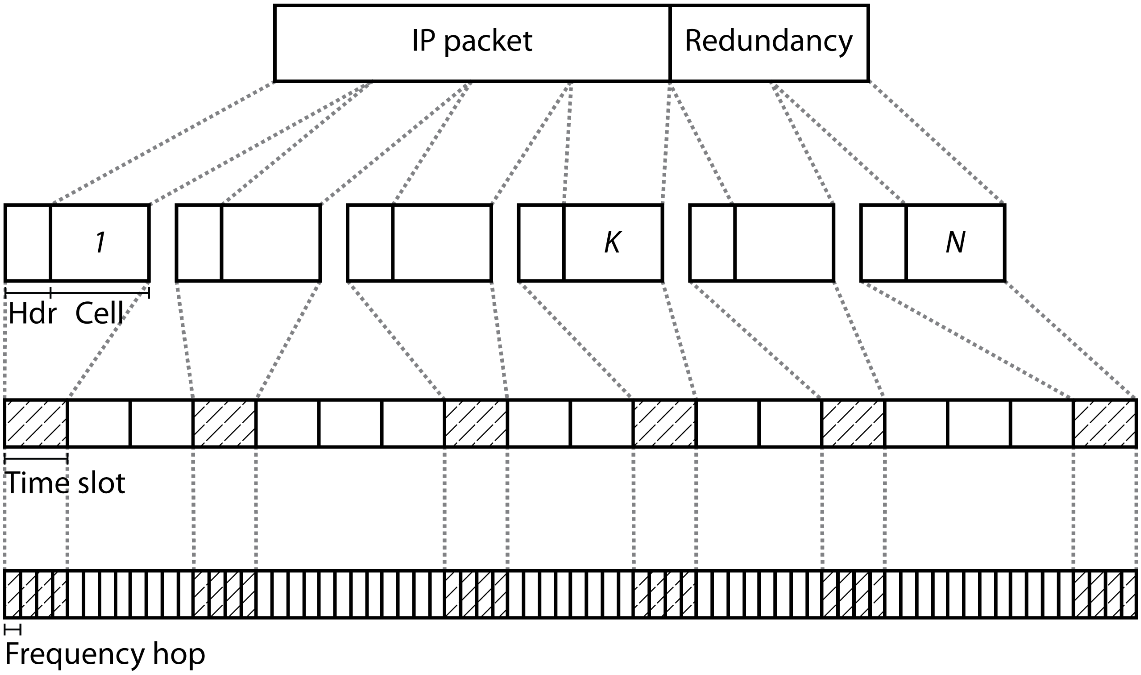
Robust Packet Delivery

JIMMI GRÖNKVIST, ANDERS HANSSON, JAN NILSSON



FOI-R--4059--SE
ISSN 1650-1942
February 2015

Jimmi Grönkvist, Anders Hansson, Jan Nilsson

Robust Packet Delivery

Titel	Robust paketförmedling
Title	Robust Packet Delivery
Rapportnr/Report no	FOI-R--4059--SE
Månad/Month	Februari/February
Utgivningsår/Year	2015
Antal sidor/Pages	29
ISSN	1650-1942
Kund/Customer	FMV
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E324213
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Summary

Robust and reliable packet delivery in mobile ad hoc networks requires dealing with unstable links. Focus of this report is on two methods to mitigate this problem.

Firstly, we study Cross-Packet Coding which uses forward error correction to protect an IP packet end-to-end through a network. We show that it can provide a substantial increased packet delivery ratio when a packet is so large that it cannot be sent in one transmission but need to be fragmented into several transmissions.

Secondly, we investigate the network diversity which provides robustness through redundancy if a message is transmitted over several paths between a source and a destination. By simulations we estimate the amount of network diversity that is utilized by MPR flooding. The network diversity in the studied networks is equivalent to between one and two independent paths depending on network density.

Keywords: Cross-Packet Coding, reliable packet delivery, MPR flooding, network diversity.

Sammanfattning

För att uppnå hög robusthet och tillförlitlig paketförmedling krävs i ad hoc-nät att instabila länkar hanteras på ett bra sätt. Fokus i denna rapport är två olika metoder att hantera problem kring instabila länkar.

Första metoden kallas ”Cross-packet Coding” och är en teknik att skydda IP-paket end-till-end i nätet genom felrättande koder. Vi visar att detta kan ge signifikanta minskningar i paketfelhalterna för IP-paket som är så stora att de måste delas upp i många sändningar.

Den andra metoden är nätverksdiversitet vilket skapar robusthet genom att informationen kan komma fram på flera olika vägar i ett nät. Med hjälp av simuleringar estimerar vi hur mycket nätverksdiversitet som utnyttjas vid MPR flödning. Nätverksdiversiteten är i de studerade näten ekvivalent med motsvarande mellan en till två oberoende rutter beroende av nätverkstätheten.

Nyckelord: Cross-Packet Coding, tillförlitlig paketförmedling, MPR flödning, nätverksdiversitet

Contents

1 Introduction

Robust and reliable packet delivery in mobile ad hoc networks requires effective measures to deal with topology changes and unstable links. Node movements together with multipath wave propagation result in a time varying fading channel that can cause links to go up and down very rapidly. A link that is of good quality during one packet transmission can be unusable because of a deep fade during the next transmission. Hostile jamming or other types of interferences may also cause links to become unstable. Means to mitigate the problem with unstable links are several. For example one can, besides using a robust physical layer waveform, utilize network diversity i.e., the redundancy obtained when a message is transmitted over different paths between a source and a destination.

The main subject of this report is a method to mitigate the problem of unstable links that we call cross-packet coding (CPC). Besides CPC, the achievable gain for network diversity is investigated in the report. In contrast to physical layer forward error correction (FEC) which protects a packet segment (here called cell) that is sent between two nodes, CPC protects a whole end-to-end transmission of IP-packets. CPC can either be used for protecting a packet flow sent over a single path, or, be combined with network diversity to further increase the robustness. Moreover, it can be used for both unicast and broadcast/multicast traffic.

Chapter 2 provides a background to CPC and discusses in what situations CPC are effective. Chapter 3 treats possible code constructions to accomplish CPC. A quantitative investigation of the gains that can be reached with CPC, network diversity, and a combination of CPC and network diversity is provided in Chapter 4. In Chapter 5, the network diversity obtained by flooding and MPR flooding are studied. Finally, the overall conclusions are presented in Chapter 6.

2 Background

There are several methods that can be used to provide reliable communication of messages in a network. Sending the message over several different paths (utilizing network diversity), retransmissions/ARQ, and a robust physical layer waveform are some examples of methods to increase reliability. One additional method that can be used is CPC. CPC provides additional protection above physical layer FEC for an end-to-end transmission of a packet. It is useful when a packet is so large that it cannot be sent in one transmission but need to be fragmented into smaller sub-packets sent in several transmissions. To be effective, CPC and (non-hybrid) ARQ-techniques require that the cell error occurrences are independent, i.e., the channel coherence time should be less than the time for a cell transmission. This means that how well CPC protects against fading depends on how fast the fading is. CPC is most effective when the channel coherence time is on the order of cell transmission time, or slightly slower. That is, when the physical layer interleaving and FEC does not help to protect a cell. On the other hand, CPC is ineffective in cases with very slow fading as several cells may experience the same deep fade. For slow fading, however, network diversity in terms of several paths may provide a mean to increase reliability. CPC and ARQ are similar in the sense that both techniques aim to protect against packet fragment errors. However, ARQ-techniques are ineffective and complicated to use for broadcast/multicast traffic which suggests that CPC are of particular interest for that type of traffic.

The cross packet coding we consider is an end-to-end coding of IP packets. That is, packets are entities on the IP layer. To distinguish an IP packet from what can be sent in a time slot we call the latter a cell, i.e., an IP packet is fragmented into cells. One cell is normally sent in one time slot, deviations may occur though, e.g., when two cells can be combined and sent in a single time slot. Here we assume that a time slot contains one cell only and that a cell needs a whole time slot to be transmitted. A cross-packet coder divides an IP-packet into cells and generates redundant cells. The CPC coding is made so that the IP-packet can be reassembled correctly, despite that one or several cells are lost during the transmission.

Cells are received correct, erroneous, or not at all. Erroneous reception or no reception at all, may occur because of several reasons. One reason is a poor channel with a low signal-to-noise ratio (SNR), either caused by a high path loss or multipath fading. Other possible reasons are interferences and jamming. Yet another reason is that a cell is dropped in a node because that either no path to the destination exists or no resources in terms of time slots are available.

The instantaneous bandwidth and the length of a time slot vary between different system designs. However, for waveforms with instantaneous bandwidths around 1 MHz, typical time slot lengths are between 1-5 ms. With an assumption of a spectral efficiency of 1 bit/s/Hz, it means that a time slot can carry 1000-5000 bits of information. For narrowband waveforms, with instantaneous bandwidths around 25 KHz, typical time slot lengths are between 20-50 ms. Again, with an assumed spectral efficiency of 1 bit/s/Hz this means that a time slot can carry 500-1000 bits of information. An IP packet of 12 000 bits then needs from only 3 cells, with the wideband system, up to about 24 cells with the narrowband system.

3 Coding alternatives

Coding of the IP-packet could be done over frequency hops, or cells. Generally, a code is better the longer it is, suggesting a code at frequency hop level. On the other hand, there are some limitations on how the encoding of IP-packets can be done due to networking. A cell needs to be decoded at each node, at least to be able to extract the control/header information. Hence, a cell needs to be encoded by a separate decodable code, meaning that a cell can only be correct or erroneous after the cell decoding. In the latter case, the best the CPC can do is to treat the cell as an erasure. CPC cannot utilize a potentially stronger code construction that could be achieved by coding at frequency hop level, i.e., each frequency hop is treated as correct or erasure of the CPC.

The CPC codes we consider are erasure codes at cell level. We assume that an IP-packet is divided into K cells at the source node. Then CPC adds redundant cells so that altogether N cells are transmitted, see Figure 1.

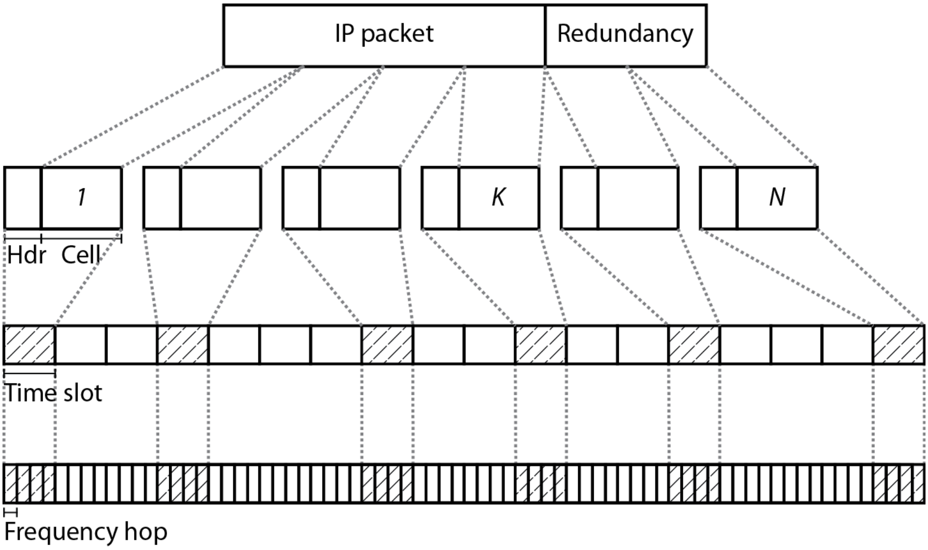


Figure 1: An IP-packet is divided in K cells and transmitted with redundancy in N cells

Then we have protected the IP-packet with a CPC with parameters (N, K). The code can correct $N - K$ erroneous cells, provided these erroneous cells can be identified and treated as erasures in the decoding. Such CPC codes can be constructed in different ways. The simplest is to use a XOR-construction resulting in a $(K + 1, K)$ CPC but it has the limitation that only one erroneous cell can be corrected.

A more flexible solution can be obtained by using a CPC based on RS-codes [1]. RS-codes are MDS (Minimum Distance Separable) which are an important class of block codes since, for a fixed n and k, they have the greatest error correcting, erasure correcting, and detecting capabilities. As CPC codes, they can correct $N - K$ erasures.

For every choice of parameters q, n, and k, there is a Reed–Solomon code that has a symbol alphabet of size q, a block length $n \leq q$, and a message length $k < n$. Moreover, the alphabet is interpreted as the finite field of order q, and thus, q has to be a prime power. A natural choice of prime is two, which also considerably simplifies the coding implementation considerably. Thus, q can take values 2, 4, 8, …,1024, 2048 etc, where $q = 2^m$. For example, assume that an IP packet consists of 12000 bits and a cell of 1000 bits. Furthermore, assume that we need a $(N = 15, K = 12)$ CPC to be able to correct 3 erroneous cells. This requires a RS-code over the field 2^{11}. Such an RS code can be of length up to n=2048, where each symbol consists of $m = 11$ bits, thus having a length of up to 22 528 bits. The CPC code for our assumed length of 12000 is obtained by shorten the long RS $(n = 2048, k = 1091)$ code to obtain a RS $(n = 1364, k = 1091)$ over 2^{11}. Such a code corrects 273 symbol erasures, i.e., $273 \times 11 = 3003$ bit erasures or 3 cell erasures. Unfortunately, decoding process of large RS codes, which involves correction of many erasures over large finite fields, is complicated. In [2] a recent RS-decoder implementation is described. The decoder handles code block length up to 4095 over 2^{11}. Thus, it could decode the example code above, but the decoding time would be long.

Fountain codes (also known as rateless erasure codes) are an alternative to RS-codes [3,4]. In particular, the Fountain Raptor codes, which are the most efficient fountain codes at this time, have very efficient linear-time encoding and decoding algorithms. These algorithms require only a small constant number of XOR operations per generated symbol, both for encoding and decoding.

A fountain code is capable of producing an unlimited sequence of encoded symbols (i.e., $n \rightarrow \infty$) from a block of k fixed-length source symbols. The actual number of encoded symbols, and thus the code rate, can be determined as needed, which is why they are called rateless. At the receiver, a fountain decoder is able to recover the source block from any set of k' received output symbols, where k' is slightly greater than k. Thus, a fountain code can correct $n - k'$ erasures. When compared with RS-codes, fountain codes introduce an additional reception overhead $\varepsilon = (k' - k)/k$. This overhead depends on the value of k and the desired probability that the source block can be fully recovered from the received output symbols. In [4] the authors claim that the fountain code reception overhead ε typically is less than 1 %.

Under similar protection assumptions, a Raptor code requires less processing power than Reed-Solomon erasure codes for encoding and decoding. According to [4], processing requirements for a DF Raptor code grows linearly with the source block size k, whereas Reed-Solomon erasure codes exhibit processing requirements that grow quadratically with source block size. However, in [5] a more efficient practical algorithm for erasure decoding of RS-codes is presented. Its processing requirements grow between linearly and quadratically. Furthermore, in [5] a large RS-code over the finite field 2^{16}can be decoded in less than a second on an Intel core 2 processor at 1.86GHz.

Finally we can conclude that using RS codes would be preferable if the decoding complexity could be afforded. However, to answer the latter question further investigations are required. The exact code or code family that is needed has to be determined. Then, the different implementation options for that code family, as well as what can be afforded to be implemented in a radio node, have to be analyzed. However, if the decoding complexity with RS codes would be too large, other code constructions exist and a code construction based on, e.g., Fountain Raptor codes seems like a viable alternative.

4 Performance of CPC or/and diversity

In this chapter we analyze the gains that can be obtained with CPC, network diversity, and a combination of CPC and network diversity in a multihop TDMA broadcast network.

4.1 General assumptions

We assume that all IP packets generated in source nodes have all other nodes in the network as destination. As each time slot can only handle a fixed number of bits, often smaller than the IP packets to be transmitted, each packet is assumed to be divided into K cells, each transmitted in a separate time slot. CPC is adding redundancy resulting in N cells in total.

Each hop and time slot is assumed to have a probability p for correct transmission of a cell. The probability depends on a number of factors, such as time slot size, slot code rate, path loss, noise, jamming, etc. However, to simplify the analysis we assume that p is equal for all links.

Here we study a single destination only, but as the traffic is assumed to be broadcast, this destination can be seen as one of many. We will not use any feedback channels as they are difficult to generate for broadcast traffic. In this chapter we will use simple network model that assumes that the broadcasting of packets allow for v independent paths on which a message can arrive at a destination. In reality things will be more complex, for full flooding, e.g., the number of paths can be very large although they will not be independent. For MPR flooding, the number of possible paths will be much lower (but potentially less correlated), see Chapter 5. We will not analyze what are reasonable values of v here, but rather try to study how utilized network diversity (in terms of v) can affect Packet Delivery Ratios (PDRs), especially over multiple hops. Each path is assumed to be h hops, where h can have values from 1 to somewhere around 4 or 5. More hops than that is probably not so relevant in a military radio network.

The probability to correctly receive a cell on a specific path with length h is

$$Pr(\text{correct cell}) \;=\; p^h.$$

If we have more than one path, the reception needs to fail on all paths in order to fail the reception of the cell, i.e.

$$Pr(\text{failed cell on all } v \text{ paths}) = (1 - p^h)^{\mathrm{v}}.$$

We denote by P_c the probability of a correctly received cell. It can be calculated as

$$P_c = \; 1 - (1 - p^h)^v \tag{1}$$

in the simplified model with v independent paths at h hops from the source.

The probability for a correct message if $N - K$ cells can be lost can now be written as:

$$\sum_{i=0}^{N-K} \binom{N}{i} P_c^{N-i}(1 - \; P_c)^i.$$

4.2 Results for different packet sizes and path lengths without CPC and network diversity

In Figure 2 the multi-hop problem with packet delivery in networks is shown. Increasing the number of hops will decrease delivery ratio. For unicast traffic, this is usually handled with ARQ on each hop, something that is difficult for broadcast traffic. In Figure 3, we see an additional problem; the delivery probability will decrease further for large packets if only traditional link FEC is used.

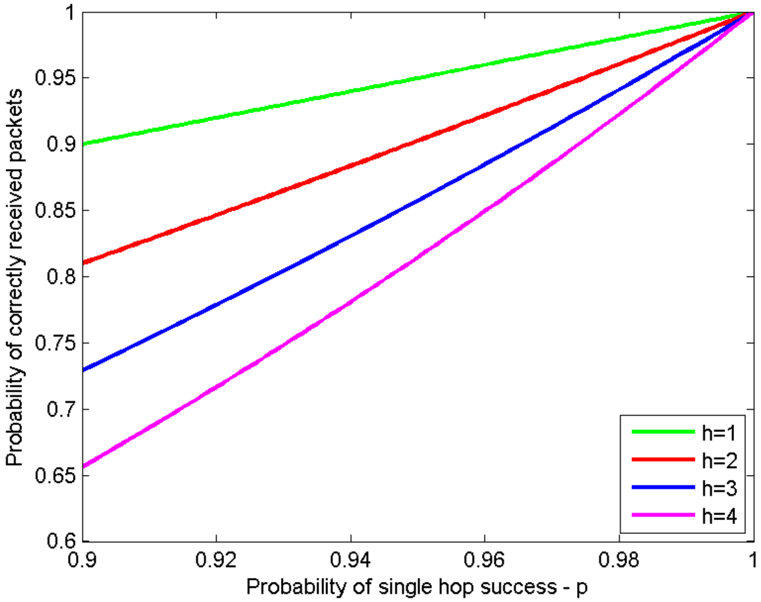


Figure 2: Probability of received packets for a single path $(v = 1)$ for $K = 1$.

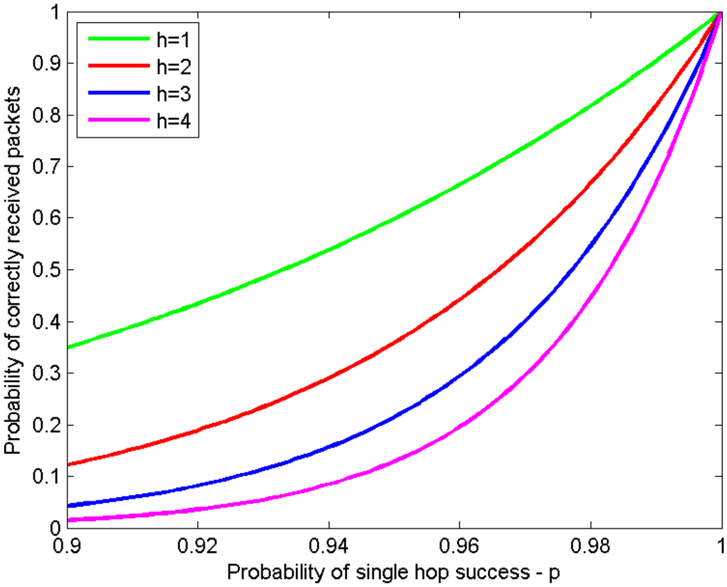


Figure 3: Probability of received packets for a single path $(v = 1)$ for $K = 10$.

4.3 Results for multiple paths without CPC

For broadcast traffic the number of paths may be higher than one though, which may resolve the problem somewhat. In Figure 4 we show the case for $h = 3, K = 1$, for $v = 1$ (same as before), $v = 2$, and $v = 3$.

In Figure 5 this is shown for $K = 10$. In this case, we see that for short packets, just a second path adds considerably help in handling the problem of long paths. The probability of correct packet delivery is higher than the single hop delivery. Network diversity adds considerably advantage. For long packets though one can question if it is sufficient, though.

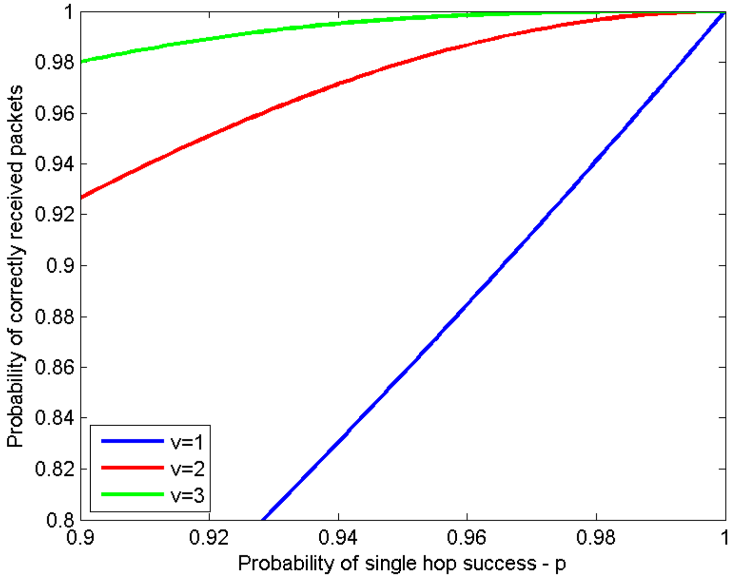


Figure 4: Probability of received packets for paths of length $h = 3$ and $K = 1$ with varying number of independent paths.

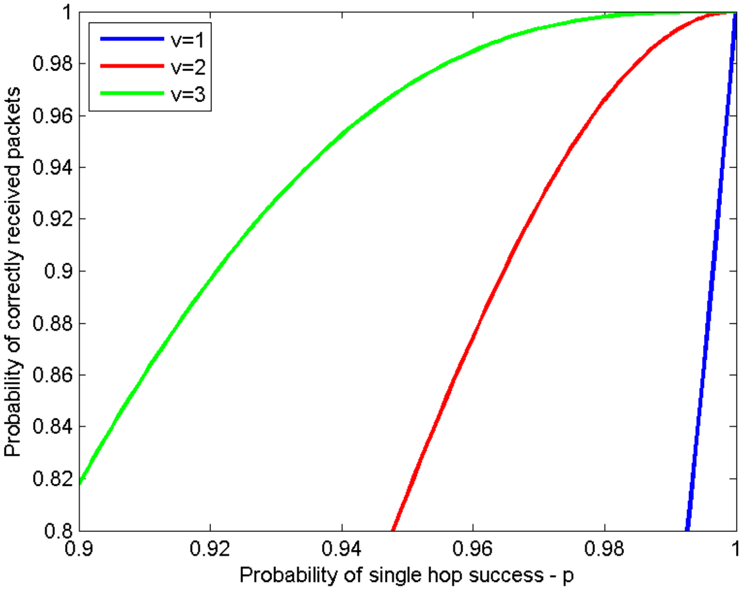


Figure 5: Probability of received packets for paths of length $h = 3$ and $K = 10$ with varying number of independent paths.

4.4 Results for multiple paths with CPC

We now study what happens if we can correct for the loss of a few packets. We start by studying the effect of CPC without any support of network diversity for large packets. This is plotted in Figure 6 for different error correction abilities. As can be seen, CPC improves the delivery ratio, but, unless a very high p can be achieved, the probability of correctly received packets is still rather low for large packets.

Figure 7 shows the result for two independent paths. As can be seen already if a single lost time slot can be corrected we see a considerable gain. In fact, as long as p is above around 0.93 the packet delivery ratio will be above p, at which case it may be more beneficial to improve p (by lowering the link rate) instead of increasing the CPC redundancy.

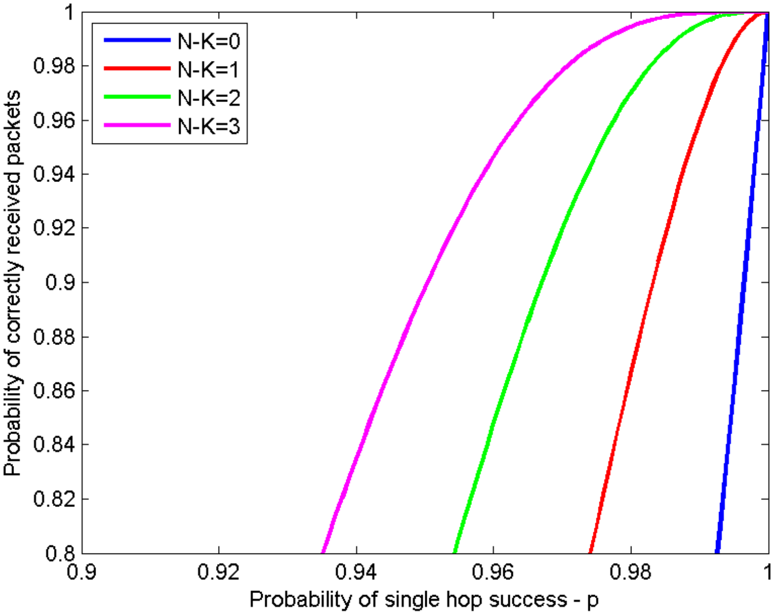


Figure 6: Probability of received packets for single paths ($v = 1$) of length 3 for $K = 10$.

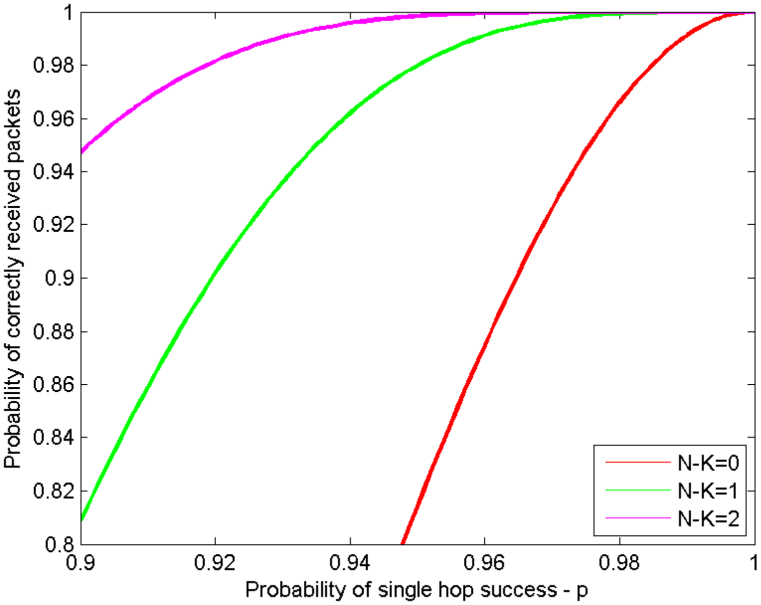


Figure 7: Probability of received packets for two independent paths ($v = 2$) of length 3 for $K = 10$.

4.5 Discussion on packet size

When transmitting short packets (i.e. with size less than what fits in a single time slot) over several hops, CPC will be of little benefit (especially if low delay is required) as most redundancy often will end up in the same time slot (which will succeed or fail). This means that the success probability over a single hop p needs to be sufficiently high to handle cases with little or no network diversity. Most likely 98 - 99% (notice this is average values and not worst case values) in order to get reasonable packet delivery ratios.

When packets are getting larger, and get divided into multiple cells, CPC becomes necessary to bring the probability to a sufficiently high level. If 98-99% correct slots are needed for small packets there is no need for more than one, or two, redundant cells to obtain the same error probability for large packets on single paths, see Figure 6. However, even a single redundant cell is a significant increase in traffic load for a 2 cell packet ($K = 2$).

An alternative solution is to increase p (for example by lowering data rates on the link) so that also larger message size can be handled without CPC. The drawback of that is that a higher p will affect all message sizes, i.e., not just $K = 2$ or $K = 3$. There is a risk that 2 cell packets or 3 cell packets will be rare compared to smaller packets, e.g., voice packets and position packets) and to larger packets with bulk data (1500 Byte). Adapting p to very few packets may simply not be worth it. Another question is how high the message delivery ratio needs to be for different applications. It may be possible for the source to determine the level of network diversity and adaptively choose the level of redundancy based on required packet delivery ratio (if such a thing can be guessed from QoS parameters).

5 Evaluation of MPR flooding diversity

From the previous chapters, it is clear that network diversity can be a significant factor in the improvement of the packet delivery in networks. Already for two independent paths, only a small amount of redundancy (through CPC) is necessary even for large packets. With no network diversity, on the other hand, it is expensive in terms of redundancy (and thereby capacity), to achieve a sufficient packet delivery ratio for long packets. In addition, also shorter packets may need CPC if there is no network diversity.

In this section, we study the level of network diversity for the two broadcasting techniques: full flooding (where each node retransmit each packet once) and MultiPoint Relay (MPR) flooding. MPR flooding is one of the most used broadcast techniques today and attempts to reduce the number of nodes that retransmit a message with the help of two-hop information. We use the MPR flooding technique as described in RFC 6621 [6]. Each node selects a minimum number of its neighbors so that retransmissions via those neighbors together reach all two-hop neighbors.

The MPR selection principle reduces the necessary number of retransmissions to reach all nodes in the network, thereby increasing the capacity. But the increasing capacity comes at a price of reduced network diversity. It is easy to construct examples where almost no network diversity is utilized by MPR flooding, as compared to full flooding where all nodes retransmit cells. We are therefore examining the average network diversity utilized by full flooding and by MPR flooding in networks with random node positions and a fixed communication range.

5.1 Simulation setup

For the evaluation we, generate two examples with random networks of 30 nodes, with uniformly distributed positions inside a square. We assume that there is a communication link between all pairs of nodes that are within a distance of 10 km to each other. In order to get network examples with different connectivity, two different square sizes are used: one with side 15 km and one with side 30 km. For every network, we calculate the number of hops h in the shortest path length between each node pair, and the set of multi-point relays that each node selects.

To simulate the end-to-end cell transmissions, we randomly set the communication over each link to be successful, or not successful, with a success probability p. These random choices of successful links are generated a large number of times for each network. For each random choice, we sequentially set each node to be broadcast source. By flooding simulations, we estimate the probability P_c of successful cell transmissions on original distance h from the broadcast source. These estimated probabilities of P_c, for full flooding and MPR flooding, are in chapter 5.2 compared to the theoretical expression of P_c given in equation (1). In Table 1, we show the average network parameters for the two random network examples that we evaluate. We note that the networks generated in a square of size 15×15 km are quite dense, with only 5 multipoint relays in average. The networks generated in a square of size 30×30 km are sparse, and requires an average of 15 multipoint relays.

Table 1. Average network parameters for the two sets of randomly generated networks.

Square side	**15 km**	**30 km**
Number of MPRs	5,2	15,1
Path length h	1,3	2,4
Maximum path length	2,2	5,3
Number of neighbours	20,7	7,5
Number of links	310	113

5.2 Results

In Figure 8 and Figure 9, we plot the estimated probability P_c of successful cell transmissions on distance $h = 3$ hops from the broadcast source. The estimates for MPR flooding and full flooding are compared to the theoretical expression of P_c in equation (1), for $v = 1$ and $v = 2$.

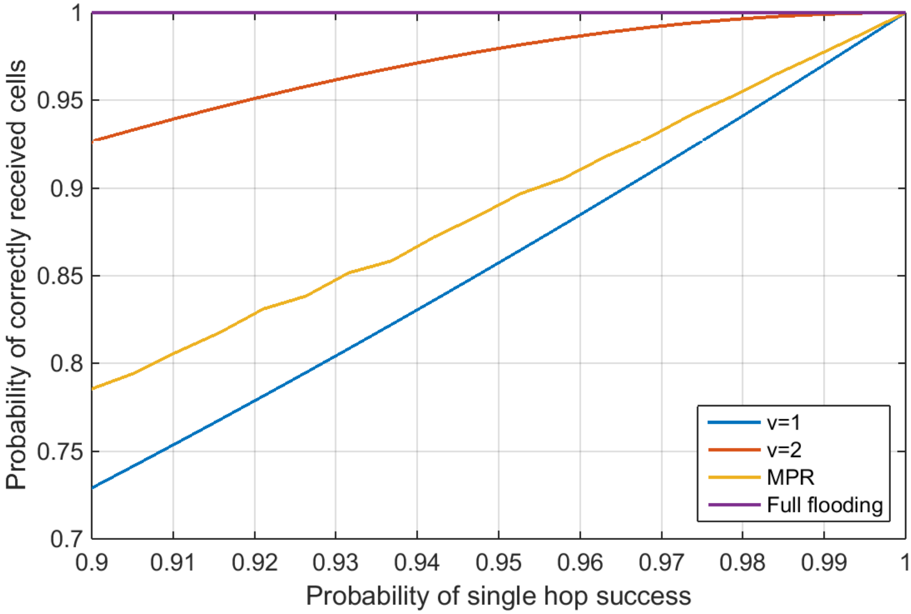


Figure 8: Probability of successful cell transmissions at 3 hop distance from source in dense networks.

By this comparison, we can indirectly estimate the amount of network diversity utilized by the flooding method. Since full flooding uses all possible links in the network, we can say that all of the network diversity is utilized by this method. This can be seen in Figure 8 and Figure 9, where the estimated probability P_c is close to 1 for full flooding, i.e., there are very few transmissions with lost cells.

Figure 8 show the example with dense random networks (square side 15 km). We note that the estimated probability P_c for MPR flooding is just a little larger than the theoretical probability P_c for $v = 1$ (a single path without diversity). So we can conclude that MPR flooding utilizes a small amount of the network diversity in these networks.

Figure 9 show the example with sparse random networks (square side 30 km). Compared to the dense networks, we see a considerably better utilization of the network diversity for MPR flooding, close to the theoretical probability P_c for two independent paths. Moreover, we can see a few lost cell transmissions even for full flooding in these networks.

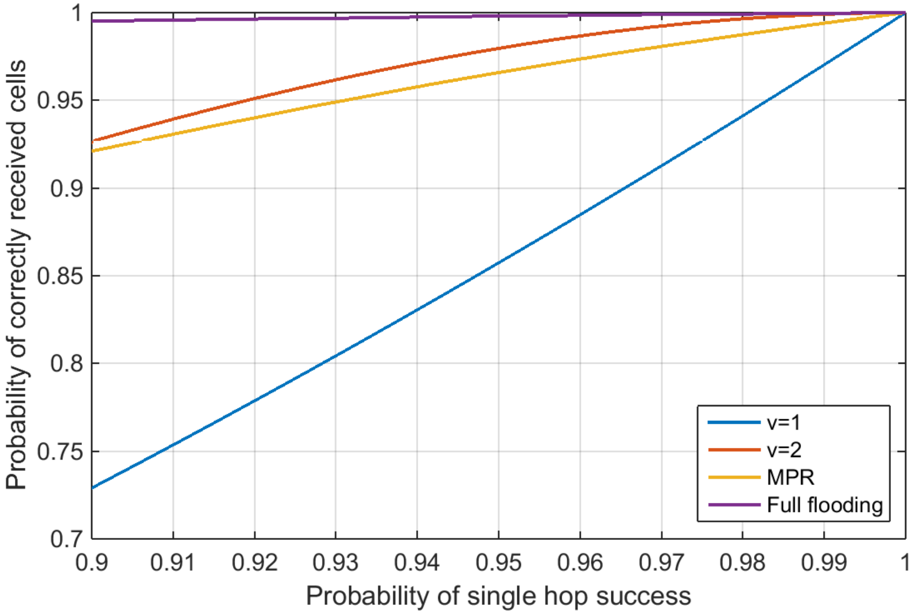


Figure 9: Probability of successful cell transmissions at 3 hop distance from source in sparse networks.

A possible reason to low utilization of network diversity in dense networks is that fewer nodes are selected as multipoint relays, compared to sparse networks. With MPR flooding, only the multipoint relays retransmit cells. If a cell transmission to a multipoint relay fails, it is probable that no other neighbor is selected as multipoint relay. Thus none of the neighbors retransmit the cell, even if several of them did receive it. As the network becomes sparser, more nodes are selected as multipoint relays. If a link transmission fails in a sparse network, it is more likely that another neighbor is a multipoint relay and is retransmitting the cell so that it reaches the node from this direction instead.

It should be noted that since the average path length in dense networks is shorter, the average cell delivery ratio for the entire network is larger in dense networks than in sparse networks.

6 Conclusions

Robust and reliable packet delivery in mobile ad hoc networks requires efficient techniques to handle the problem of unstable links. First of all, a robust physical waveform is needed to combat the link instabilities as much as possible. However, in many situations that may not be enough to obtain a reliable multi-hop transmission of long packets. In broadcasting, network diversity also provides robustness through redundancy when a message is transmitted over different paths. An additional method is cross-packet coding (CPC) which gives additional protection above physical layer FEC for an end-to-end transmission of a packet. CPC is useful when a packet is so large that it cannot be sent in one transmission, but needs to be fragmented into smaller sub-packets, here called cells, sent in several transmissions. CPC codes can be seen as erasure codes on cell level

A CPC code construction based on Reed-Solomon codes would be preferable if the decoding complexity can be afforded. The drawback is that protecting large IP-packets requires decoding of large RS codes, correcting many erasures, over large finite fields, which is complicated. However, other viable CPC code constructions, with lower decoding complexity exist, e.g., a construction based on Fountain Raptor codes.

Regarding overhead, CPC is only efficient for IP-packets that are fragmented into several independently transmitted cells. In such cases CPC can provide a substantial increased packet delivery ratio. Furthermore, network diversity further improves the packet delivery ratio. Therefore, when to use CPC, and the necessary CPC redundancy, is related to the amount of network diversity that is utilized by the broadcasting method.

An investigation of the utilized network diversity obtained in a 30 node network with MPR flooding and full flooding is carried out. Full flooding provides all of the inherent network diversity, but at the cost of a high overhead traffic. Therefore it is seldom used compared to MPR flooding that is a more common broadcast technique. Dependent on the network topology, MPR flooding utilizes network diversity equivalent to between one and two independent paths: one path for dense networks and two paths for sparse networks. As the MPR flooding packet delivery ratio is low with unstable links, we conclude that CPC is required for the analyzed network scenarios.

References

[1] S. Wicker, V. Bhargava, “Reed-Solomon Codes and Their Applications”, September 1999, Wiley-IEEE Press

[2] XILINX, “LogiCORE IP Reed-Solomon Decoder, Product Guide” April 2, 2014

[3] S. Arslan, “Incremental redundancy, Fountain codes and advanced topics”, Graph Codes and Their Applications, arXiv preprint arXiv:1402.6016 (2014)

[4] Digital Fountain, “Why Digital Fountain’s DF Raptor™ technology is better than Reed-Solomon erasure codes for streaming applications”, San Diego, 2010

[5] F. Didier, “Efficient erasure decoding of Reed-Solomon." arXiv preprint arXiv:0901.1886 (2009) codes”

[6] J. Macker, “Simplified Multicast Forwarding" RFC 6621, Internet Engineering Task Force, May 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