Analysis of CSMA broadcast performance in tactical ad hoc networks

ARWID KOMULAINEN AND ULF STERNER

FOI-R--4219--SE
ISSN 1650-1942 January 2016

Arwid Komulainen and Ulf Sterner

Analysis of CSMA broadcast performance in tactical ad hoc networks

Titel	Analys av broadcastprestanda för CSMA i taktiska ad hoc-nät
Title	Analysis of CSMA broadcast performance in tactical ad hoc networks
Rapportnr / Report No.	FOI-R--4219--SE
Månad / Month	Januari / January
Utgivningsår / Year	2016
Antal sidor / Pages	37
ISSN	1650-1942
Kund / Customer	FMV
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT område	Ledning och MSI
Projektnr / Project No.	E324534
Godkänd av / Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Abstract

This report investigates the possible use of carrier sense multiple access (CSMA) for transmitting broadcast traffic in mobile military ad hoc networks. CSMA is a widely used medium access control (MAC) protocol, most prominently as being part of the distributed coordination function (DCF) in the IEEE 802.11 standard for wireless local are networks (WLAN). Unlike most non-military wireless networks, tactical ad hoc networks focused on here, are often characterized by a majority of the traffic sent being multicast or broadcast. The report describes how the parameter setting and function of CSMA need to be adjusted when used for broadcast traffic rather than unicast traffic and ultimately how this affects the performance of the protocol. An overview of related work at adapting CSMA to better handle broadcast-type traffic is given and the applicability of the proposed methods is discussed. To evaluate the performance of CSMA in tactical ad hoc networks simulations are used.

An important factor that determines the broadcast traffic performance in ad hoc networks, aside from the MAC protocol, is the routing protocol and its coupling with the MAC protocol being used. In the simulations, multipoint relay (MPR) flooding is used, which is a commonly used protocol for multicast and broadcast traffic in ad hoc networks and part of the Optimized Link State Routing (OLSR) standard. The results show that when MPR flooding is used with CSMA, robustness problems arise due to the contention-based access that CSMA provides for the control packets needed for MPR-node selection. The result is that under high traffic loads or in sparse networks, MPR-node selection fails due to a high number of collisions, which in turns causes more duplicate packets to be sent and thereby increasing the collisions further. This behaviour results in a very limited network capacity for broadcast-type traffic when CSMA is used, due to high packet losses from collisions.

Finally, CSMA is compared to a benchmark system using a fixed time division multiple access (TDMA) protocol instead of CSMA. The comparison shows that the performance of CSMA is inferior to the benchmark system in all cases except under low traffic loads when the network is very well-connected.

Keywords: CSMA, OLSR, ad hoc networks, multicast, broadcast

Sammanfattning

I denna rapport undersöks möjligheten att använda CSMA (carrier sense multiple access) för att skicka broadcasttrafik i mobila taktiska ad hoc-nätverk. CSMA är ett MAC-protokoll (Medium Access Control) som används i många civila nätverk, i synnerhet utgör CSMA en del av DCF (distributed coordination function) i IEEE:s standard 802.11 för trådlösa lokala nätverk (WLAN) . Till skillnad från många civila trådlösa nätverk utgörs en stor del av trafiken i de taktiska ad hoc-nätverk som rapporten fokuserar på av multicast- och broadcasttrafik. I den här rapporten beskrivs hur parametersättning och funktionalitet hos CSMA behöver anpassas när trafiken som sänds är av broadcast-natur och i slutändan vilken påverkan det har på prestandan för CSMA. I rapporten ges också en översikt av arbeten som gjorts för att anpassa CSMA till att bättre hantera broadcast-trafik samt diskussioner kring huruvida dessa tekniker kan användas i aktuella taktiska scenarion. Utvärdering av prestandan för CSMA i taktiska ad hoc-nätverk har skett genom nätverkssimuleringar.

Utöver MAC-protkollet har även routingprotokollet och hur det kopplar till MAC-protokollet stor inverkan på förmågan att hantera broadcasttrafik i mobila ad hoc-nätverk. I simuleringarna används MPR-flooding (multipoint relay flooding), som är en del av OLSR (optimized link state routing) och vanligt förekommande protokoll för multicast- och broadcasttrafik i ad hoc-nätverk. Resultaten visar på att när MPR-flooding används i samband med CSMA uppstår problem med robusthet på grund av kollisioner. Dessa kollisioner påverkar även kontrolltrafiken som OLSR använder för att välja relänoder, vilket orsakar att fler paketkopior skickas som i sin tur leder till ytterligare kollisioner. Kapaciteten för broadcasttrafik i nätet blir därför kraftigt begränsad, på grund av kollisionerna och dessas påverkan på routingprotokollet.

Slutligen presenteras en jämförelse mellan CSMA och ett system baserat på ett fixt TDMA-protokoll (time division multiple access). Jämförelsen visar på att prestandan hos det CSMA-baserade systemet är sämre än för det TDMA-baserade systemet i alla undersökta fall, bortsett från när trafiklasten är väldigt låg eller nätet är mycket välförbundet.

Nyckelord: CSMA, OLSR, ad hoc-nät, multicast, broadcast

Contents

1 Introduction

Medium access control (MAC) protocols for mobile ad hoc networks (MANET) are typically divided into two classes: contention-free, such as time division multiple access (TDMA), and contention-based protocols, such as carrier sense multiple access (CSMA). In military applications, contention-free protocols are usually preferred due to their ability to provide quality of service (QoS) and predictable delay characteristics. Contention-based protocols, on the other hand, often lack ability to provide QoS and delay limits can rarely be guaranteed. The benefits of a contention-based MAC protocol, such as CSMA, is instead that it is flexible; nodes joining or leaving the network is handled automatically, for instance. Another advantage of CSMA compared to TDMA is that the demand for synchronization is typically more relaxed.

CSMA is a well-studied and broadly used protocol, owing to the fact that a version of CSMA called CSMA with collision avoidance (CSMA/CA) is part of the IEEE 802.11 standard for wireless local area networks. In this report we use the version of CSMA/CA, in 802.11 called distributed coordination function (DCF), as the basis for our evaluations as it is well defined. Much work has been presented showing CSMA to perform effectively for unicast traffic by using techniques such as channel reservation and automated repeat request (ARQ). For multicast traffic, on the other hand, these techniques cannot be used as they require the receiver to send acknowledgements, which becomes infeasible when there are multiple receivers. There is considerably less work available analysing multicast/broadcast performance of CSMA-based networks. Another shortcoming of many of the studies of CSMA performance is simplified channel models utilizing strictly distance dependent path loss. Under such assumptions, problems regarding carrier sensing distances and performance becomes too simplified to reflect realistic scenarios, especially in difficult terrains.

In this report, we present a performance analysis of CSMA for scenarios that are relevant to military applications; we focus on performance for broadcast traffic of packets of moderate size, using realistic channel models and physical layer assumptions. The assumed applications for these kind of scenarios are multicast voice applications and situation awareness messaging, i.e. applications requiring high reliability and low delays.

We start by presenting a brief overview of the CSMA protocol, as used in IEEE 802.11, and present some analytical performance bounds for multicast traffic to determine what the fundamental limitations of the protocol are in the specified scenario. An important aspect of efficient multicast in mobile ad hoc networks, aside from the MAC protocol, is the routing protocol. A popular network protocol for ad hoc networks is optimized link state routing (OLSR) which uses multi point relay (MPR) flooding for efficient distribution of multicast and broadcast traffic [1]. OLSR is often used on top of a scheduled MAC protocol, mostly an implementation of a TDMA-based MAC protocol. We analyse how certain performance metrics of OLSR are affected when it is used on top of CSMA rather than a scheduled MAC protocol. In the evaluation we show how protocol parameter setting affects the performance of the protocol and present robustness and capacity analyses for mobile networks under various traffic loads. The report is concluded with a discussion regarding protocol performance in the evaluated

scenarios and the applicability of CSMA-based protocols in military ad hoc networks focused on multicast traffic.

1.1 Related Work

CSMA is a well studied protocol due to its inclusion in the IEEE 802.11 standard. Much of the evaluations, however, mostly consider unicast traffic. Another aspect lacking in many studies is the use of a realistic channel model and its effect on the protocol performance, specially in terms of sensing performance. Usually, a purely distance-dependant path loss model is used. In this section we briefly comment on some works more closely related to what is evaluated in this report.

CSMA with OLSR

In [2], the performance of OLSR when used on top of the access scheme and physical layer defined in IEEE 802.11 is investigated using OPNET simulations. The paper focuses on comparing two versions of the OLSR protocol and their ability to handle high mobility. The results presented are, however, based on simple physical layer assumptions and are performed for short inter-node distances.

The broadcast performance of MPR flooding when used on top of a IEEE 802.11 stack is compared to a number of routing protocols in [3]. Using the two-ray ground reflection propagation model, which is a form of distance dependent disc model as there is no fading included, the different protocols are evaluated using the Network Simulator 2 (ns2). The results show that OLSR performs best out of the protocols presented, but still never manages to achieve a packet delivery ratio above 50% for the scenario studied.

Another study of broadcast performance of MPR flooding combined with IEEE 802.11 MAC is presented by the authors of [4]. The paper presents a new method for choosing MPR nodes in a robust manner and presents performance comparisons for the different methods. The evaluation is, however, very unclear and it is hard to tell if the simulated results are based on scenarios with only one source node.

Multicast Enhancements for CSMA

Some work has been done to improve the performance of CSMA for broadcast traffic. The authors of [5] presents a scheme for using request-to-send/clear-to-send (RTS/CTS) transmission for broadcast packets. The scheme consists of the transmitter sending an RTS packet before transmitting a broadcast packet and then wait for a CTS packet from at least one neighbour before transmitting the data packet. A similar approach is presented in [6] where the transmitting node chooses a so called collision detector responsible for sending the CTS packet. Common to both approaches is that the benefits they provide quickly diminish as the traffic increases due to the added overhead caused by the RTS/CTS exchange.

Another approach to reliable multicast when using CSMA is presented in [7] by

the name of early multicast collision detection for CSMA/CA (EMCD). In EMCD a second period of sensing is inserted a short time after the start of a transmission in order to detect collisions early. Collisions that are successfully detected early causes the channel to be occupied for a shorter time as compared to regular collisions. There is an added cost of adding a second sensing period and transmission lengths need to be long compared to the sensing time in order to keep the cost low. Another problem with this kind of approach is that the sensing is performed at the transmitting nodes while the collisions take place at the receiving node. For collisions to be avoided all nodes involved in the collision therefore needs to be able to sense each others' transmissions. This means that in a multi-hop scenario the sensing needs to be quite sensitive to be effective and would therefore be quite time-consuming.

2 Carrier Sense Multiple Access

In this chapter we present a description of the carrier sense multiple access (CSMA) protocol, as implemented in the IEEE 802.11 standard and note how the requirement of multicast traffic, typical in the military networks focused on in this report, affects the protocol. Following the protocol description is a theoretical analysis of capacity and robustness to provide an understanding of some fundamental performance bounds and to give a basis for how protocol parameters should be chosen.

2.1 Protocol Description

In this report we use an implementation of the CSMA protocol that is based on the widely used 802.11 standard for wireless local area networks (WLAN). Networks running 802.11 use Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) in one of two modes: Point Coordination Function (PCF) and Distributed Coordination Function (DCF). The PCF is a polling scheme with a designated access point while the DCF is fully distributed access scheme and therefore the access scheme we consider here.

The basic principle of CSMA is that a node that has data to transmit, first senses the channel for a given time to assess that the channel is clear, called Clear Channel Assessment (CCA). If the channel is sensed idle following a transmission, the node backs off for a random time interval called a *contention window*, before attempting to transmit. This is done in order to reduce the number of collisions at the time the channel becomes free which is when the risk of collision is greatest. In IEEE 802.11 time is divided in short time slots, called *backoff slots* and back-off is performed for an integer number of such slots. The backoff counter's initial value is uniformly distributed between [0,CW], CWmin $\leq$ CW $\leq$ CWmax, where CWmin and CWmax determines the minimum and maximum values possible for CW respectively and CW is the current contention window size. During each backoff slot a node waiting to transmit data shall perform a CCA and if the channel is determined idle, reduce its back-off counter by one. If the channel is sensed busy, the back-off procedure is suspended until the ongoing transmission has ended. After the reception of a frame a node waits a short time before the sensing is started called a DCF interframe space (DIFS).

The dominant traffic type in non-military wireless networks is unicast traffic, which is handled effectively in IEEE 802.11 networks by utilizing some additional collision avoidance techniques. The primary mechanic used for providing robust delivery of unicast packets in IEEE 802.11 is acknowledgements (ACKs) of received packets. All packets sent that are sufficiently long are acknowledged by the receiver and the sender can detect a failed transmission by the lack of an acknowledgement; a missing acknowledgement could, however, also be the result of the ACK packet colliding. Upon detecting a packet collision, packets are retransmitted and the contention window is increased, by increasing CW until it reaches CWmax, to reduce the risk of further collisions. After a successful transmission the contention window is reset to its initial size by setting CW equal to CWmin. Using acknowledgements enables a robust delivery of packets despite a moderate number of collisions. Another benefit of using acknowl-

edgements is that the contention window size can be adapted dynamically. This leads to short access times when there is little activity on the channel and increased collision avoidance during busy channel conditions.

In addition to using acknowledgements, channel reservation is typically used to reduce the number of collisions, more specifically by using request-to-send and clear-to-send principles. Before transmitting a long packet, a node transmits a request to send (RTS) packet. Upon reception of an RTS packet the intended receiver responds with a clear to send (CTS) packet. The RTS-CTS packet exchange improves the regular CSMA protocol in several aspects. Most prominently the use of RTS and CTS packets reduces the amount of channel resources lost due to collisions. When a collision occurs it will mostly involve RTS or CTS packets, which are much shorter than data packets, hence the channel is occupied a much shorter time during a collision. Also, for CTS packets a short interframe space (SIFS) is used, which is shorter than the DIFS, meaning that CTS packets will have higher priority than regular packets leading to a more robust channel reservation procedure. Another benefit of using RTS/CTS packets is that it mostly solves the so called hidden node problem. The hidden node problem can for instance occur when two nodes who are unable to sense each other causes collisions at an intermittent node able to hear both nodes. Since both the colliding nodes can sense the intermittent node the CTS packet will notify them about each other's transmissions.

When the traffic sent is of multicast or broadcast type, as is common in military networks, neither RTS-CTS exchange nor acknowledgements can be used effectively since there are multiple receivers. This means that the robustness is inherently much lower for this kind of traffic. It also means that the contention window cannot be adapted according to the success or failure of transmissions, as there is no feedback. Thus, the size of the contention window needs to be fixed and a proper value is assumed to be chosen upon initial configuration of the network. In the following analysis we establish what effects these limitations have on the robustness of the protocol and the capacity available, as well as how the contention window size should be chosen.

2.2 Analytical Capacity Limits

A lot of work has been done in terms of analysing the theoretical performance limits for the DCF in IEEE 802.11 in terms of capacity and collision probability. The typical assumptions used include a 1-hop network of n nodes, all of which are fully saturated, i.e., all nodes always have packets to transmit. For unicast traffic, with varying contention window size, a Markov chain can be used to model the contention window size, in order to calculate the probability that a node attempts to transmit in a certain slot, τ. In our case, with a fixed contention window size, it is shown in [8] that τ can easily be calculated as

$$\tau = \frac{2}{W+1}, \tag{2.1}$$

where W is the size of the contention window. In order to calculate the capacity we also need to know the average time it takes to transmit a packet, the average time a collision takes and the stationary probabilities of a slot being idle, a successful transmission

taking place and a collision occurring. A slot is idle if no node attempts to transmit, hence the probability of an idle slot is

$$P_i = (1-\tau)^n. \tag{2.2}$$

The probability of having at least one node transmitting, P_{tr}, in a slot then becomes

$$P_{tr} = 1 - P_i, \tag{2.3}$$

and the probability of a success, P_s, is the probability that only one node transmits, given that at least one node transmits

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} = \frac{n\tau(1-\tau)^{n-1}}{1-(1-\tau)^n}. \tag{2.4}$$

Using these probabilities, the capacity C, i.e. the proportion of the time the channel is used for sending payload data, can be calculated as

$$C = \frac{P_{tr}P_sE[P]}{(1-P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}(1-P_s)T_c}, \tag{2.5}$$

where $E[P]$ is the expected payload size, given in seconds, σ is the length of a backoff slot, T_s is the total time the channel is occupied by a successful transmission and T_c the time the channel is occupied during a collision. Assuming for a start that only one packet size is used, ignoring the fact that OLSR is transmitting HELLO packets which are typically much smaller than a data packet, and considering the fact that no acknowledgements are used for broadcast traffic, we have

$$T_c = T_s, \tag{2.6}$$

and (2.5) is then simplified to

$$C = \frac{P_{tr}P_sE[P]}{(1-P_{tr})\sigma + P_{tr}T_s}. \tag{2.7}$$

The time the channel is occupied during a transmission is

$$T_s = E[P] + H + \text{DIFS}, \tag{2.8}$$

where H is the total amount of header information sent, in seconds, and DIFS is the DCF Interframe Space. For simplicity we let H be equal to the preamble length, ignoring any additional physical header information such as packet size information, and we assume no rx-tx-turnaround time or mac processing delays. Under these simplifications we get

$$\text{DIFS} = 2\sigma. \tag{2.9}$$

Using (2.4) we can calculate the success rate for a 1-hop network for different contention window, W and network sizes. Assuming that packets are only lost during collsions, i.e. no packets are dropped due the link quality being too low, the success

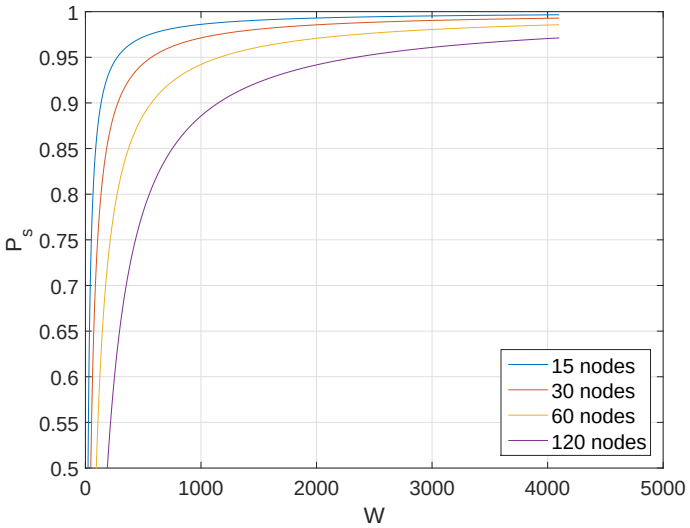


Figure 2.1: Analytically calculated robustness bounds versus contention window size for 1-hop networks of different size.

rate can be used as an upper bound on the robustness that can be achieved under full saturation. The resulting curves are shown in Figure 2.1 and looking at the figure we can make some observations. Achieving robust delivery of multicast traffic requires very large contention window sizes. Reaching above 90% for a 30 node network requires a window size of 280, while reaching a robustness of 95% for the same network size requires a window size of 570. For 60 nodes the corresponding window sizes are 570 and 1160, hence for 90% robustness we need a window size roughly 10 times the number of nodes and for 95% a window size roughly 20 times the number of nodes. Having a large contention window can still be fine though, capacity wise, as long as the backoff slot time σ is much smaller than the average packet length. It should be noted though that the channel access delay naturally increases as the contention window size is increased, leading to longer end-to-end delays.

In Figure 2.2 the maximum capacity as a function of the packet size, for a given robustness demand, is presented for a 30 node network. For the capacity estimates we have assumed a preamble length of 100 symbols and and CCA time corresponding to 50 symbols. We have also assumed that the sensing distance expected is 10 kilometers leading to a backoff slot time of 83 μs. From Figure 2.2 we can observe that in order to use the channel effectively the packet size needs to be large, in comparison to the slot time. With a robustness demand of 90 or 95%, a packet size of at least 5000 bits is needed, when the packet size is made smaller than that the capacity quickly diminishes. Requiring an even higher robustness of 99% delivery causes the capacity to become much lower, unless very large packet sizes are used. Using packets of 1000 bits, which is a reasonable size concerning the type of applications intended, means that the capacity drops right below 50% when requiring 90% reliability and at

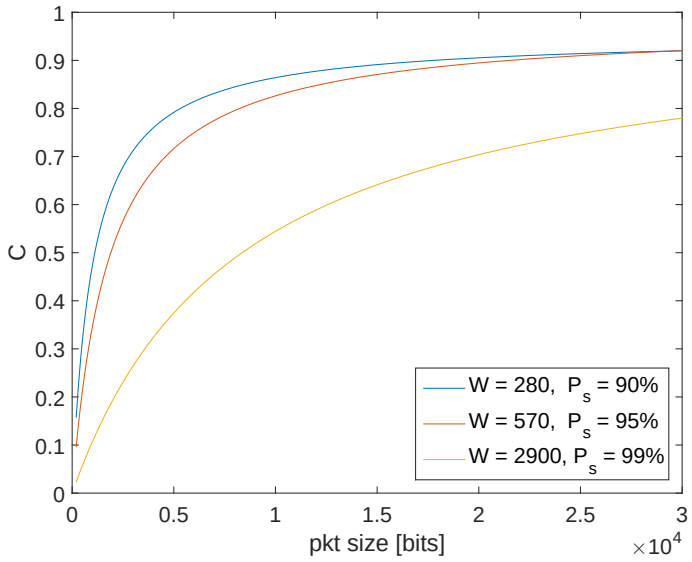


Figure 2.2: Capacity bound versus packet size for a 30 node network when the contention window size is set in order to guarantee 90, 95 and 99% delivery ratio respectively.

99% reliability only 10% of the channel capacity can be utilized. These numbers are estimates based on the assumptions laid out above but still provide some insight into what can be expected. Increasing the network size means that the contention window W needs to be increased, which would mean that even larger packets are needed to get a reasonable capacity. In Section 4.1.1 the theoretical performance bounds presented here are validated using network simulations.

2.3 Carrier Sensing Jamming Considerations

Without any additions to the protocol, CSMA is inherently easy to jam. The standard way of detecting whether or not the channel is busy, is by simple energy detection; if there is energy above a given threshold, the channel is considered busy. When a node senses that the channel is busy, the node defers its own transmission until the channel is sensed to be idle. As a jammer it is therefore sufficient to put out enough energy to trigger the energy detection to jam the network and put it on hold.

Common jamming protection alternatives usually consist of either Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping (FH). When DSSS is used for jamming protection, the sender and receiver use a common pseudo-random number (PN) sequence to spread the data symbols. The clear channel assessment is then performed by first attempting to despread the signal and then performing CCA on the resulting signal, either by energy detection or by correlation. This means that only signals generated using the correct PN sequence should trigger the the channel busy state. Other

energy in the form of noise or non-DSSS signals should not trigger the channel to be considered busy. A potential jammer would therefore need to acquire the correct chip rate and PN sequence used in order to effectively perform jamming of the carrier sensing mechanism. Without the correct PN sequence, jamming requires high power over a wide bandwidth. The main drawback with using DSSS is the need for synchronization at receiver side in order to be able to despread the signal and perform the carrier sensing. One of the main benefits of using CSMA over TDMA are the relaxed demands for synchronization. Adding DSSS to a protocol stack using CSMA practically removes that advantage. How fast PN sequence synchronization can be achieved largely determines the impact DSSS has on CSMA performance, in terms of increasing the channel sensing time required.

For of frequency hopping, jamming protection is provided by hopping over a large bandwidth, in a pattern unknown to a potential jammer. Carrier sensing is then performed on a sub-band basis, requiring hop pattern synchronization. Implementations of frequency hopping might require each hop being started with a preamble, for synchronization and channel equalization. The impact of FH on the channel utilization is mainly affected by how short the preamble can be kept, as this is an added cost, compared to a fixed frequency system. Another aspect of FH that lowers the efficiency is the fact that the frequency hops have a fixed length; a transmission needs to start a certain time before the end of a frequency hop, to allow at least the preamble to be sent before the end of the hop in order for the transmission to be meaningful. If a node wants to start a transmission past this point it still needs to send some form of busy signal during the end of the frequency hop to prevent other nodes from, erroneously, reducing their back-off counters.

Whether DSSS or FH is used, access to a large bandwidth over which the the signals are spread, is required. If a large enough bandwidth is not available, neither DSSS or FH will provide protection to the carrier sensing mechanism of CSMA and it is therefore not a robust alternative. The main impact of adding DSSS or FH on the CSMA protocol performance is a reduced capacity due to increased overhead, in the form of additional preambles, and an increased need for synchronization. Thus, if the main motivation for using CSMA over TDMA is to lower the need for synchronization, any need for jamming protection will make such benefits of CSMA become insignificant.

3 Simulation Setup

To evaluate the broadcast performance of CSMA-based tactical ad hoc networks we perform network simulations. The aim of the simulations is to assess how CSMA performs when realistic physical layer and channel models are used. In this chapter we present models and assumptions used on the different levels of the simulated protocol stack.

3.1 Traffic Model

The focus of the evaluation is to assess how well CSMA handles traffic common in tactical ad hoc networks. The traffic type focused on is therefore broadcast traffic of moderately sized packets, which is meant to model applications such as situation awareness information. The traffic source used in the evaluation is a standard Poisson traffic source. Packets are generated according to a Poisson process and the transmitting node is randomly chosen for each packet.

3.2 MPR Flooding

For routing we use the multi point relay (MPR) method according to the simplified multicast forwarding (SMF) framework [9] and the MPR selection mechanisms in Optimized Link State Routing protocol (OLSR). OLSR is a commonly used network protocol for ad hoc networks. In OLSR, hello messages are used to disseminate neighbourhood information. Using the neighbourhood information, nodes choose Multi Point Relay (MPR) nodes that are responsible for forwarding broadcast and multicast traffic to reduce retransmissions. Details about the OLSR protocol and the algorithms for choosing MPRs used in this report can be found in the RFC [1].

3.3 Physical Layer Modelling

The channel sensing is an essential part of making CSMA work properly and should be modelled well. Physical channel sensing is performed by two functions: preamble detection and energy detection. Preamble detection is performed by correlating the received signal to a known preamble sequence called a *PLCP preamble* (physical layer convergence protocol). THe PLCP preamble is used both for detection and for synchronization. In order to be able to sense packets for which the preamble is not detected, for instance if there is a collision during the preamble sequence, energy detection is also used. The energy detection consists of comparing the total energy on the channel to a given threshold.

We assume here that all packets sent start with a preamble sequence used for signal detection and synchronization. Furthermore, the preamble used is assumed to consist of 100 symbols, which is a number that depends on the implementation of the physical layer but should be somewhere around that length. As long as the radio is not transmitting or receiving the correlators are continuously looking for preambles.

Preamble detection is typically performed using matched filters tuned for the preamble sequence used and does therefore provide a processing gain, as compared to energy detection. A preamble length of 100 symbols gives a processing gain of roughly 20 dB, compared to energy detection assuming the energy detection is performed on fewer symbols than the preamble detection. The chosen values are based on the 802.11 standard [10, pp. 525, 618] in which CCA thresholds given, state that a CCA performed on preambles should have a sensitivty 20 dB better than if CCA is performed on random data.

3.4 Channel Model

The path-gains between the nodes are modeled using the propagation library DetVag90® which utilizes a uniform geometrical theory of diffraction (UTD) model by Holm [11]. The path-gain calculations are performed for a terrain-profile contained in a digital database with a resolution of 50 meters. The terrains used are flat and hilly rural terrain and the carrier frequency is assumed to be 300 MHz. The bandwidth is set to 1 MHz and the spectral efficiency is set to 1 bit/s/Hz meaning that the total data rate is 1 Mbit/s.

3.5 Scenario

In the evaluations a 30 node network is considered. For the verifications of the theoretical results a static network is used while for the capacity evaluations mobility is included. Two terrains are used in the evaluations, one flat and one hilly rural terrain. In all simulations the node density is kept at 1 node/km^2 and the speed of the nodes in the mobile scenarios is set to 36 km/h.

3.6 Summary of System Parameters

The system parameters that are used for the simulation are summarised in Table 3.1. The PLCP detection threshold is the signal to noise ratio (SNR) threshold that the PLCP detection process needs to pass in order to flag the channel as busy. The decoding threshold is the SNR needed to be able to decode packets. The PLCP preamble length is the length of the preamble used and the CCA time is amount of time that energy detection is performed, given in seconds. The propagation delay is the additional time added to the length of the backoff slots to account from delays from nodes on the maximum sensing distance. The maximum sensing distance in the simulations is assumed to be 10 km which leads to the chosen value of 33 μs.

Table 3.1: System parameters

Parameter	Value
Number of nodes	30
Node density	1 node/km^2
Node speed	36 km/h
Geographic area	Flat or hilly rural
Bandwidth	1 MHz
Contention window, W	512
Packet size	1024, 4096
PLCP detection threshold	-10 dB
Decoding threshold	10 dB
PLCP preamble length	100 μs
CCA time	10 μs
Propagation delay	33 μs

4 Results

In this section we aim to quantify how a tactical ad hoc network based on CSMA perform when used for sending broadcast traffic. To start with, the analytical results presented in Section 2.2 are verified by simulating a static 1-hop network. For the 1-hop network we continue to examine the how the sensitivity of the physical sensing affects the protocol performance. We then continue with mobile networks to present what capacity and robustness can be achieved in a realistic scenario. Finally, to put the results into a context we compare the results of using CSMA to the performance that can be achieved using a fixed TDMA protocol

4.1 Static 1-hop Network

We start by investigating network performance and the impact of essential protocol parameters in a static network. As there is no mobility, and therefore more stable links, effects of certain protocol parameters become easier to distinguish.

4.1.1 Validation of Theoretical Bounds

To validate how accurate the estimated capacity and robustness bounds are, we have simulated a 30 node 1-hop network in a rural terrain. By 1-hop network we mean that all nodes are able to receive packets from all other nodes. So far, in all calculations we have assumed no HELLO messages and fully saturated nodes. In the simulations we present results both with short HELLO messages turned off and with HELLO messages being sent every 2 seconds, as is default in OLSR. In our simulations we use a Poisson traffic source, which is not the exact same thing as all nodes being fully saturated since the traffic load is spread out among the nodes in a random fashion. The results of the simulations are shown in Figure 4.1 where the packet delivery ratio is shown for varying input traffic loads, and a data packet size of 4096 bits. The input traffic load is presented as the fraction of the total channel capacity, G. It can be seen that when no HELLO packets are transmitted, and nodes just send packets to their 1-hop neighbours, the system delivers more than 90% of the packets for input traffic loads up to a fraction of 0.8 of the total channel capacity available. According to the theoretical calculation, given a window size of 512 slots as used in the simulation, the robustness should be close to 95 % and the capacity 0.77. The simulated performance is slightly lower than the theoretical bound but reasonably close.

When the OLSR protocol is configured to send HELLO messages every 2 seconds the capacity is greatly reduced. There are a couple of explanations to the low capacity experienced when OLSR is being used, even though all nodes are 1-hop neighbours. To begin with, the HELLO packets sent are much smaller than the data packets, for the network considered here they are on average around 330 bits, when short addresses are used see [12], comapred to 1024 or 4096 bits. As considered previously, small packets are not handled effectively using this kind of protocol. Additionally, when there is a mix of small and large packets being sent, as is the case here, the time the channel is occupied during a collision becomes a bit more complex to estimate. During

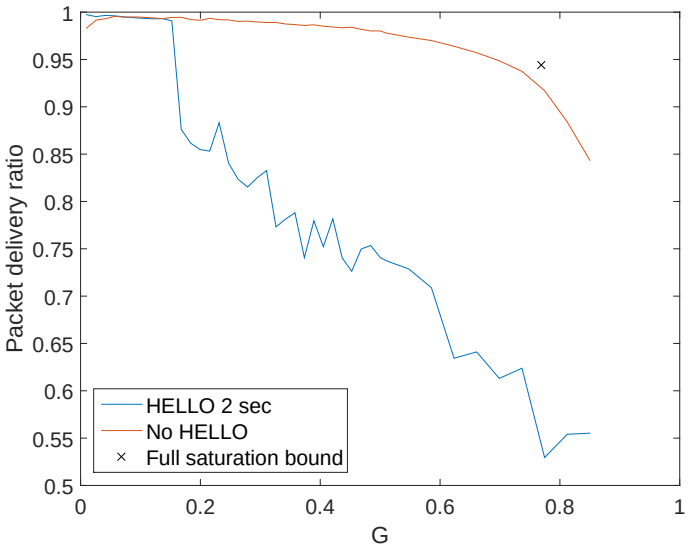


Figure 4.1: Packet delivery ratio versus input load, G, for a 1-hop 30 node network and the impact of sending HELLO messages. The calculated theoretical capacity with 90% robustness, given the used input parameters, is also shown for reference.

a collision, the time the channel is seen as busy is determined by the largest packet involved in the collision. This means that when a data packet and a HELLO packet collides, the channel will be busy for the entire duration of the data packet. To sum up, by sending HELLO packets in addition to data packets the effective packet size of delivered packets is reduced but the time the channel is busy during collisions is not reduced as much as it is determined by the largest packet involved.

The second and most important explanation to the quick drop in packet delivery ratio seen when HELLO packets are used, stems from the neighbourhood management of OLSR. A node determines its 1-hop and 2-hop neighbours based on the HELLO messages it receives. When a node does not receive any HELLO messages from a node during a time, the link to that node will be considered broken. As soon as a node considers there are nodes who are not 1-hop neighbours it will start choosing multi point relay (MPR) nodes in order to reach those nodes. This means that as soon as HELLO packets fail to deliver, due to collisions, the number of MPRs will increase and so will the number of retransmissions. This behaviour causes a cascading effect, in a way that CSMA reduces the performance of OLSR, which in turn reduces the performance of CSMA, ultimately leading to very unstable behaviour. This effects can be seen in Figure 4.1 where the packet delivery ratio (PDR) quickly drops at an input load between 15 and 20% of the total channel capacity. By inspecting the average number of neighbours, as perceived by the OLSR protocol, and the average number of MPRs chosen, see Figure 4.2, we can see that the number of neighbours drop and the number of MPRs increase at the same input traffic load at which the PDR drops.

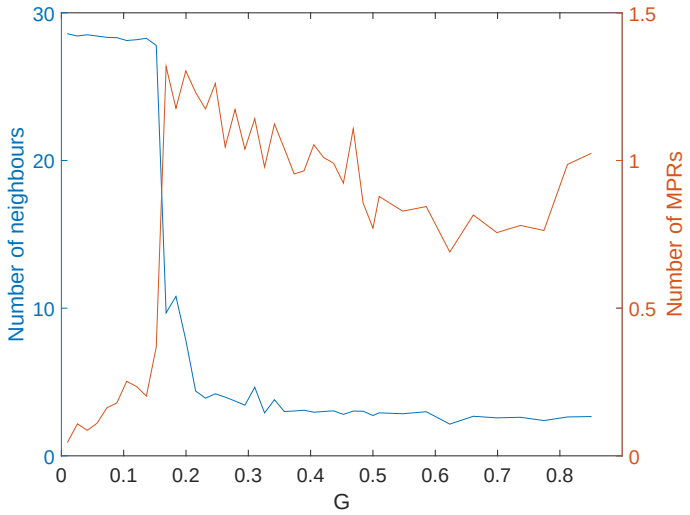


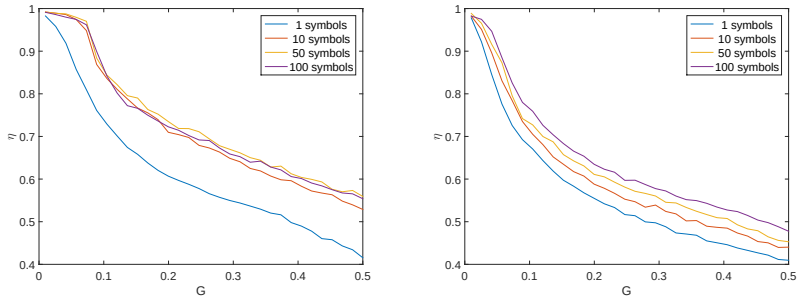
Figure 4.2: The average number of 1-hop neighbours as perceived by the OLSR protocol and the average number of MPRs chosen for a 30 node, 1-hop network under varying input traffic load, G.

4.1.2 Channel Sensing

The length of the backoff slots used in CSMA is determined by a number of factors: the time it takes for the radio to switch from transmitting to receiving, processing delays, clear channel assessment (CCA) time and propagation delay. The parameters of interest here are the CCA time, which is the time that is used to perform energy detection, and the propagation delay that is accounted for. The CCA time reflects how long time is needed in the energy detection to make an accurate clear channel assessment. The propagation delay accounted for determines the sensing distance.

To maximize the performance of CSMA, the length of the backoff slots should be kept as short as possible since the length of the backoff slots directly determines the amount of time the channel is idle due to nodes backing off. When there are a lot of nodes and high traffic loads, a large contention window is preferable to reduce the number of collisions and the backoff slot length becomes even more crucial. The propagation delay needs to be large enough, so that a node listens for long enough time such that it can sense transmissions from all nodes within detection range.

Determining the CCA time requires balancing sensing time versus sensitivity. Using a longer sensing time means more samples are averaged during the energy detection, leading to a better sensitivity. On the other hand, a long sensing time leads to long slot times which in turn lowers the efficiency in the network. Shortening the CCA detection time to only a few symbols reduces the slot time but also reduces the sensitivity of the energy detection. This could mean that the slot time becomes shorter than the PLCP preamble length, which is the time needed to do carrier sensing based on PLCP preamble detection. If the CCA then is too insensitive, nodes will reduce their backoff



(a) -10 dB (b) 5 dB

Figure 4.3: PDR, η, at different input traffic loads for a PLCP preamble detection threshold of -10 dB (a) and 5 dB (b). Decoding threshold of 10 dB common for both figures and varying length of the CCA time, shown in legend in terms of number of symbols.

counters incorrectly which increases the risk of collisions.

We model the sensitivity of the energy detection CCA by relating it to the PLCP preamble length. In our simulations we assume a physical preamble of 100 symbols, which is equal to 100μs with 1 MHz bandwidth, is used for signal detection and synchronization. Preamble detection is usually performed by matched filtering which provides a processing gain proportional to the length of the preamble sequence compared to simple energy detection of a single sample. Using a CCA time of one symbol (1μs) would therefore incur a sensitivity loss of 20 dB compared to the preamble detection of a 100 symbols long preamble, but with a much shorter detection time. In our simulations we model the CCA sensitivity to be a factor K_{CCA}

$$K_{\text{CCA}} = \frac{\text{preamble length}}{\text{CCA time}} \tag{4.1}$$

above the preamble detection threshold, which is probably a bit optimistic. In Figure 4.3 the impact of using different values for CCA time is shown for a 1-hop network of 30 nodes. Figure 4.3a shows the PDR for varying CCA length, given in number of symbols, and a preamble detection threshold of -10 dB. The results show that a significant performance gain is achieved when the CCA detection is based on more than one symbol, however, increasing the CCA time beyond 10 symbols (10 μs) provides practically no gain. Comparing Figure 4.3a and Figure 4.3b shows two things: when preamble detection threshold is increased, the overall performance decreases quite significantly and in that case increasing the CCA detection time makes less of an impact. In both of the cases shown the decoding threshold is set to 10 dB.

4.2 Mobile Network

In this section the capacity of a CSMA-based system is evaluated for mobile networks in order to asses the impact of mobility on the system performance. When mobile

networks are considered the choice of MPR nodes plays an important role in respect to the capacity that can be achieved. When using CSMA, the HELLO messages of the OLSR protocol competes with data packets for the channel resources and in these simulations we asses how this affects the performance in mobile scenarios.

Further, the performance of the CSMA-based system is compared to a simple TDMA-based system. The TDMA based system does not use any traffic adaptivity methods and can be seen as a baseline system.

4.2.1 Capacity

The term capacity used here refers to the fraction of the total available channel data rate that can be used to transmit data from an application. The actual amount of input traffic that can be handled is determined by the robustness and end-to-end delay demands of intended applications. In this section we focus on the robustness and the end-to-end delay is handled in the following section. To visualize the relationship between robustness and capacity, the capacity is shown as the packet delivery ratio (PDR) for different network connectivity levels and input traffic load. The capacity for a given application is then given by the maximum input traffic load that is delivered with a PDR above a threshold given by the application in question.

The capacity for a CSMA-based system of given network size is primarily determined by two factors: the node density and the packet size. The more sparse the network becomes the more MPR nodes are chosen and therefore the number of retransmissions increase. As the number of retransmissions increase so does the risk of collisions. When the packets are made longer the capacity increases, as was discussed in Section 2.2.

An overview of the capacity of CSMA is given by Figure 4.4 which shows the packet delivery ratio (PDR) at varying connectivity and input traffic load when 4 kbit packets are used, in a flat rural terrain. The connectivity is shown on the y-axis in the form of the average number of neighbours and the input traffic load is shown on the x-axis. As can be seen in Figure 4.4, close to 200 kbit/s input traffic load is handled in a robust manner (PDR close to 1) if the network is very well connected (more than 26 neighbours on average, of the total of 30 nodes). As the network becomes more sparse, only input traffic loads below 50 kbit/s are handled in a robust manner.

To illustrate the impact of varying the packet size, a similar overview but for 1 kbit long packets is shown in Figure 4.5. When the packet size is decreased, the most obvious effect is that the maximum input traffic load that can be handled is reduced, most prominently at higher connectivity levels, as seen by comparing the size of the yellow areas in the two figures.

4.2.2 Comparison to TDMA

To put the capacity results for CSMA in to some perspective, in this section the capacity is compared to the capacity that can be achieved with TDMA-based system. The TDMA system used as reference replaces CSMA with a fixed TDMA schedule on the MAC layer. For the TDMA system, the HELLO messages of OLSR are sent in

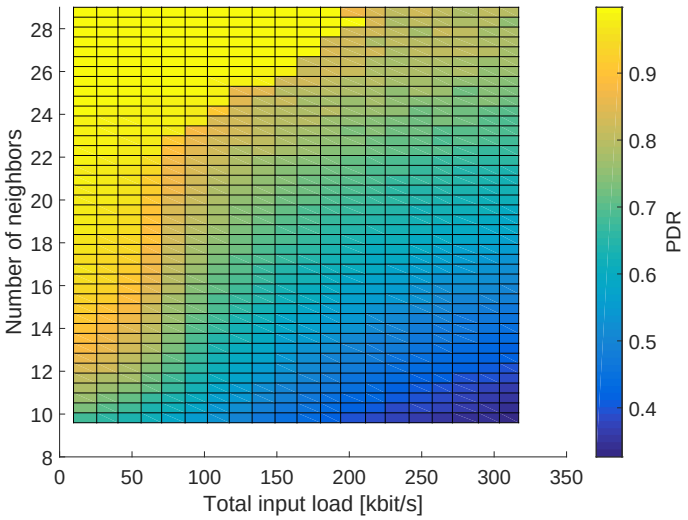


Figure 4.4: Packet delivery ratio as a function of total input traffic load and the average number of neighbours. Packet size used is 4096 bits.

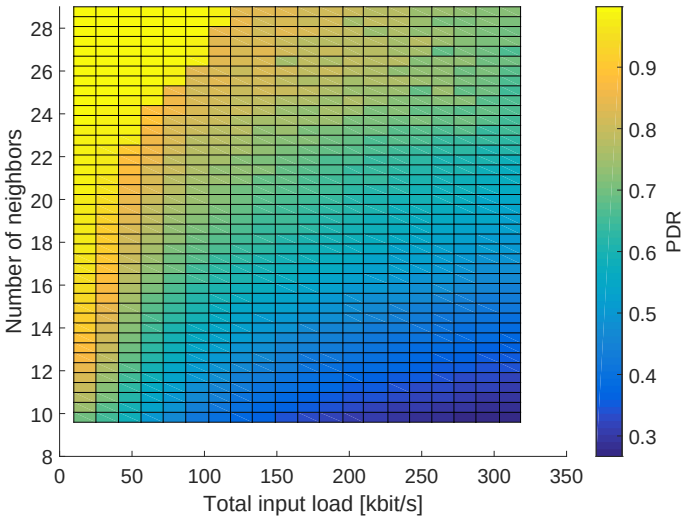


Figure 4.5: Packet delivery ratio as a function of total input traffic load and the average number of neighbours. Packet size used is 1024 bits.

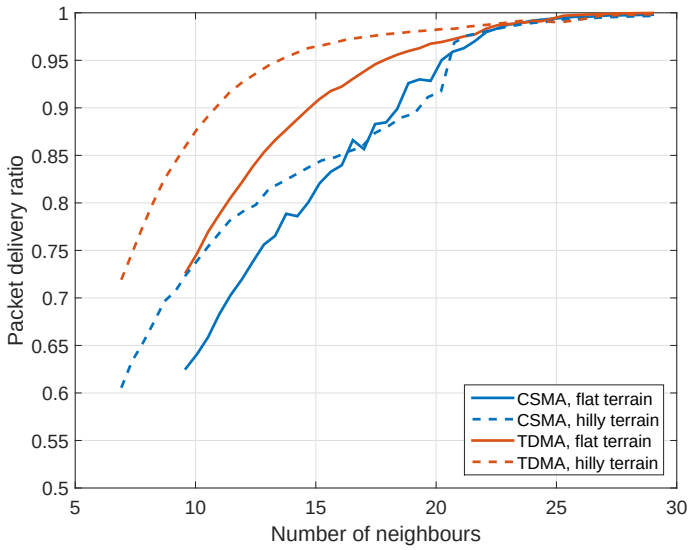


Figure 4.6: Packet delivery ratio comparison. Total input traffic load is 50 kbit/s and packet size is 1024 bits.

administrative time slots devoted to control traffic. Separating the access mechanisms for control and data traffic provides a significant performance gain of a TDMA system compared to a CSMA system; increasing the input traffic load does thereby not hamper the delivery of administrative traffic critical for the functionality of the routing protocol. The simulations have been performed for two rural terrain types: one flat and one hilly terrain. Two terrains are included to verify that effects seen are not tied to a specific terrain, rather than to compare the perfomance between the two terrains.

At low traffic loads the performance of CSMA and TDMA does not differ by much as long as the network is quite well connected, as can be seen in Figure 4.6. The figure presents the packet delivery ratio (PDR) for CSMA and TDMA respectively at a total input traffic load of 50 kbit/s, which corresponds to a capacity of 5%. The performance for CSMA differs less between the two terrains than it does for TDMA, though the decrease for CSMA is somewhat sharper in the hilly terrain.

As the input traffic level is increased to 100 kbit/s, the risk of collisions when using CSMA increases, both for data packets and for OLSR HELLO messages. The effects of increasing numbers of collisions can be observed in Figure 4.7. At high connectivity levels CSMA performs on par or better than the TDMA-based system but as the network starts becoming more sparse, at about 24 neighbours on average in the flat terrain and 26 in the hilly terrain, the PDR for CSMA quickly decreases. The sharp decrease in PDR echoes the results presented in Section 4.1.1 where it was shown for the static network that as collisions starts to accumulate, more and more MPR nodes are chosen leading to even more collisions. The PDR for the TDMA-based system also start to decrease as the network becomes more sparse but the decrease is more linear, since the HELLO messages are not affected by the increased data traffic load,

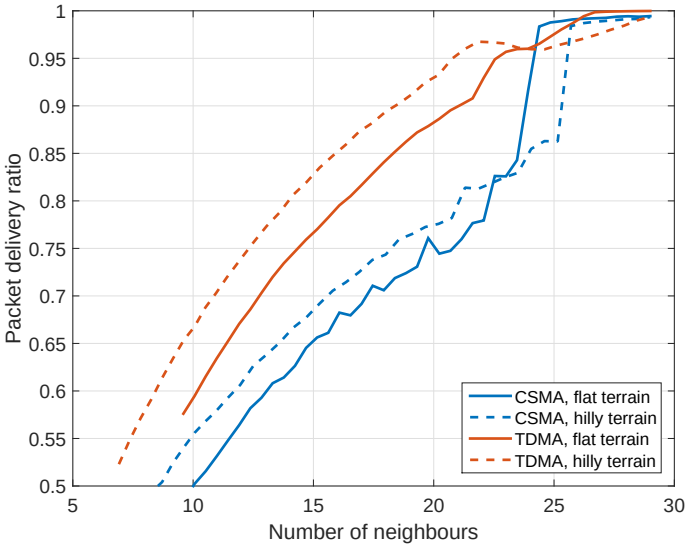


Figure 4.7: Packet delivery ratio comparison. Total input traffic load is 100 kbit/s and packet size is 1024 bits.

as described above.

Finally when the traffic is increased even further to 200 kbit/s, corresponding to channel usage of 20%, the CSMA-based system collapses even in the most dense networks, never reaching a PDR above 90%, see Figure 4.8. The TDMA system, while only delivering a PDR above 95% in the most dense networks, at least delivers the traffic as the network becomes well connected.

It was shown analytically in Section 2.2 how the capacity increases for CSMA as the packet size increase. Figure 4.9 shows that for low traffic loads there is very little difference in performance between CSMA and TDMA when the packet size is increased fourfold to 4096 bits. The performance increases for both CSMA and TDMA, though the increase is larger for CSMA. At an input traffic load of 100 kbit/s the effect of the increased packet size is that the connectivity regime in which CSMA delivers a PDR close to one increases, however, there is still the behaviour of a sharp drop in PDR for CSMA, though at a lower connectivity level (Figure 4.10). There is a significant difference in performance at 200 kbit/s when the packet size is increased, which can be seen by comparing Figure 4.11 to Figure 4.8, as the PDR for CSMA now reaches close to one in the well connected networks. When the input traffic is increased further to 300 kbit/s, Figure 4.12, CSMA starts to collapse.

To summarize, the results show that the packet size used affects the capacity and CSMA especially benefits from large packet sizes. Compared to simple TDMA solution, CSMA is able to perform on par with TDMA at low traffic input loads in well-connected networks. When the traffic is increased or the network becoms sparse, however, CSMA tends to collapse.

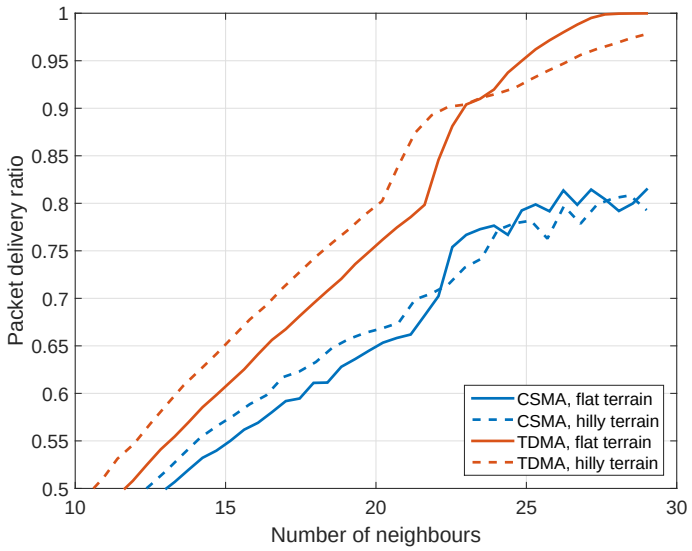


Figure 4.8: Packet delivery ratio comparison. Total input traffic load is 200 kbit/s and packet size is 1024 bits.

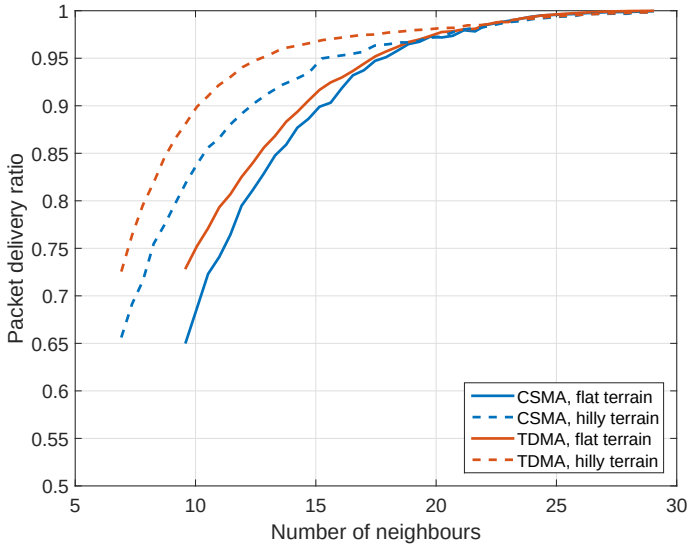


Figure 4.9: Packet delivery ratio comparison. Total input traffic load is 50 kbit/s and packet size is 4096 bits.

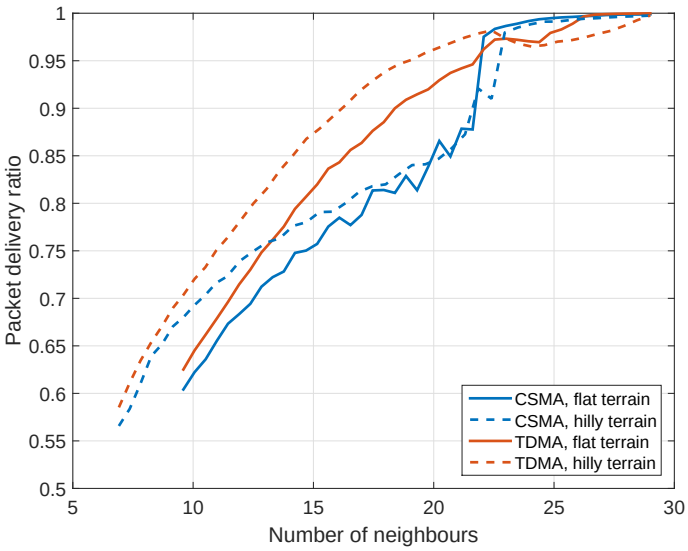


Figure 4.10: Packet delivery ratio comparison. Total input traffic load is 100 kbit/s and packet size is 4096 bits.

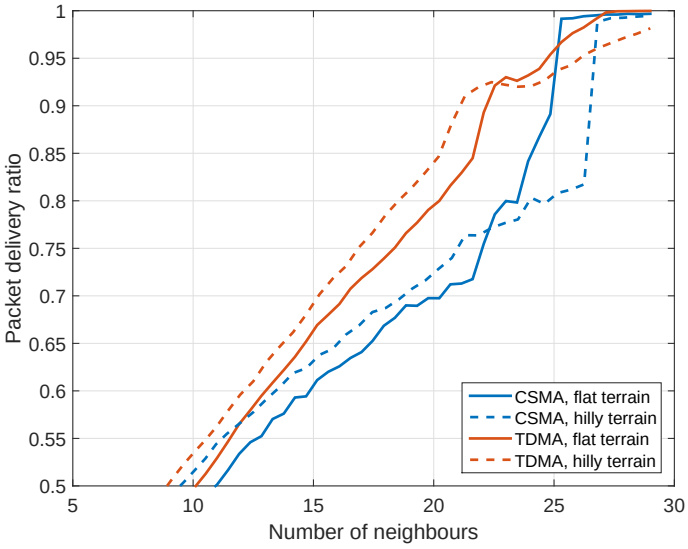


Figure 4.11: Packet delivery ratio comparison. Total input traffic load is 200 kbit/s and packet size is 4096 bits.

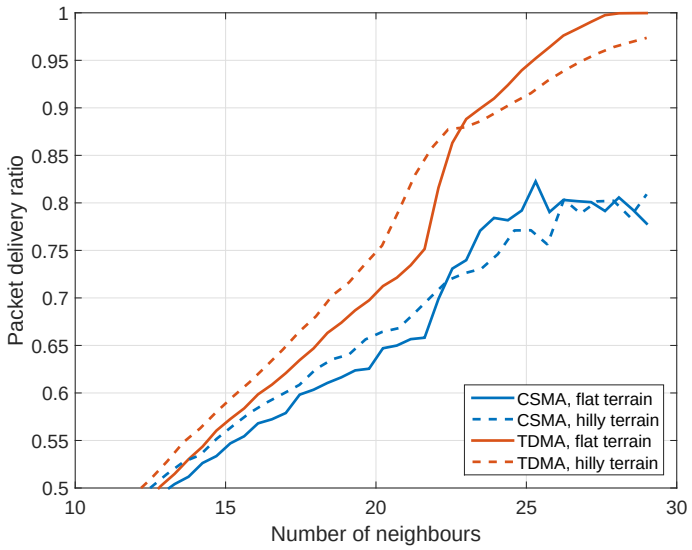


Figure 4.12: Packet delivery ratio comparison. Total input traffic load is 300 kbit/s and packet size is 4096 bits.

4.2.3 End-to-end Delay

Up to this point only robustness, in terms of packet delivery ratios, have been considered for the mobile network evaluations. Another performance metric which is important in military ad hoc networks is the end-to-end delay. A system which is robust but delivers packets with high end-to-end delays is only useful for a limited number of applications, such as file transfers. Connected to the end-to-end delay is the notion of quality of service (QoS), which can be described as guaranteeing that certain application-specific data rate and delay limits are met.

At low input traffic loads, the end-to-end delays are very short and even slightly shorter for CSMA than the TDMA-based solution, see Figure 4.13 which shows a comparison of the delay at 50 kbit/s input traffic load. When the traffic load is increased to 100 kbit/s, Figure 4.14 the two systems start to show different delay behaviours; at high connectivity levels both systems provide short delays but as the average number of neighbours starts decreasing the delay for CSMA quickly peaks to around 40 seconds on average and then gradually decreases. The TDMA-based system on the other hand shows a close to linear increase in delay when the average number of neighbours decrease below 25. Reviewing the PDR results in Figure 4.7 shows that the sharp increase in delay for CSMA, around 25 neighbours on average, happens when the PDR quickly starts to drop and the decreasing delay for CSMA afterwards is due to the low number of packets that are delivered when the connectivity is further decreased. The packets that do get delivered are most likely the ones received in a single hop which would lead to decreased delays.

When the input traffic was increased to 200 kbit/s with a packet size of 1 kbit, it was

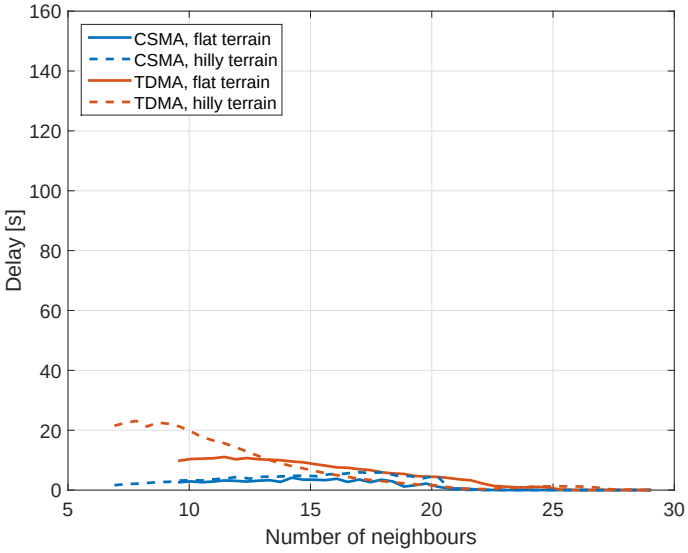


Figure 4.13: End-to-end delay comparison. Total input traffic load is 50 kbit/s and packet size is 1024 bits.

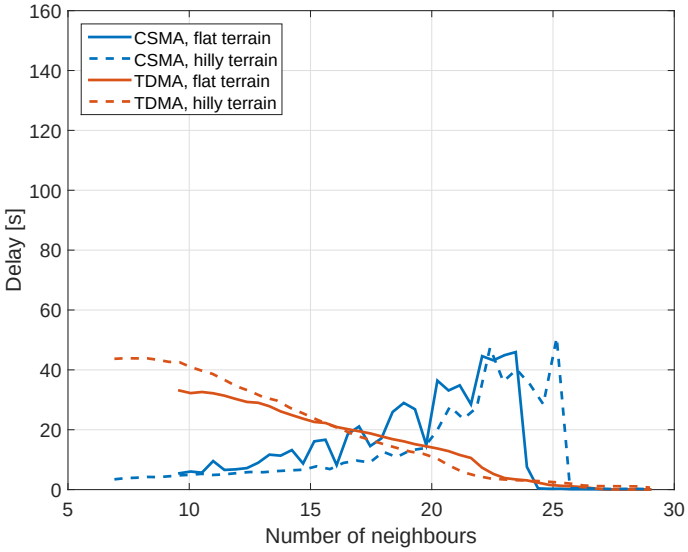


Figure 4.14: End-to-end delay comparison. Total input traffic load is 100 kbit/s and packet size is 1024 bits.

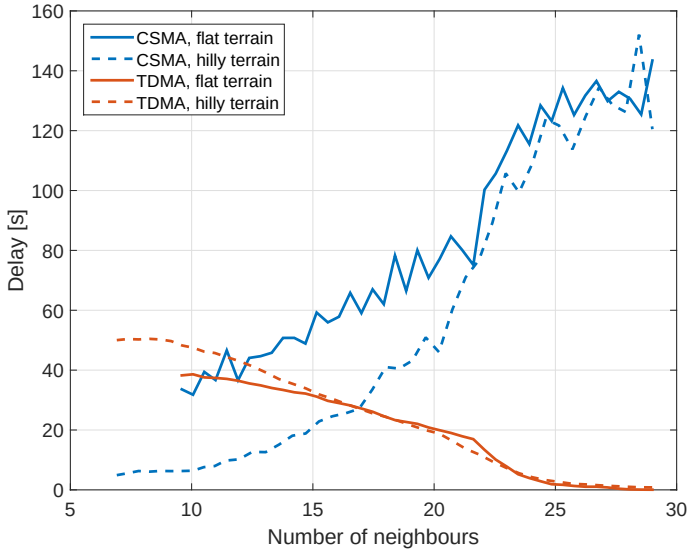


Figure 4.15: End-to-end delay comparison. Total input traffic load is 200 kbit/s and packet size is 1024 bits.

shown in Figure 4.8 that CSMA collapsed, and it becomes clear looking at the delay as well. As shown in Figure 4.15, even at the highest connectivity levels, the packets that are successfully delivered have an average end-to-end delay of roughly 140 seconds. As seen at lower traffic loads, the delay then starts to decrease as the PDR decreases at lower connectivity levels.

5 Conclusions

In this report we have analysed the suitability of using CSMA for broadcast in military ad hoc networks. More precisely we have evaluated the actual performance achieved when realistic channel models and sensing assumptions are used. We have started by defining the limiting factors, such as packet size and contention window length. The following are the most important conclusions that can be drawn from the results.

CSMA and MPR flooding does not work well together under heavy traffic load. Collisions on the MAC layer causes OLSR to choose more MPRs, which in turn leads to an increased number of collisions. Another problem with using OLSR on top of a CSMA protocol is the small size of the HELLO packets sent by the OLSR protocol. Small packets generally make CSMA perform bad since much time will be spent in back-off in respect to the time transmitting; however, collisions are also shorter meaning less channel capacity is lost during a collision. A mix of small control packets and large data packets is not optimal either as the small control packets means that the average utilization is lowered since they do not carry data; additionally, during a collision the channel will be seen as busy for the duration of the longest packet involved in the collision.

In order to make CSMA efficient, the packet sizes needs to be large in comparison to the backoff slot time used by CSMA. The length of the backoff slot time is determined by the CCA detector and the propagation delay that is accounted for during carrier sensing. Shortening the CCA detection time to only a few symbols reduces the backoff slot time but also reduces the sensitivity of the energy detection. This could mean that the slot time becomes shorter than the PLCP preamble length, which is the time needed to do carrier sensing based on PLCP preamble detection. If the CCA then is too insensitive, nodes will reduce their backoff counters incorrectly which increases the risk of collisions. On the other hand, if a very sensitive CCA energy detector is used, i.e, it averages over many symbols, the backoff slot times become rather long and in order to make the system efficient large packet size are needed. Very large packets may not be the primary type of data sent in military ad hoc networks, however.

Due to the lack of acknowledgements and RTS/CTS messages CSMA is inherently unreliable at transporting multicast traffic. In order to provide reliable communications, collisions need to be minimized which translates to using large contention windows. The downside of using large contention windows is that the channel access delay, and therefore the end-to-end delay also increases. Long delays is another feature that is commonly unwanted in military applications.

Broadcast traffic with CSMA was compared to using a static TDMA protocol. The comparison showed that CSMA is less robust in all cases except for very dense networks when the traffic load is moderately low. As static TDMA is a very simple solution with no traffic adaptivity it is hard to recommend using CSMA over TDMA for these kinds of applications. CSMA works best with very large packets which would more likely relate to video streaming or file transfer. But the inherent lack of robustness and inability to guarantee QoS makes CSMA unsuitable also for these kinds of applications as they typically require very high PDR.

In order for CSMA to be used in military networks at all, jamming protection is

needed to protect the carrier sensing. If there is not enough bandwidth available for DSSS or frequency hop, simply putting out energy on the channel will cause the network to stall. The absolute need for jamming protection in the scenarios we consider also means that precise synchronization is needed; generally the fact that CSMA does not need precise synchronization is held as one of the benefits compared to TDMA. The results presented in the report are based on simulations without any jamming protection. Adding jamming protection reduces the available capacity further, due to an increased need for preambles, meaning the results presented here are optimistic, compared to a real system using DSSS or FH.

Another beneficial property of CSMA is the fact that the protocol in itself is very robust towards mobility. However, for the applications considered in military ad hoc networks, where multicast traffic is dominant, this property is rendered negligible due to routing issues. In this evaluation we have used the common choice of MPR flooding and in practice the mobility robustness will be limited by the MPR flooding algorithm, rather than CSMA itself.

The main result from the study is that CSMA is not suitable for the kind of scenario examined in this report: broadcast of small packets in tactical, mobile ad hoc networks. The main reason is that many of the features that make CSMA effective for unicast traffic cannot be used for broadcast traffic, such as RTS/CTS and acknowledgements. Another important reason is that the routing of broadcast traffic relies on robust delivery of network layer control packets, such as HELLO messages of OLSR, which cannot be guaranteed with a contention-based protocol such as CSMA.

References

[1] T. Clausen and P. Jacquet (Editors). Optimized link state routing protocol (OLSR). In *IETF, Request for Comments 3626*, Oct 2003.

[2] Hakim Badis and Khaldoun Al Agha. Scalable model for the simulation of OLSR and Fast-OLSR protocols. In *IFIP Med-Hoc-Net*, page 12pp., Mahdia, Tunisia, Tunisia, June 2003.

[3] T.H. Clausen, L. Viennot, T. Olesen, and N. Larsen. Investigating data broadcast performance in mobile ad-hoc networks. In *Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on*, volume 2, pages 786–790 vol.2, Oct 2002.

[4] Ji Hyoung Ahn and Tae-Jin Lee. Multipoint relay selection for robust broadcast in ad hoc networks. *Ad Hoc Networks*, 17:82 – 97, 2014.

[5] Ken Tang and M. Gerla. Mac layer broadcast support in 802.11 wireless networks. In *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, volume 1, pages 544–548 vol.1, 2000.

[6] J. Tourrilhes. Robust broadcast: improving the reliability of broadcast transmissions on CSMA/CA. In *Personal, Indoor and Mobile Radio Communications, 1998. The Ninth IEEE International Symposium on*, volume 3, pages 1111–1115 vol.3, Sep 1998.

[7] T. Nilsson, G. Wikstrand, and J. Eriksson. Early multicast collision detection in CSMA/CA networks. In *Mobile and Wireless Communications Network, 2002. 4th International Workshop on*, pages 294–298, 2002.

[8] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *Selected Areas in Communications, IEEE Journal on*, 18(3):535–547, March 2000.

[9] J. Macker. Simplified multicast forwarding (SMF). Internet-draft, IETF, Network Working Group, January 2012.

[10] Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages 1–1076, June 2007.

[11] P. D. Holm. UTD-diffraction coefficients for higher order wedge diffracted fields. *IEEE Trans. Antennas Propagat.*, AP-44(6):879–888, June 1996.

[12] J. Nilsson and U Sterner. Robust MPR-based flooding in mobile ad-hoc networks. In *MILITARY COMMUNICATIONS CONFERENCE, MILCOM*, 2012.

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se