment (Bicakci & Tavli, 2009). Many 802.11 DoS vulnerabilities were experimentally demonstrated in recent years. These vulnerabilities are aimed either at the physical layer (RUA attacks, preamble attacks, reactive attacks, HR attacks) or at the MAC layer (deauthentication attacks, duration inflation attacks, request floods) (Xu et al., 2006). Several solutions were proposed in order to prevent DoS attacks (Gummadi et al., 2007), with varying effectiveness, but with a constant characteristic: an increased implementation complexity.

Our work regarding wireless mesh networks and the 802.11 MAC was aimed at implementing a transmission power control mechanism with the following objectives: decrease the power consumption of communicating nodes; and increase the network capacity by spatial reuse (Botezatu & Dhaou, 2011). Further, we wanted to study the effectiveness of our modified MAC against some classes of DoS attacks. This paper presents these results compared side by side with the ones obtained for the standard 802.11 MAC.

2. CCPC-MAC PROTOCOL

One of the simplest solutions that address the power control problem, by modifying the IEEE 802.11, is named Max-Min protocol (Chen et al., 2006). It uses RTS and CTS packets transmitted at the highest possible power level and DATA and ACK packets transmitted at the minimum power level necessary to reach their destinations. The RTS-CTS handshake is used to decide the transmission power for subsequent DATA and ACK packets based on (1).

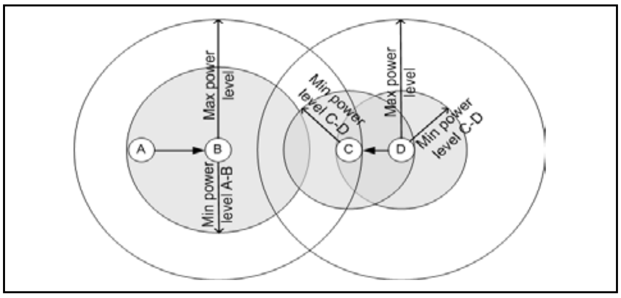

Fig. 1. Sample transmit power adaptation

$$PT_{DATA/ACK} = \frac{PT_{RTS}}{PR_{CTS}} \cdot Rx_{Th} \qquad (1)$$

Where PT is the transmission power level, PR is the reception power level and Rx_{Th}, the reception range threshold, is the minimum necessary signal strength to correctly receive a data packet. When a destination node receives an RTS, it responds by sending a CTS, also at the maximum power level. When the node that started the handshake receives the CTS, it calculates the needed power level $PT_{DATA/ACK}$ based on the received power level PR_{CTS} and on the transmitted power level PT_{RTS}.

Our solution is based on the Min-Max idea of power control. The RTS packets are sent with the highest transmit power available. For the CTS ones, we take into account other concurrent transmissions, while the DATA and ACK packets are sent with the lowest possible power level. In order to address the problem introduced by the extra collisions, the data transmission sessions are started selectively, based on two factors: the distance between the transmitter and the receiver; and information about the neighboring nodes that may interfere with the transmission. This raises the need to evaluate the effectiveness of the RTS-CTS handshake, in order to see how the reception is affected by the nodes in the *IR* (i.e. interference range - nodes that can corrupt data reception even if they are farther away than the transmitter).

In order to describe how our *CTS conservative power control protocol* (CcPc-MAC) addressed the interference problem, we start from an example situation (Fig. 1). When nodes A and B perform the RTS-CTS handshake, node C logs the information regarding the two nodes: the distance between them, the power levels used and the duration of the operation. Next, we presume that the power level needed for the transmission of the DATA and ACK packets is low enough, for node C only to sense the carrier. If node D wants to start a transmission to node C, after node C receives the RTS, it determines if it can transmit a CTS packet with a power level that does not interfere with the A-B transmission. Of course, the power level must be high enough to reach D. If none of the available power levels are suited, node C discards the RTS request and does not send a CTS. As with the IEEE 802.11 standard, if node D does not receive the CTS in a time window, it tries to send the RTS for a number of times. If the A-B transmission finishes, node C responds to the request, otherwise the node D drops the data packet.

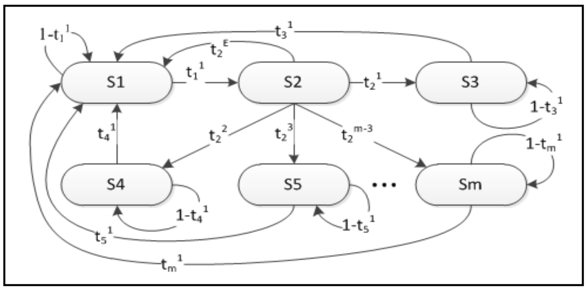

Fig. 2. Markov model for the CcPc-MAC

3. DOS ATTACK MODEL

In order to study how our mechanism reacts to DoS attacks, we constructed a simulation model based on a Markov chain. Its purpose is to determine the effectiveness of our proposed MAC against the following types of physical DoS attacks: constant jamming (i.e. the attacker constantly emits a radio signal that disrupts neighboring communication), random jamming (i.e. the attacker alternates between jamming and sleeping based on a pattern or in a random manner). Each simulation is configured by the following tuple <n_p, p_v, r_A, r_h>. n_p represents the number of power levels used by the adaptive mechanism and p_v is the power level array. The power levels are named p_1, p_2, …, p_n, where p_1 is the minimum transmission power level and p_n is the maximum transmission power level. r_A is the activation rate for the attacker (i.e. a value of 1 stands for a continous activation, the constant jamming attack) and r_h is the refresh rate for the history (i.e. the time taken for a history entry to clear). In order to express the latter two parameters we expressed the time base as *communication rounds*. A communication round stands for the time needed to execute a standard 802.11 data transfer session (RTS-CTS DATA-ACK) considering a constant data payload.

The Markov model is presented in Fig. 2. The number of states and transitions are dependent on the number of power levels used and are equal to n_p+2 states and 3n_p+3 transitions.

The model contains the following four types of states:

1) S1 – the transmitter (T) and the receiver (R) communicate with p_1. The system stays in this state when the attacker (A) is in *ER* (i.e. exclusion range – the attacker cannont affect the communication) or when the attacker is in *IR* and is not active.

2) S2 – the attacker is active. If R is receiving data, a collision occurs; and if R is passive (listening mode), it logs the neighbor information and takes the interference into account when negotiating a data session.

3) S3 – R declines all data sessions due to neighboring nodes that transmit (i.e. attackers) and because it cannot reduce the interference level even when communicating with p_n. The receiver remains in this state while the neighboring nodes information remains in the running history.

4) S4-Sm – these n_p-1 states correspond to the use of p_2 – p_n power levels, in order to reduce *IR* (i.e. excluding the attacker). The system remains in this state until A stops transmitting and its information is cleared from history.

The transition types are described below:

- t_1^1 – activation rate of the attacker. (r_A parameter).
- t_2^1 – the probability that p_1 cannot prevent collisions at the receiver.
- t_2^E – the probability that the interfering node is in *ER*.
- t_2^2-t_2^{m-3} – the probability that the power level corresponding to every destination state is sufficient for the exclusion of the attacker from *IR* (i.e. the interference level is small enough not to corrupt the data at the receiver).
- t_3^1-t_m^1 – history refresh rate (r_h parameter).

All simulation runs start from S1 state. The communicating nodes are considered to be jammed when data collisions occur (S2 state) or when data sessions are declined due to the conservative CTS reply (S3 state).

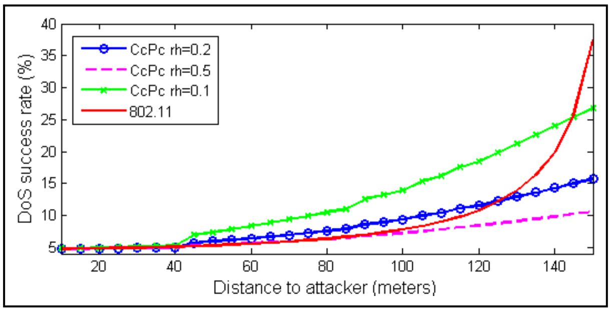

Fig. 3. Simulation results for random jamming attack

4. SIMULATION RESULTS

Simulations were run for the *CcPc-MAC* protocol, as well as for the standard 802.11 MAC. For the latter case, the Markov model was simplified by considering only one transmision power level (210 mW) and by removing the t_2^1 transition. For the proposed protocol, the simulation setup included 12 power level evenly distributed between 1 and 210 mW. We varied the history refresh rate as well as the distance between the attacker and the communicating pair (Fig. 3). For the random jamming simulations the activation rate for the attacker had a uniform distribution with a mean value of 0.5. The results show that when the history refresh rate is high (r_h=0.5), *CcPc-MAC* outperforms the standard 802.11 one over the entire distance range. For the other two refresh rate considered, the DoS success rate is equivalent to the one for 802.11 for distances smaller than 40 meters and is lower for distances above 125 meters and 144 meters respectively. For the continous jamming attacks, *CcPc-MAC* obtained a success rate for DoS attacks 7.6% smaller than the one for 802.11 MAC.

5. CONCLUSION

In this paper we studied the effect of DoS attacks on the *CcPc-MAC* mechanism. We showed by simulation that our solution outperforms the 802.11 MAC in the case of continous jamming. More, the performance in the case of random jamming varies with the history refresh rate. Future research includes the development of an experimental setup to verify the simulation results. We want to see how CcPc-MAC reacts to jamming in 802.11 based sensor networks and how the availability issue is related to the energy consumption metric.

6. REFERENCES

Bicakci, K. & Tavli, B. (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, *Computer Standards & Interfaces*, Vol. 31, No. 5, Sept 2009, pp. 931-941, ISSN 0920-5489

Botezatu, N. & Dhaou, R. (2011). Adaptive Power Control in 802.11 Wireless Mesh Networks, *Proceedings of the 2011 International Conference of Wireless Networks*, July 2011, London, UK, ISBN 978-988-18210-6-5

Chen, H.-H.; Fan, Z. & Li, J. (2006). Autonomous Power Control MAC for Mobile Ad Hoc Networks, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2006, No. 2, Apr 2006, pp. 1-10, ISSN 1687-1499

Gummadi, R.; Wetherall, D. & Seshan S. (2007). Understanding and Mitigating the Impact of RF Interference in 802.11 Networks, *Proceedings of the ACM SIGCOMM*, Aug 2007, Japan, ISBN 978-1-59593-713-1

Xu, W.; Ma, K. & Zhang, Y. (2006). Jamming Sensor Networks: Attack and Defense Strategies, *IEEE Network*, Vol. 20, No. 3, May/June 2006, pp. 41-47, ISSN 0890-8044