Impact of Optimal MAC Layer Attacks on the Network Layer*

Svetlana Radosavac, John S. Baras
Department of Electrical and Computer Engineering
and The Institute for Systems Research
College Park, MD 20742
{svetlana,baras}@isr.umd.edu

George V. Moustakides
Department of Computer and Communications Engineering
University of Thessaly
Volos, Greece
moustaki@uth.gr

ABSTRACT

Node misbehavior in wireless ad hoc networks leads to sudden unpredictable changes in network topology, resulting in fluctuation of traffic load and capacity for already existing links. In this work we consider node misbehavior in the Medium Access Control (MAC) layer and its effects on the performance of the network layer. In order to capture uncertainty of the attacker's strategy as well as the unpredictable nature of the wireless medium, we quantify the optimal attack strategy by using the principle of minimum cross-entropy. Following that, we apply the obtained results for analysis of the IEEE 802.11 DCF MAC protocol and investigate the effects of such optimal attacks on the network layer. Finally, we evaluate the robustness of two different routing protocols against the worst-case MAC layer attacks and justify the need for the MAC layer-based Intrusion Detection Sytems (IDS).

Categories and Subject Descriptors

C.2.0 [**Computers-Communication Networks**]: General—*Security and Protection*

General Terms

Design, Security, Algorithms

Keywords

Ad hoc networks, MAC layer, minmax robust detection, protocol misbehavior, cross-layer

1. INTRODUCTION

The problem of deviation from legitimate protocol operation in wireless networks and efficient detection of such behavior has become a significant issue in the research community in recent years. Information has become a resource of strategic importance and wireless networks are the primary means for ensuring availability, offering access to and enabling transfer of data. The strategic significance of timely dissemination of information in the network offers incentives for malicious entities to launch attacks against critical operations and network functionality. In this work we address the impact of MAC layer attacks that aim at disrupting critical network functionalities and information flow in wireless networks and we quantify the impact of such attacks, placing emphasis on proactive actions against attacks aimed against wireless networks. Following that, we analyze the effects of such attacks on the network layer, showing their multi-layer nature.

The first issue addressed in this work is that of appropriately modeling misbehavior by identifying the objectives of the intruder, its benefits and the means that it has in its disposal for launching the attack. An additional issue is that of quantifying the degree of sophistication of the attack that includes: (i) the level of knowledge of the attacker; (ii) the set of controllable protocol parameters; (iii) the intelligence of the attacker in terms of adjusting its policy so as to avoid detection. This work assumes the existence of an *intelligent* attacker, i.e. an attacker that has a complete knowledge about the network structure and the employed IDS. In order to quantify the effects of misbehavior on the network, uncertainty of both the attacker and the wireless protocol (such as IEEE 802.11 DCF [3]) the attack is being launched against need to be taken into account. The modeling philosophy pursued in this work is optimization with respect to *worst-case* performance over uncertainty conditions. Another modeling aspect calls for expressing intruder gain as a function of the intrusion policies. Towards this goal, we define parameters that are controllable by the attacker and depend on its capabilities and constraints imposed by the IDS. We improve the framework introduced in [8] by introducing the notion of *cross-entropy*, proving that *all* optimal attacks are of exponential nature. The results are then applied for analysis of the worst-case attack in the presence of one attacker and multiple misbehaving nodes in the IEEE 802.11 DCF MAC protocol. In order to quantify the effects of such optimal attacks we measure the performance loss of the system in terms of delayed detection and percentage of channel access of the misbehaving node, under the assumption that the quickest detection-based IDS is employed.

The different layers in the network stack communicate with each other, enabling the propagation of misbehavior instances between layers. Thus, misbehavior that takes place at the MAC layer can significantly affect the routing process as well. The selfish behavior of some nodes can hinder channel access for the rest, disabling these nodes from taking part in the routing process and decreas-

*Research supported in part by the U.S. Army Research Office under CIP URI grant No DAAD19-01-1-0494

SASN'06, October 30, 2006, Alexandria, Virginia, USA.

ing end-to-end performance. We investigate the effects of optimal MAC layer attacks on routing protocols and demonstrate their cross-layer nature. We show by analysis and simulation that cross-layer propagation gives rise to new threats, such as false accusation of legitimate nodes by the IDS located in the network layer. Additionally, the distributed nature of the wireless ad hoc networks as well as the randomness of the employed protocols, makes the task of detection and localization of malicious participants extremely challenging.

Our work adds to the analysis of cross-layer effects presented in [1] by addressing the effects of an *optimal* MAC layer attack on the network layer. We show by analysis and simulation that MAC layer attacks presented in [1] can be almost instantly detected in the MAC layer by observing the backoff sequence of the sender [8]. Consequently, quickest detection of such attacks minimizes their effects on the network layer and prevents further propagation throughout the network.

Our work contributes to the current literature by: (i) generalizing the derivation of the worst-case attack in the MAC layer by using the approach of minimum cross-entropy; (ii) analyzing the effect of vertical attack propagation and (iii) implementing the optimal MAC layer-based IDS from [8] and showing its efficiency against vertical propagation of attacks.

The paper is organized as follows. Sect. 3.1 outlines the details of the IEEE 802.11 DCF protocol and analyzes possible misbehavior scenarios. Sect. 3.3 introduces the notion of minimum cross-entropy, which is then applied for derivation of the worst-case attack strategy in Sect. 3.4. Sect. 4.1 evaluates the performance of the network layer under different traffic patterns. The impact of the optimal MAC layer attacks on the MAC layer itself is analyzed in Sect. 5.1. Following that, the impact of such attacks on two routing protocols with no MAC layer-based IDS is evaluated in Sect. 5.2. The effects of such IDS on the performance of routing protocols are evaluated in Sect. 5.3. Finally, Sect. 6 concludes our study.

In subsequent sections, the terms "misbehavior" and "attack", "misbehaving node", "attacker" and "adversary" will be used interchangeably with the same meaning.

2. RELATED WORK

Various IDS techniques, mostly based on misuse and anomaly detection principles, have been proposed for attack detection and prevention. Most of the existing intrusion detection approaches focus on attack detection and response at a particular layer of the protocol stack, mostly the network layer. The effects of the various attacks launched in one layer on the performance of another layer have not been widely investigated. The authors in [5] presented a cautionary perspective on cross-layer design. They emphasized the importance of the approach and discussed the architectural problems that cross-layer design, if done without care, can create. In the more recent work [12], the authors define the notion of cross-layer design and state three main reasons for using it in the wireless environment: the unique problems created by the wireless links, the possibility of opportunistic communication on wireless links and the new modalities of communication offered by the wireless medium. In addition to that they classify cross-layer design proposals and present proposals for implementing cross-layer interactions. The field of intrusion detection has not appropriately addressed the importance of cross-layer design and its benefits in attack detection and prevention. In [13] the authors use a cross-layer based IDS system to analyze the anomalies in the network. They introduce the concept of integrating multiple layers of the protocol stack for more efficient intrusion detection. In [1] the authors study the interaction of the routing and MAC layer protocols under different mobility parameters. They simulate interaction between three MAC protocols (MACA, 802.11 and CSMA) and three routing protocols (AODV, DSR and LAR scheme) and perform statistical analysis in order to characterize the interaction between layers in terms of latency, throughput, number of packets received and long term fairness. To our knowledge, the current literature does not address the effects of optimal MAC layer attacks on the upper layers.

3. OPTIMAL DETECTION PROCEDURES FOR THE MAC LAYER ATTACKS

In [8] the problem of quickest detection of an optimal attacker was considered and the performance was evaluated based on the average detection delay. A specific class of exponential functions was found to represent the worst case attack scenario. In this work we present the first step towards building a general procedure for constructing an optimal attack scenario in the MAC layer under general set of constraints that can be adapted based on specific settings of a given IDS. To achieve this, we use the principle of minimum cross-entropy [11] which represents a general method of inference about an unknown probability density when new information in the form of constraints on expected values is given. More specifically, we use the fact that given a continuous prior density and new constraints, there exists only one posterior density satisfying these constraints and can be obtained by minimizing cross-entropy [10]. Using the above facts, we prove that the general expression for the worst-case optimal attack in the IEEE 802.11 MAC is of exponential nature.

3.1 IEEE 802.11 MAC Misbehavior

In the distributed coordinating function (DCF) of the IEEE 802.11 MAC protocol, coordination of channel access for contending nodes is achieved with carrier sense multiple access with collision avoidance (CSMA/CA) [3]. A node with a packet to transmit selects a random back-off value b uniformly from the set $\{0,1,\ldots,W-1\}$, where W is the (fixed) size of the contention window. The back-off counter decreases by one at each time slot that is sensed to be idle and the node transmits after b idle slots. In case the channel is perceived to be busy in one slot, the back-off counter is stopped. After the back-off counter is decreased to zero, the transmitter can reserve the channel for the duration of data transfer. First, it sends a request-to-send (RTS) packet to the receiver, which responds with a clear-to-send (CTS) packet, reserving the channel for the transmission. Both RTS and CTS messages contain the intended duration of data transmission in the duration field. Other hosts overhearing either the RTS or the CTS are required to adjust their network allocation vector (NAV) that indicates the duration for which they will defer transmission. This duration includes the SIFS intervals, data packets and acknowledgment frame following the transmitted data frame. An unsuccessful transmission instance due to collision or interference is denoted by lack of CTS or ACK for the data sent and causes the value of contention window to double. If the transmission is successful, the host resets its contention window to the minimum value W.

IEEE 802.11 DCF favors the node that selects the smallest back-off value among a set of contending nodes. Therefore, a malicious or selfish node may choose not to comply to protocol rules by selecting small back-off intervals, thereby gaining significant advantage in channel sharing over honest nodes. Moreover, due to the exponential increase of the contention window after each unsuccessful transmission, non-malicious nodes are forced to select their future back-offs from larger intervals after every access failure. Therefore their chance of accessing the channel becomes even

smaller. Apart from intentional selection of small back-off values, a node can deviate from the MAC protocol in other ways as well: (i) he can choose a smaller size of contention window; (ii) he may wait for shorter interval than DIFS; (iii) reserve the channel for larger interval than the maximum allowed network allocation vector (NAV) duration. In this work, we will adhere to protocol deviations that occur due to manipulation of the back-off value.

The nodes that are instructed by the protocol to defer transmission are able to overhear transmissions from nodes whose transmission range they reside in. Therefore, silenced nodes can observe the behavior of transmitting nodes and measure their backoffs [8]. The question that arises is whether there exists a way to take advantage of this observation capability and use it to identify potential misbehavior instances. If observations indicate a misbehavior event, the observer nodes should notify the rest of the network about the situation or launch a response action in order to isolate the misbehaving nodes. Detecting misbehavior is not straightforward even in the simplest case, namely that of unobstructed observations. The difficulty stems primarily from the non-deterministic nature of the access protocol that does not lead to a straightforward way of distinguishing between a legitimate sender, that happens to select small back-offs, and a misbehaving node that maliciously selects small back-offs. The open wireless medium and the different perceived channel conditions at different locations add to the difficulty of the problem. Additional challenges arise in the presence of interference due to ongoing concurrent transmissions. We now present the derivation of the worst-case attack strategy of an intelligent adaptive attacker in the absence of interference under the general set of constraints.

3.2 Adversary model

Throughout this work we assume existence of an intelligent adaptive attacker that is aware of the environment and its changes over a given period of time. Consequently, the attacker is able to adjust its access strategy depending on the level of congestion in its environment. Namely, we assume that, in order to minimize the probability of detection, the attacker chooses legitimate over selfish behavior when the level of congestion in the network is low. Similarly, the attacker chooses adaptive selfish strategy in congested environments. Due to the previously mentioned reasons, we assume a benchmark scenario where all the participants are backlogged, i.e., have packets to send at any given time in both theoretical and experimental evaluations. We assume that the attacker will employ the worst-case misbehavior strategy in this setting, and consequently the detection system can estimate the maximal detection delay. It is important to mention that this setting represents the worst-case scenario with regard to the number of false alarms per unit of time due to the fact that the detection system is forced to make maximum number of decisions per time unit.

3.2.1 Capabilities of the Adversary

We assume the adversary generates its backoff values according to a non-uniform probability distribution function (pdf) $f_1(x)$ over which he has full control. Consequently, we can assume the adversary has full control over the backoff values generated by the given pdf. In addition to that, we assume that the adversary is intelligent, i.e. he knows everything the detection agent knows and can infer the same conclusions as the detection agent.

3.2.2 Goal of the adversary

We assume the objective of the adversary is to design an access policy with the resulting probability of channel access P_1, while minimizing the probability of detection. As it has already been mentioned, the optimal access policy results in generation of back-off sequences according to the pdf $f_1^*(x)$.

3.2.3 Evaluation of adversary capabilities

We introduce the *misbehavior coefficient* ε for more efficient evaluation of the performance of the adversary. Misbehavior coefficient represents additional gain the attacker enjoys as a result of the optimal attack strategy. The values of ε are scaled to the $[0,1]$ interval, where $\varepsilon = 0$ represents legitimate behavior and $\varepsilon = 1$ represents the Denial of Service (DoS) Attack. Due to the fact that the adversary is intelligent, we assume it never attempts to use the strategy with $\varepsilon = 1$.

3.3 Derivation of the worst-case attack using the principle of minimum cross-entropy

The principle of minimum cross-entropy [11] provides a general method of inference about an unknown probability density q when there exists a prior estimate and new information about q in the form of constraints on expected values. The principle states that, of all densities that satisfy the constraints, one should choose the *posterior* q with the least cross-entropy

$$H[q,p] = \int q(x)\log(q(x)/p(x))dx,$$

where p is a *prior* estimate of q. Furthermore, in [10], the authors show that the principle of minimal cross-entropy is the uniquely correct method for inductive inference when new information is given in the form of expected values. More specifically, given information in the form of constraints on expected values, there is only one distribution satisfying the constraints that can be chosen by a procedure that satisfies the consistency axioms.

It is now easy to connect the principle of minimum cross-entropy with the worst-case attack strategy. The attacker is aware of his limitations with respect to the given IDS and will attempt to deviate from the original pdf in such way that he conforms to already known constraints of the system and at the same time will attempt to express maximum uncertainty with respect to all other system parameters that are unaffected with the given constraints. In other words, we assume that the attacker can be in any one of a given set of states that conform to the constraints on the mean and makes the final decision about the misbehavior strategy in a way that maximizes its deviation from the original, "fair", uniform pdf.

If $f_k(x)$ and $\bar{f}_k$, $k = 1,\ldots,m$ represent the known set of constraint functions and constraints on the mean respectively, then the cross-entropy method can be outlined as follows. Given a positive prior density p and new information that takes form of a finite set of constraints:

$$\int q(x)dx = 1, \tag{1}$$

$$\int f_k(x)q(x)dx = \bar{f}_k,\ k = 1,\ldots,m \tag{2}$$

we wish to find a density q that minimizes

$$H(q,p) = \int q(x)\log\frac{q(x)}{p(x)}dx \tag{3}$$

subject to the given set of constraints (1) and (2). By introducing Lagrangian multipliers β and λ_k ($k = 1,\ldots,m$) corresponding to the constraints, the following expression for the Lagrangian is obtained:

$$L(q,\beta,\lambda_k,k=1,\ldots,m) = \int q(x)\log\frac{q(x)}{p(x)}dx + \beta\int q(x)dx + \sum_{k=1}^{m}\lambda_k\int f_k(x)q(x)dx,$$

Differentiating the above expression with respect to q and equating it to zero leads to:

$$q(x) = p(x)exp\left(-\lambda_0 - \sum_{k=1}^{m}\lambda_k f_k(x)\right) \quad (4)$$

with $\lambda_0 = \beta + 1$. The cross-entropy at the minimum can be expressed in terms of the λ_k and f_k as

$$H(q,p) = -\lambda_0 - \sum_{k=1}^{m}\lambda_k\bar{f}_k \quad (5)$$

It is necessary to choose λ_0 and λ_k so that all the constraints are satisfied. In the presence of the constraint (1) we can rewrite the remaining constraints in the form

$$\int (f_k(x) - \bar{f}_k)q(x)dx = 0 \quad (6)$$

If we find values for the λ_k such that

$$\int (f_i(x) - \bar{f}_i)p(x)exp(-\sum_{k=1}^{m}\lambda_k f_k(x))dx = 0 \quad (7)$$

the constraint (6) is satisfied and (1) is satisfied by setting

$$\lambda_0 = \log\int p(x)exp\left(-\sum_{k=1}^{m}\lambda_k f_k(x)\right)dx. \quad (8)$$

If the solution of Eqn. (8) can be found, the values of λ_k can be found from the following relation:

$$-\frac{\partial}{\partial\lambda_k}\lambda_0 = \bar{f}_k \quad (9)$$

By finding λ_0 and λ_k, $k = 1,\ldots,m$ from the given set of constraints, the new pdf, $q(x)$, that minimizes cross-entropy is derived.

3.4 Optimal attack scenario in the MAC layer: cross-entropy approach

We now apply the results from Sect. 3.3 to the specific case of the IEEE 802.11 MAC protocol, deriving the general expression for distribution of optimal attacks.

It has been proven in [8] (for the case of a single legitimate node and a single attacker) and [9] (for the case of n legitimate nodes and one attacker) that the Sequential Probability Ratio Test (SPRT) is the optimal detection test for the worst case attack in the MAC layer. The performance of the optimal IDS is measured in terms of detection delay (expected number of samples needed for attack detection) and can be expressed as

$$\mathbb{E}[N] = \frac{C}{\int_0^W f_1(x)\ln\frac{f_1(x)}{f_0(x)}dx}, \quad (10)$$

where $C = f(P_D, P_{FA})$ and is a constant for a given IDS. We omit the proof of the optimality of SPRT and the derivation of the Eq. 10 and refer the reader to [8] and [9] for the detailed proofs.

By observing the Eq. 10 we conclude that the attacker achieves maximal detection delay by minimizing the denominator which represents cross-entropy $H(f_1, f_0)$ (Eq. 3). We assume that the attacker's goal is to diverge from the original distribution $f_0(x)$ to a new distribution $f_1(x)$, subject to the set of constraints given by the Eq. 1 and Eq. 2. The Eq. 1 represents the normalization property of a pdf. Assuming that both $f_0(x)$ and $f_1(x)$ are defined on the state space $[0,W]$, the Eq. 1 can be expressed as $\int_0^W f_1(x)dx = 1$. In order to obtain the expression for an optimal pdf, we need to express $\bar{f}_k, \lambda_k$ and λ_0 as a function of known parameters. Utilizing the fact that the cross-entropy method employs constraints on the mean [11], we can express $f_k(x)$ from Eq. 2 as $f_k(x) = x$, where x represents the backoff value of the attacker. In order to quantify $\bar{f}_k$ from Eq. 2 we need to note that when each peer in the network follows the protocol rules, the probability of channel access of peer i is equal to $\frac{1}{n}$. This work quantifies the network performance for the case of 1 attacker and n legitimate nodes. If we denote the probability of channel access of the attacker by P_1, the attacker's goal can be described as

$$P_1 = \frac{\eta}{1+n}, \eta \in (1, n+1] \quad (11)$$

Let us first compute the probability P_1 of the attacker to access the channel as a function of the pdf's f_1 and f_0. Following the IEEE 802.11 protocol, the backoff counter of any node freezes during the transmissions and reactivates during free periods. Therefore, let us observe the backoff times during a fixed period T that *does not include* transmission intervals. We first consider the case of one misbehaving and one legitimate node and assume that within the time period T, we observe $X_1,\ldots,X_N$, N samples of the attacker's backoff and $Y_1,\ldots,Y_M$, M samples of the legitimate node's backoffs. It is then clear that the attacker's percentage of accessing the channel during the period T is $N/(N+M)$. In order to obtain the desired probability we need to compute the limit of this ratio as $T \to \infty$. Notice that

$$X_1 + \cdots + X_N \le T < X_1 + \cdots + X_{N+1}$$
$$Y_1 + \cdots + Y_M \le T < Y_1 + \cdots + Y_{M+1},$$

which yields

$$\frac{\frac{N}{S(X_N)}}{\frac{N}{N+1}\frac{N+1}{S(X_{N+1})} + \frac{M}{M+1}\frac{M+1}{S(Y_{M+1})}} \ge \frac{\frac{N}{T}}{\frac{N}{T} + \frac{M}{T}} \ge \frac{\frac{N}{N+1}\frac{N+1}{S(X_{N+1})}}{\frac{N}{S(X_N)} + \frac{M}{S(Y_M)}}. \quad (12)$$

where $S(X_i) = X_1 + \cdots + X_i$. Letting $T \to \infty$ results in $N, M \to \infty$ and from the previous double inequality, by applying the Law of Large Numbers, we conclude that

$$\mathrm{P}_1 = \lim_{N,M\to\infty}\frac{N}{N+M} = \frac{\frac{1}{\mathbb{E}_1[X]}}{\frac{1}{\mathbb{E}_1[X]} + \frac{1}{\mathbb{E}_0[Y]}}. \quad (13)$$

Using exactly similar reasoning the probability P_1, for the case of one misbehaving node against n legitimate ones, takes the form

$$\mathrm{P}_1 = \frac{\frac{1}{\mathbb{E}_1[X]}}{\frac{1}{\mathbb{E}_1[X]} + \frac{n}{\mathbb{E}_0[Y]}} = \frac{1}{1 + n\frac{\mathbb{E}_1[X]}{\mathbb{E}_0[Y]}} = \frac{1}{1 + n\frac{2\mathbb{E}_1[X]}{W}}, \quad (14)$$

where the fact that the average backoff of a legitimate node is $W/2$ (because f_0 is uniform in $[0,W]$) was used in the last equality.

If the attacker were legitimate, then $\mathbb{E}_1[X] = \mathbb{E}_0[Y]$ and his probability of accessing the channel, from Eq. (14), would have been

$1/(n+1)$. It is therefore clear that whenever

$$\mathbb{E}_1[X] = \alpha \mathbb{E}_0[Y], \text{ with } \alpha \in (0,1) \quad (15)$$

the attacker enjoys a gain as compared to any legitimate node since then

$$P_1 = \eta \frac{1}{n+1} > \frac{1}{n+1}, \text{ where } \eta = \frac{1+n}{1+\alpha n} \in (1, n+1). \quad (16)$$

In other words, his probability of accessing the channel is greater than the corresponding probability of any legitimate node by a factor $\eta > 1$. In order to obtain the expression for $\bar{f}_k$, we note that the general results derived in Sec. 3.3 also hold for the case when the equality in Eq. 2 is substituted with inequality (the complete proof of this claim can be found in [2]). By plugging in the value of P_1 from Eq. 14 into Eq. 16, we now rewrite Eq. 1 and Eq. 2 updated with the new information:

$$\int_0^W f_1(x)\,dx = 1 \quad (17)$$

and

$$\int_0^W x f_1(x)\,dx \leq \frac{1-\frac{\eta}{n+1}}{n\frac{\eta}{n+1}} \frac{W}{2}, \quad 1 < \eta < n+1. \quad (18)$$

Using the fact that the $=$ sign in Eq. 2 can be exchanged with $\leq$ sign and comparing the obtained expression with Eq. 18, we derive the expression for $\bar{f}_k$. Before proceeding with calculations of λ_0 and λ_k we quantify the notion of an "attack". Let η be a quantity that satisfies $1 < \eta < n+1$ and consider the class F_η of all pdfs that induce a probability P_1 of accessing the channel that is no less than $\eta/(n+1)$. Using (15) and (16) the class F_η can be explicitly defined as

$$F_\eta = \left\{ f_1(x) : \int_0^W x f_1(x)\,dx \leq \frac{1-\frac{\eta}{n+1}}{n\frac{\eta}{n+1}} \frac{W}{2} \right\}, \quad 1 < \eta < n+1. \quad (19)$$

This class includes all possible attacks for which the incurred relative gain exceeds the legitimate one by $(\eta - 1) \times 100\%$. The class F_η is the uncertainty class of the robust approach and η is a tunable parameter. Notice from (16) that since P_1 is a probability the *gain factor* η must not exceed $n+1$ in order for the previous inequality to produce a nonempty class F_η. By defining the class F_η, we imply that the detection scheme should focus on attacks with larger impact to system performance and not on small-scale or short-term attacks. We define the severity of the attack by changing the gain factor η. Values of η larger but close to 1 are equivalent to low-impact attacks whereas values significantly larger than 1 are equivalent to DoS attacks.

We now proceed to formally define the optimal pdf of an attacker in the IEEE 802.11 DCF MAC by using cross-entropy principle. Due to the fact that the only constraint imposed upon the new pdf (apart from the normalization property expressed by Eq. 1) is the constraint in mean, and using the fact that $f_k(x) = x$ and $p(x) = \frac{1}{W}$ (uniform pdf for all legitimate nodes), we obtain the general expression for $f_1(x)$ from Eq. 4. The parameter λ_0 is expressed as a function of λ_1 by using the Eq. 8 from Sect. 3.3. This yields the expression for an optimal attack pdf:

$$f_1(x) = \frac{\lambda_1}{e^{\lambda_1 W} - 1} e^{\lambda_1 (W - x)} \quad (20)$$

Finally, the value of parameter λ_1 is easily obtained from the Eq. 9:

$$\frac{1}{\lambda_1} - \frac{W e^{\lambda_1 W}}{1 - e^{-\lambda_1 W}} = \frac{1-\frac{\eta}{n+1}}{n\frac{\eta}{n+1}} \frac{W}{2} \quad (21)$$

It is now obvious that the results obtained by using the cross-entropy principle are identical to the ones obtained in [8] and [9]. The crucial difference between the two approaches is that the cross-entropy approach provides a *universal* expression for an optimal attack distribution and the approaches in [8] and [9] analyze a specific case of misbehavior. In addition to that, the cross-entropy approach enables the attacker to launch *multi-stage adaptive attacks*, by updating the the constraints from Eq. 2. This enables the attacker to converge towards the desired level of aggressiveness (or equivalently towards the desired pdf) in more than one step, gradually "blending" into the environment. Multi-stage attacks are not investigated in this work and represent an important extension towards building a more comprehensive analysis of adaptive attacks.

We now analyze the effects of optimal attacks launched in the MAC layer on the performance of the network layer. We show by mathematical analysis and simulation that the absence of a MAC layer-based IDS can significantly decrease the performance of the network layer. In addition to that, we show that the absence of a MAC layer-based IDS can lead to false accusations of legitimate nodes (i. e. large number of false positives) by a network layer-based IDS.

4. IMPACT OF MAC LAYER ATTACKS ON THE NETWORK LAYER

Under regular conditions the MAC layer has to go through multiple transmissions before detecting a link failure. The detection delay induced by additional congestion due to the presence of one or more attackers causes the feedback delay to the routing layer. We now prove that an intelligent attacker acting under the optimal strategy described with the pdf $f_1(x)$ (Eq. 20) can cause devastating effects in the network layer if no MAC layer-based IDS is employed. Furthermore, we show that by employing a quickest detection scheme proposed in [8], the effects of such attacks can be easily prevented by isolating the detected attacker at the origin of the attack. Finally, we propose a cross-layer based cooperation scheme that is mainly oriented towards preventing propagation of local effects of MAC layer attacks.

We start our analysis by observing the scenario presented in Fig. 1 where selfish node accesses the channel by using an optimal attack strategy defined in Sect. 3.4. When the backoff counter decreases to zero, the selfish node sends an RTS to node *Int*2, which replies with CTS. The RTS message silences *Node*2 which is in the wireless range of the selfish node. *Source*1 and *Node*1 are out of the range of both sender and receiver. Under the assumption that *Source*1 establishes a route to *Destination*1 through *Node*1 and *Node*2, it is reasonable to assume that *Node*1 will attempt to transmit to *Node*2 during the transmission period of selfish node (we assume, just like in Sect. 3.3, that all nodes are backlogged and always have traffic to send). *Node*2 is silenced by selfish node's RTS and is not able to reply with a CTS. After a time period equal to CTS timeout, *Node*1 increases its contention window exponentially and attempts to retransmit upon its expiration. We assume that *Node*1 constantly attempts to communicate with silenced nodes and consequently increases its contention window until it reaches its maximal value. At the same time, *Source*1 sends its regular traffic to *Node*1, increasing its backlog over time. As the misbehavior coefficient of the selfish node increases (or equivalently its backoff decreases), the selfish node gains larger percentage of channel access. Conse-

quently, *Node*2 is silenced more frequently, increasing the backlog at *Node*1.

Assuming that each node has a finite buffer of size ν, we now derive a general expression for expected time to buffer overflow at *Node*1. Furthermore, by analyzing the scenario in Fig. 1 we simplify the general expression, deriving an expression applicable for analysis of effects of an optimal attack. We show by analysis an simulation that if no ID mechanism is employed in the MAC layer, the optimal MAC attack forces legitimate nodes to drop significant number of packets due to buffer overflow. If a watchdog-based or a more sophisticated reputation-based detection scheme is employed in the network layer, one or more legitimate nodes can easily be flagged as malicious due to the large number of dropped packets.

Finally, we analyze the scenario presented in Fig. 2 and present the effects of an optimal MAC layer attack on routes that are out of the wireless range of the attacker. We show that an intelligent attacker can easily cause route failure by attacking nodes that belong to the routes with the highest capacity. The results are presented for two routing protocols: Dynamic Source Routing Protocol (DSR) [4] and Ad hoc On Demand Distance Vector (AODV) [6].

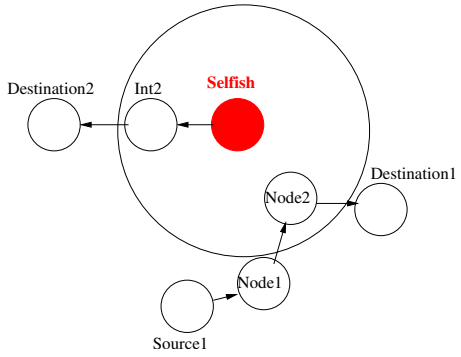

Figure 1: *Node*2 is silenced by the transmission of the selfish node. Consequently, *Node*1 drops large number of packets.

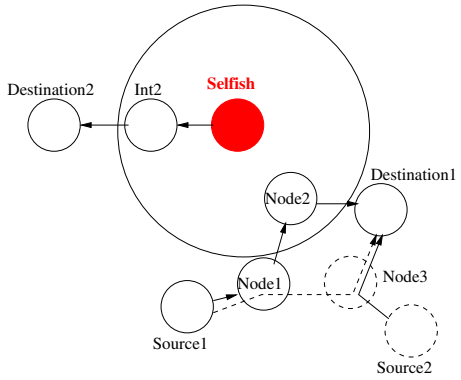

Figure 2: An ongoing attack in the MAC layer breaks the original route, re-routing the traffic through *Node*3.

4.1 Impact of MAC Layer Misbehavior on the Network Layer: Time to Buffer Overflow

As it has been mentioned in Sect. 4, the secondary effect of an optimal MAC layer attack can be as devastating as the primary ones with respect to the network connectivity. If no alternative route can be found, a non-DoS optimal MAC layer attack can produce a DoS-like effects in the network layer due to the exponential nature of the IEEE 802.11 DCF backoff algorithm (such as causing buffer overflow in *Node*1 from Fig. 1). This section provides a comprehensive analysis of the scenario presented in Fig. 1, followed by analysis of the scenario presented in Fig. 2 and simulation results.

We denote the incoming traffic as α_t and the outgoing traffic as β_t and assume that both processes are Poisson with parameters α and β respectively. Consequently, δ_t represents the difference between the incoming and outgoing traffic: $\delta_t = (\alpha_t - \beta_t)^+$ at time t. Equivalently, δ_t represents the increase rate of packets in the buffer over time or *backlog*. In this setup we are interested in finding the time of buffer overflow

$$T = \inf_t \{\delta_t \geq \nu\} \tag{22}$$

where ν denotes the buffer size. Clearly T is random, in fact it is a *stopping time*. Next we are going to develop closed form expressions for the *average-time-to-overflow*, that is, $\mathbb{E}[T]$.

If $U_1 < U_2 < U_3 < \ldots$ represent the arrival times and $V_1 < V_2 < V_3 < \ldots$ the departure times, a typical form of the paths of δ_t is depicted in Fig. 3. We observe that δ_t exhibits piecewise constant

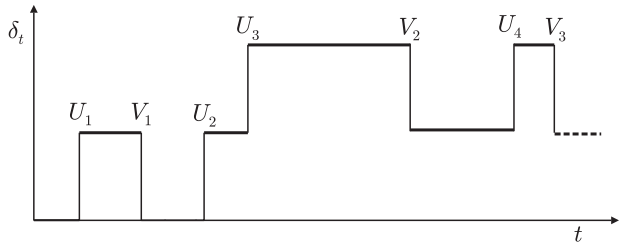

Figure 3: Arrival and departure times in the queue of length δ

paths with discontinuities of size equal to ± 1. Without loss of generality we are going to assume that these paths are *right continuous*. In order to be able to compute $\mathbb{E}[T]$ we need to study the paths of the process $g(\delta_t)$ where $g(\cdot)$ denotes a continuous nonlinear function. If $t \leq T$ is any time instant before overflow, using the right continuity of δ_t, we can write

$$g(\delta_t) - g(\delta_0) = \sum_{n=1}^{\alpha_t} g(\delta_{U_n}) - g(\delta_{U_n}\text{-}) + \sum_{n=1}^{\beta_t} g(\delta_{V_n}) - g(\delta_{V_n}\text{-}) \tag{23}$$

where U_n-, V_n- denote the time instant right before the n-th arrival and departure respectively. Since the discontinuities of δ_t are equal to ± 1 (depending on whether we have arrival or departure), we can write

$$g(\delta_{U_n}) = g(\delta_{U_n}\text{-} + 1), \quad \text{and} \quad g(\delta_{V_n}) = g\left((\delta_{V_n}\text{-} - 1)^+\right)$$

with the latter positive part needed because we have a departure only when the buffer is not empty. Substituting both equalities in (23) the following expression is obtained

$$\begin{aligned} g(\delta_t) - g(\delta_0) &= \int_0^t [g(\delta_s\text{-} + 1) - g(\delta_s\text{-})] d\alpha_s \\ &+ \int_0^t [g\left((\delta_s\text{-} - 1)^+\right) - g(\delta_s\text{-})] d\beta_s. \end{aligned}$$

Replacing in the latter expression $t = T$ and applying expectation we have

$$\begin{aligned} \mathbb{E}[g(\delta_T)] - g(\delta_0) &= \mathbb{E}\left[\int_0^T [g(\delta_s\text{-} + 1) - g(\delta_s\text{-})] d\alpha_s\right] \\ &+ \mathbb{E}\left[\int_0^T [g\left((\delta_s\text{-} - 1)^+\right) - g(\delta_s\text{-})] d\beta_s\right]. \end{aligned}$$

Because T is a stopping time and δ_s- is in the past of the time instant s, according to [7], in the previous two expectations we can replace $d\alpha_t$ with αdt and $d\beta_t$ with βdt where α, β, recall, are the corresponding rates of the two Poisson processes α_t, β_t. This leads to the following equation

$$\mathbb{E}[g(\delta_T)] - g(\delta_0) = \mathbb{E}\Bigg[\int_0^T \Big\{\alpha[g(\delta_s\text{-}+1) - g(\delta_s\text{-})] + \beta[g\left((\delta_s\text{-}1)^+\right) - g(\delta_s\text{-})]\Big\} ds\Bigg]. \quad (24)$$

Notice now that if we select $g(\cdot)$ to satisfy the difference equation

$$\alpha[g(\delta+1) - g(\delta)] + \beta[g\left((\delta-1)^+\right) - g(\delta)] = -1 \quad (25)$$

then Eqn. (24) simplifies to

$$g(\delta_0) - \mathbb{E}[g(\delta_T)] = \mathbb{E}[T]. \quad (26)$$

Since $\delta_t \geq 0$ the function $g(\cdot)$ needs to be defined only for non-negative arguments. However, in order to avoid using the positive part in (25), we can extend $g(\cdot)$ to negative arguments as follows

$$g(\delta) = g(0), \text{ for } -1 \leq \delta \leq 0, \quad (27)$$

and this simplifies (25) to

$$\alpha[g(\delta+1) - g(\delta)] + \beta[g(\delta-1) - g(\delta)] = -1. \quad (28)$$

Furthermore, since at the time of stopping T we have a full buffer, that is, $\delta_T = \nu$ (with ν denoting the buffer size), if we impose the additional constraint

$$g(\nu) = 0, \quad (29)$$

and recall that $\delta_0 = 0$, from (26) we obtain $\mathbb{E}[T] = g(0)$.

Summarizing, we have $\mathbb{E}[T] = g(0)$ where $g(\cdot)$ is a function that satisfies the difference equation (28) and the two boundary conditions (27), (29). Since ν is an integer it suffices to solve (28) for integer values of δ meaning that (28) can be seen as a recurrence relation of second order. The solution to our problem can thus be easily obtained and we have

$$\mathbb{E}[T] = \begin{cases} \frac{1}{\alpha}\left\{\frac{\rho}{(1-\rho)^2}[\rho^\nu - 1] + \frac{\nu}{1-\rho}\right\} & \text{for } \alpha \neq \beta, \\ \frac{1}{\alpha}\left\{\frac{\nu+\nu^2}{2}\right\} & \text{for } \alpha = \beta, \end{cases} \quad (30)$$

where $\rho = \beta/\alpha$ denotes the ratio between the outgoing and incoming traffic rates. In order to examine the effects of various levels of traffic on the network stability needs to be examined. By definition, stability of the network means bounded backlogs over time, i.e. $\sup E[\delta_i(t)] < \infty$ for all nodes i in the network. We observe that whenever $\alpha > \beta$ (or $\rho < 1$) the exponential term (for large buffer size ν) is negligible as compared to the linear term and the queue needs, in the average, linear time to overflow (instability). In the opposite case $\alpha < \beta$ (or $\rho > 1$), the exponential term prevails and the average-time-to-overflow becomes exponential (stability). These observations can also be seen in Fig. 4 for $\rho = \beta/\alpha = 3/2$ and $\rho = \beta/\alpha = 2/3$ where we plot the average time as a function of the buffer size ν. Equivalently, $\alpha > \beta$ implies increase of backlog in the given node over a period of time and vice versa.

In the stable case, we observe the extremely large average time required to overflow even for small values of the buffer size. In Fig. 5 we plot the average time as a function of the traffic rate ratio $\rho = \beta/\alpha$, assuming normalized incoming rate $\alpha = 1$ and buffer size $\nu = 100$. For any other value of α, according to (30), we simply need to divide by α.

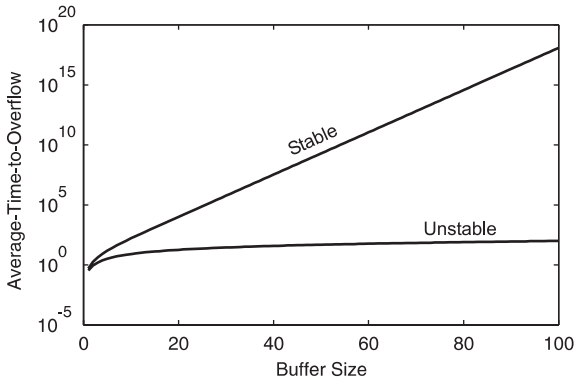

Figure 4: Average Time to buffer overflow for $\rho = \beta/\alpha = 3/2$ (stability) and $\rho = \beta/\alpha = 2/3$ (instability), as a function of the buffer size ν.

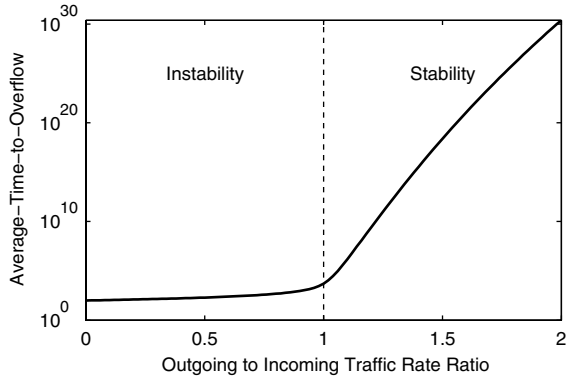

Figure 5: Average time to buffer overflow as a function of the traffic rate ratio $\rho = \beta/\alpha$ and buffer size $\nu = 100$.

We now return to the analysis of the scenario presented in Fig. 1. It has already been mentioned that with the increase of the aggressiveness of the attacker (i. e. parameter η in Eq. 16), the percentage of channel access for *Node*2 will accordingly decrease. Meanwhile, *Source*1 keeps generating traffic at the same rate, sending packets to *Node*1. With *Node*2 being silenced, *Node*1 has the parameter β equal to zero. Eq. 30 also suggests that whenever $\alpha \gg \beta$ (or $\rho \ll 1$) then $\mathbb{E}[T] \approx \frac{\nu}{\alpha}$. In order to proceed further with the discussion we need to note that finding the average time to buffer overflow $\mathbb{E}[T]$ is equivalent to finding the average time until the observed node starts losing traffic due to buffer overflow. We need to note that the scenario in which $\alpha \gg \beta$ represents the secondary effects of an optimal attack. We assume that the network has an Intrusion Detection System (IDS) implemented and that it detects a network layer attack with an average delay of Δt. Assuming that the buffer overflow happens at time t, the attack is detected at time $t_1 = t + \Delta t$. Consequently, the amount of traffic lost (TL) due to buffer overflow in node i in a network of k nodes at time t_1 can be defined as:

$$TL = \sum_{i=1}^{k} \alpha_i \left(t_1 - \frac{\nu}{\alpha_i}\right).$$

It can be easily observed from this expression that even small detection delays of the order of a couple of seconds have relatively large traffic loss as a consequence.

To illustrate the amount of lost traffic due to detection delay in

the network layer we present the results of the above analysis for a single node in Fig. 6 for various rates of incoming traffic. As expected, the amount of lost traffic increases as the incoming traffic rate increases. It can be easily observed that even small detection delays of the order of a couple of seconds have relatively large traffic loss as a consequence.

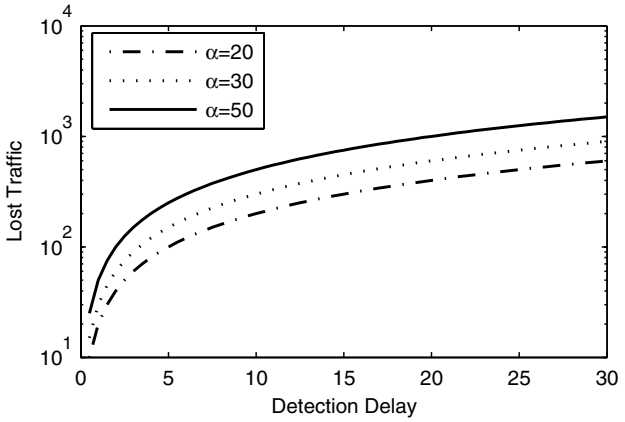

Figure 6: The amount of lost traffic as a function of detection delay for fixed buffer size ν=100.

5. NUMERICAL RESULTS

5.1 Direct effects of the optimal MAC layer attacks

In order to quantify the performance of the optimal attacker we introduce the *absolute gain*, defined as $\frac{\eta}{n+1}$ for $1 < \eta < n+1$, where η was defined in Sect. 3.4. We observe that the maximum value of the absolute gain is equal to 1 and corresponds to the DoS attack and the minimum value of the absolute gain is equal to $\frac{1}{n+1}$ and corresponds to legitimate behavior of the observed node.

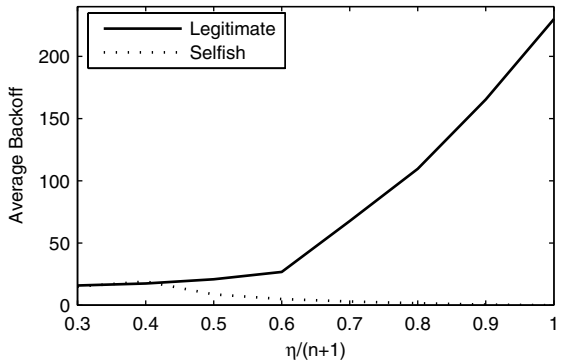

Figure 7: Average backoff (in slots) for legitimate and malicious nodes as a function of absolute gain $\frac{\eta}{n+1}$.

We now proceed to performance evaluation of the optimal attacker from Sect. 3.4. The scenario being evaluated consists of 3 nodes, one of which misbehaves using the optimal attack strategy. We assume that all nodes are backlogged and have packets to send and are in the wireless range of each other. The protocol employed is IEEE 802.11 DCF and the scenario is evaluated in the network simulator Opnet. Fig. 7 represents the average backoff of legitimate

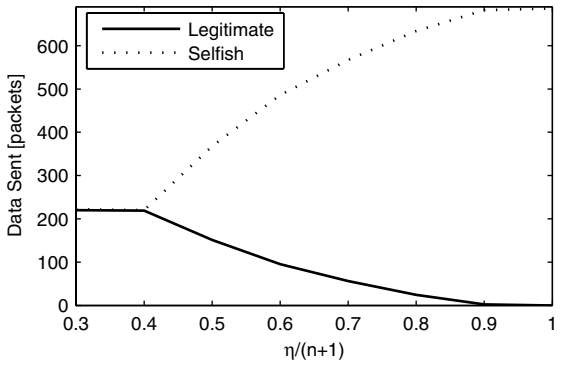

Figure 8: Average number of data packets sent for legitimate and malicious nodes as a function of absolute gain $\frac{\eta}{n+1}$.

and selfish nodes as a function of the absolute gain of the selfish node. As expected, the average value of backoff for all nodes is almost identical when all participants obtain fair share of channel access (by choosing backoff values using the uniform pdf) and does not exhibit large deviations from the average value until the attacker obtains approximately 45% of total channel access time. For high values of misbehavior, the legitimate nodes are completely denied access to the channel due to the fact that the selfish user is always able to transmit since his backoff values are close to zero. To further illustrate the effect of the worst-case MAC layer attack we observe the average number of data packets sent by each node as a function of absolute gain. The results of the analysis are presented in Fig. 8. Just like in the previous scenario, the fair sharing of the channel assumes that each participant will send the same amount of data on average. With the increase of aggressiveness of the selfish node, the legitimate nodes are denied access to the channel by choosing larger backoff values (Fig. 7) and consequently are not able to send data, since the selfish node gains higher percentage of channel access.

For the performance analysis of an optimal IDS that is employed for detection of the above attacks the proofs of optimality of the Sequential Probability Ratio Test (SPRT) from [8] and [9] are used. The proofs state that the SPRT is the quickest detection scheme for optimal MAC layer attacks. We implement such detection scheme

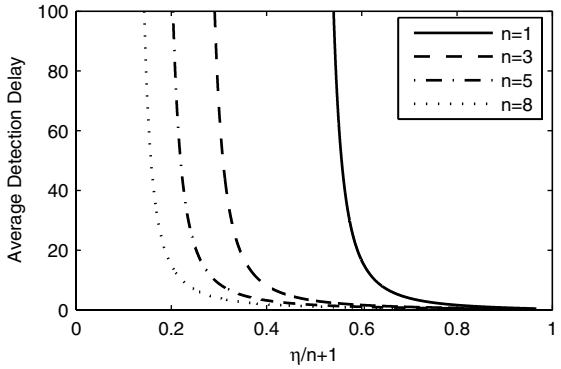

Figure 9: Average Detection Delay as a function of absolute gain $\frac{\eta}{n+1}$ for $\alpha = \beta = 0.01$.

in Matlab and use it for performance evaluation of the optimal attack strategy, measuring the performance in terms of detection de-

lay. In order to obtain some intuition from our results, we consider the case of one attacker competing with $n \geq 1$ legitimate nodes. We fix the probability of detection and the probability of false alarm to 0.99 and 0.01 respectively and measure the Average Detection Delay $\mathbb{E}[N]$ as a function of absolute gain. The evaluation results are presented in Fig. 9. The graph shows that low values of η prolong the detection procedure, since in that case the attacker does not deviate significantly from the protocol. On the other hand, a large η signifies a class of increasingly aggressive attacks for which the detection is achieved with very small delay. It can be seen that detection becomes more efficient as the number of participating legitimate nodes increases. For example, for an absolute gain of 0.6, the IDS will require 10 times less samples to detect misbehavior for $n = 5$, than for the case of $n = 1$. This is due to the fact that absolute gain of 0.6 for the case of $n = 5$ users corresponds to more aggressive access strategy than in the case of $n = 1$ users.

The results above provide useful insights about the response of the system with respect to the attack. A more aggressive attack policy brings significant benefits each time the attacker accesses the channel, but it allows limited number of channel uses before it is detected. On the other hand, a milder attack incurs lower benefit for each channel use but it enables the attacker to access the channel more times before it is detected. If the policy of a fixed gain is followed, the attackers behavior converges towards the DoS attack as n increases.

5.2 Cross-layer effects of the optimal MAC layer attacks

In order to illustrate the effects of an optimal MAC layer attack on the network layer we analyze the two scenarios presented in Fig. 7 and Fig. 9 with DSR and AODV as routing protocols. Before proceeding with the analysis, a short description of the routing protocols used in the experiments is provided.

DSR is a source routing protocol: the source knows the complete hop-by-hop route to the destination and routes are stored in node caches. It consists of two basic mechanisms: Route Discovery and Route Maintenance. When a node attempts to send a data packet to a new destination, the source node initiates a route discovery process to dynamically determine the route. Route Discovery works by flooding Route Request (RREQ) packets. RREQ packets propagate throughout the network until they are received by a node with a route to the destination in its cache or by the destination itself. Such a node replies to the RREQ with a route reply (RREP) that is routed back to the original source. The RREQ builds up the path traversed until that moment by recording the intermediate nodes and the RREP routes itself back to the source by traversing the path backwards. If any link along a path breaks, Route Maintenance mechanism is invoked by using a Route Error (RERR) packet, resulting in removal of any route that contains that link. If the route is still needed by the source, a new route discovery process is issued.

AODV uses table-driven hop-by-hop routing. It applies a similar Route Discovery process as DSR. However, instead of using route caches, it uses routing tables to store routing information, one entry per destination. AODV relies on routing table entries to propagate a RREP back to the source and to route data packets to the destination. Furthermore, AODV uses sequence numbers (carried by all packets) to determine freshness of routing information and to prevent routing loops. One notable feature of AODV is the use of timers regarding utilization of routing table entries. Namely, a routing entry in the table may expire if it is not used recently. Moreover, a set of neighboring nodes that use this entry is also maintained; these nodes are notified through RERR packets when the next hop link breaks. This process is recursively repeated by each node, thereby effectively deleting all routes using the broken link. Upon that, a new Route Discovery process is initialized.

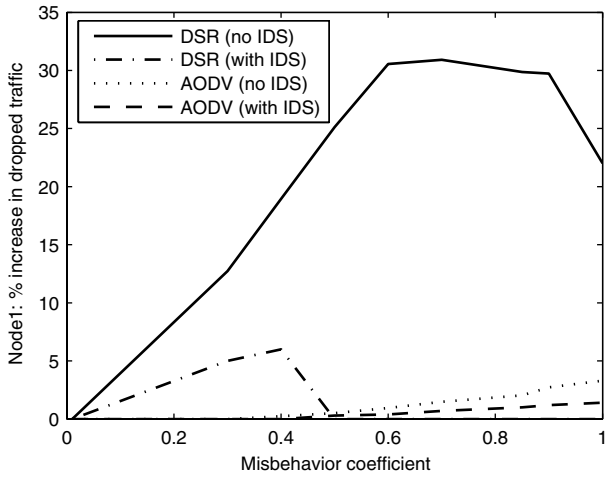

Figure 10: Increase in dropped traffic at $Node1$.

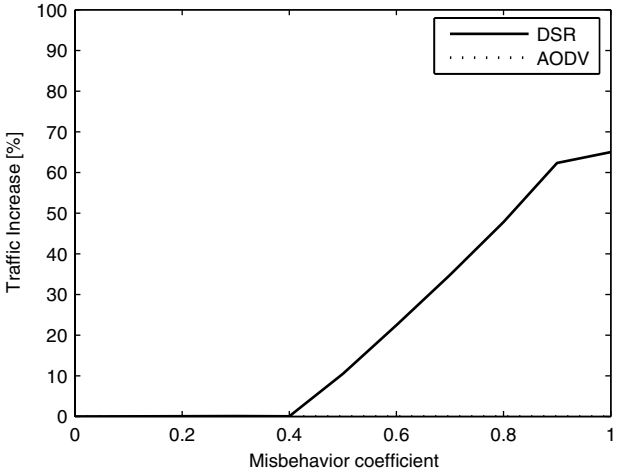

Figure 11: Percentage increase in traffic through alternate route as a consequence of an ongoing MAC layer attack.

We now evaluate the cross-layer impact of the optimal attacker in the MAC layer. The results of the simulations are presented in Fig. 10 and Fig. 11. Fig. 10 analyzes the performance of $Node1$ from Fig. 7 as a function of ε with DSR and AODV as the routing protocols for two cases (i) without MAC layer-based IDS and (ii) with the MAC layer-based IDS. It is reasonable to expect that $Node2$ is denied channel access more frequently as the aggressiveness of the selfish node increases in the absence of a MAC layer-based IDS. Consequently, $Node1$ is disabled from forwarding packets towards the destination. After evaluating the scenario from Fig. 7, we note that the percentage of dropped packets at $Node1$ increases with with the aggressiveness of the attacker, since $Node2$ is denied access to the channel due to transmissions of the selfish node. We observe that the percentage increase in dropped traffic is almost linear until ε=0.6. However, further increase in aggressiveness of the attacker does not bring any significant benefit in terms of increase of dropped traffic at legitimate nodes. This effect is

due to the operating mechanism of the DSR protocol. Namely, if the neighboring node (in this case *Node*2) does not respond to the requests of the sender for a certain period of time, the route maintenance mechanism of DSR protocol sends a RERR and a new RREQ is issued. Consequently, the contents of the buffer are flushed after the issue of RERR. Therefore, the maximum value of percentage increase in dropped traffic due to the malicious behavior in the MAC layer is bounded by (i) size of the maintenance buffer in the observed node and (ii) the route maintenance timeout value (which in this case corresponds to 40% increase in dropped traffic, even in the case of the DoS attack). Another interesting observation is that the number of dropped packet decreases for the maximal value of the misbehavior coefficient. This can be easily explained by the fact that *Source*1 cannot establish a route to *Destination*1 when a DoS attack is launched. Consequently, very few packets are sent to *Node*1, most of which are dropped due to unavailability of the neighboring node. AODV, on the other hand, exhibited high resistance to misbehavior with the percentage of dropped packets being close to zero and almost independent of the degree of misbehavior. The difference in performance of two protocols can be explained as follows. If a node that belongs to a DSR route detects a broken link, it tries to salvage packets waiting in send buffer by trying to search for an alternative route in the route cache. Once this process fails, the packets in the buffer are dropped and a RERR is sent to the source. AODV, on the other hand, has no route cache, but instead uses local repair when a broken link is detected. Namely, if a node detects a broken link, it sends RREQ directly to the destination. This implies that misuses that are targeted at disrupting services can generate only temporary impact, forcing the attacker to repeat misuses at higher frequency in order to disrupt the service. Observing the results in Fig. 10, we conclude that the local repair mechanism of AODV protocol can handle failures due to MAC layer attacks with much higher success rate than DSR.

To further illustrate the effects of an optimal MAC layer attack on the network layer we now proceed to the analysis of the scenario presented in Fig. 9. An additional traffic generating source (*Source*2) and an additional node (*Node*3) that resides in the wireless range of *Node*1 are added. These additional nodes enable creation of an alternative route to *Destination*1 in case of failure of *Node*2. We repeat the same misbehavior pattern of the selfish node as in the previous scenario and record the traffic increase through an alternative route. Due to the failure of *Node*2 and the exponential nature of backoff mechanism of *Node*1, *Node*2 becomes unreachable after the certain threshold (that corresponds to $\varepsilon = 0.4$) and traffic is re-routed to the final destination through *Node*3. This topology ensures better throughput for legitimate nodes and decreases the total number of dropped packets for the DSR protocol due to the fact that after the initial route is broken, an alternative route from its cache is used to send packets. AODV, due to the identical reasons as in the previous example, is again superior to DSR with respect to the number of packets dropped and does not use the alternative route.

5.3 Implementation of an optimal MAC layer-based IDS

The experimental results of the scenario that employs an optimal MAC layer attack were presented in Sect. 5.2 and illustrated its effects in terms of lost traffic. We now implement the optimal MAC layer-based detection scheme presented in [8] and investigate the effects on the dropped traffic in the network layer with DSR and AODV as routing protocols. We assume that all nodes that take part in the detection process are legitimate and do not falsely accuse their peers of misbehavior. The results are presented in Fig. 10. Observing the results for the DSR protocol performance we note that the IDS achieves maximum performance for misbehavior coefficients that are larger than 0.5 (i.e. more aggressive attacks). This can be easily explained by noting that the MAC layer IDS was constructed to detect a class of more aggressive attacks that have higher impact on the system performance. On the other hand, the low impact attacks take longer to be detected (see Fig. 9) and influence the performance of the routing protocol. Namely, low-impact attacks achieve certain gain in channel access time when compared to legitimate nodes. This causes temporary congestion in the MAC layer, where legitimate nodes backoff for larger periods of time due to the exponential nature of backoff mechanism in IEEE 802.11 DCF. Even after the selfish node is isolated, the legitimate nodes compete among themselves for channel access, which causes a small increase in dropped traffic. When the performance of low impact attacks is analyzed, it can be observed that the congestion effects last for additional 5-10s after the isolation of the attacker. However, the IDS detects and isolates aggressive selfish nodes almost instantly, causing no effects in the network layer. Consequently, the percentage increase in dropped traffic at legitimate nodes for aggressive strategies of an optimal attacker is equal to zero. We also note that AODV is more robust to MAC layer attacks from the reasons mentioned in Sect. 5.2 and consequently implementation of a MAC layer-based IDS has no significant influence on its performance.

We conclude that the effect of MAC layer misbehavior on the network layer is twofold: (i) legitimate nodes are forced to drop significant number of packets due to unavailability of their neighbors that are blocked by the selfish node; (ii) consequently, it causes significant decrease in throughput due to unavailability of one or more nodes belonging to the initial route. This gives rise to a larger number of false positives generated by an ID mechanism that resides in the network layer since most of the network-based ID mechanisms are threshold-based and react only after a certain number of dropped packets per second is exceeded. Consequently, if no MAC layer ID mechanism is employed, legitimate nodes can be accused of misbehaving. This proves the necessity of existence of ID mechanisms in both MAC and network layers.

6. CONCLUSIONS AND FUTURE WORK

This work represents the first step towards a more comprehensive analysis of cross-layer interaction for intrusion detection in wireless ad hoc networks. By using the principle of cross-entropy we derived a general expression for an optimal attack strategy in the IEEE 802.11 MAC. We illustrated the effects of such attacks on the network layer and implemented the framework for quickest detection of such strategies in the MAC layer. We derived a general expression for time to buffer overflow and consequently the amount of lost traffic due to buffer overflow in Sect. 4.1. Following that, we implemented such scenario in the network simulator Opnet and illustrated the effects of optimal attacks on the amount of lost traffic. Furthermore, we showed by simulation that certain routing protocols are more robust to MAC layer attack than the others. Therefore, the choice of a routing protocol has significant impact on the severity of impact of MAC layer attacks. Additionally, we proved by simulation that if a quickest detection MAC layer-based IDS is implemented, vertical propagation of attack effects is negligible. Only low-impact MAC layer attack affect the performance of the routing protocols up to a certain point. In order to eliminate these effects we suggest implementation of a cross-layer based cooperation scheme.

A first issue in building the cross-layer intrusion detection system concerns the exploitation of observations from several observers

in order to improve performance. This work assumed the existence of trusted observers, which cannot be assumed in general wireless environments. Therefore, a more comprehensive, cooperation-based scheme is needed. This amounts to the scenario where observers pass their measurements to a fusion center which then combines them appropriately and derives a decision about the occurrence or not of the attack. Due to different perceived channel conditions at different locations of observer nodes, the amount of interference at their receivers differs. If observers obtain the same sequence of measurements, different samples of the sequence are corrupted due to interference. The task of the fusion center is to combine the received sequences of measurements. Given that there exists a certain cost (e.g. consumed energy) in passing measurements to a fusion center, an interesting issue pertains to the minimum number of observers that are necessary to achieve a certain level of performance in terms of detection delay or accuracy.

On the other hand, the routing protocol is unaware of the events in the MAC layer if no vertical cooperation is implemented. It is known that if the routing protocol has several equally acceptable route choices, the route will be chosen randomly. If the chosen route belongs to the congested area, an additional bottleneck is created, degrading the performance even further. Hence, it is useful to introduce cross-layer cooperation in order to improve the performance of wireless network. We suggest tight cooperation between MAC and network layers. In order to avoid congested areas that emerged during the duration of the attack, the network layer should forward the possible route choices to the MAC layer which sends back a subset of optimal choices with respect to congestion and interference. This type of cooperation aims at avoiding bottlenecks in already congested areas in the MAC layer which can lead to early buffer overflows in the network layer. In order to avoid false accusations in the network layer that emerge due to the increased number of dropped packets, MAC layer should forward the detection results to the ID module in the network layer.

Another interesting problem that needs to be addressed is the role of the physical layer in a cross-layer based intrusion detection scheme. As it has been pointed out, the MAC layer is used for *local* detection of malicious behavior. However, the legitimate nodes are not capable of notifying the rest of the network about the malicious behavior without the help from the physical layer. The physical layer can be used for power control, i.e. the transmission power level of legal nodes that detect the malicious behavior is adjusted appropriately so that a certain area of the network can be covered by this notification, introducing the notion of global notification.

In future work we intend to analyze the effect of MAC attacks on a larger set of routing protocols and identify the properties of the most robust ones in order to construct features of an efficient cross-layer intrusion detection system. In addition to that, an interesting and more challenging issue is the one of detection of an adaptive attacker that adapts not only to the changing environment in terms of the number of participating nodes, but also in terms of the interference level.

7. REFERENCES

[1] C. Barrett, M. Drozda, A. Marathe and M. V. Marathe, "Analyzing Interaction Between Network Protocols, Topology and Traffic in Wireless Radio Networks", In *Proc. IEEE Wireless Communications and Networking Conference (WCNC '03)*,Vol. 3, pp. 1760–1766, New Orleans, 2003.

[2] I. Csiszar, T. Cover and B-S. Choi, "Conditional limit theorems under Markov conditioning", *IEEE Trans. on Information Theory*, vol. 33, No. 6, p.p. 788–801, Nov. 1987.

[3] IEEE, IEEE Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[4] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks", *Mobile Computing*, p.p. 153–181, 1996.

[5] V. Kawadia and P. R. Kumar,"A cautionary perspective on cross-layer design", *IEEE Wireless Communications*, Vol. 12, No. 1, p.p. 3–11, February 2005.

[6] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing", in *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, p.p. 90–100, February 1999.

[7] P. E. Protter, "Stochastic Integration and Differential Equations", Springer, 2nd edition, 2004.

[8] S. Radosavac, J. S. Baras and I. Koutsopoulos,"A Framework for MAC Protocol Misbehavior Detection in Wireless Networks", In *Proc. 4th ACM workshop on Wireless security (WiSe)*, p.p. 33–42, Cologne, Germany, September 2005.

[9] S. Radosavac, G. V. Moustakides, J. S. Baras and I. Koutsopoulos, "An analytic framework for modeling and detecting access layer misbehavior in wireless networks", submitted to *ACM Transactions on Information and System Security (TISSEC)*, 2006.

[10] J. E. Shore and R. W. Johnson, "Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy", *IEEE Trans. on Information Theory*, Vol. 26, No. 1, p.p. 26–37, January 1980.

[11] J. E. Shore and R. W. Johnson, "Properties of Cross-Entropy Minimization", *IEEE Trans. on Information Theory*, Vol. 27, No. 4, p.p. 472–482, July 1981.

[12] V. Srivastava and M. Motani, "Cross-Layer Design: A Survey and the Road Ahead", In *IEEE Communications Magazine*, Vol. 43, p. p. 12–19, December 2005.

[13] Y. Zhang, W. Lee and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks", *Wireless Networks*, Vol. 9, No. 5, p. p. 545–556, 2003.