Increasing Robustness of Multi-homed Systems in Heterogeneous Environment

Matej ROHLIK, Petr CHLUMSKY, Tomas VANEK

Department of Telecommunication Engineering, Faculty of Electrical Engineering,
Czech Technical University in Prague, Technicka 2, 166 27 Praha 6, Czech Republic

matej.rohlik@fel.cvut.cz, petr.chlumsky@fel.cvut.cz, tomas.vanek@fel.cvut.cz

Abstract. *Nowadays, packet error rate in fixed networks can be considered as a negligible value. However, the increasing requirements for transmission speed of mobile devices, heterogeneous technology, and other high frequency sources cause interference growth within the electromagnetic spectrum. This affects the overall reliability and throughput of the network and may cause undesirable operation malfunction of application-level services. Higher speeds can be achieved by advanced modulation techniques, but at the price of lower resistance against the interference. On the other hand, error-correcting codes or higher-level protocols are utilized to correct the delivery failures. We introduce a novel method for increasing robustness of communication for multi-homed systems in heterogeneous environment. Furthermore, we propose a security measure to ensure confidentiality, integrity and availability of the transmitted data without influencing the transmission parameters. Finally, we show positive impact of the proposed method on transmission efficiency and effective throughput, especially in networks with high probability of error occurrence.*

Keywords

Heterogeneous packet network, multi-homed load balancing, network coding, security.

1. Introduction

Contemporary 4G mobile technology standards, such as the IEEE 802.16m-2011 (WirelessMAN-Advanced) or the LTE-Advanced (LTE-A) provide solid foundation for further development of the future 5G standard and related services. However, from its substance, wireless communication evinces variable parameters in the terms of signal to interference plus noise ratio (SINR), channel capacity, delay, jitter and throughput, which affect possible deployment of new potentially emerging services.

Clearly on a global scale, the volume of mobile data traffic continuously increases. To efficiently cover the demand of customers, one of the promising solutions seems to be to split the service requests among available communication ways, thus utilize a multiple path bonding of multi-homed devices and provide higher data rate to the end users.

The authors in [1] dealt with bandwidth aggregation techniques in heterogeneous multi-homed devices and surveyed the most prominent solutions that were designed to address effective bandwidth utilization of appliances connected to several computer networks, enhance overall communication reliability, or opportunistic load offloading. Because of several aspects, which needs to be taken into account, when designing multipath communication systems, the conclusion is ambiguous and does not provide one and only protocol that should be used. However, it outlines evolution trends challenges requiring further research and one of which we address in this paper.

Therefore, we present a general approach for heterogeneous multi-homed networks, which is based on inverse packet multiplexer (IPM) while it eliminates the original disadvantage of IPM, which represents an uncoordinated sorting of packets to multiple transmission paths, that can result into an uncontrolled growth of transmission delay [1], higher layer protocol instability and/or session breakdown.

The principle is achieved by application of a control polyline function that regulates the amount of packet data passing through the data channels. Moreover from end-to-end perspective, the system is transparent, independent on operating systems or network devices, increases stability of the connection by regulation of the delay value during the transmission, optimizes data coding to provide higher service reliability, and provides adequate security for the user data.

2. Towards Secure and Reliable Packet-Based Future Heterogeneous Systems

To incorporate techniques which substantially increase end-to-end throughput of user-data, stability of the connection and reliability of transferred data delivery into the future mobile networks, a transparent and architecture independent solution needs to be designed. Moreover, where efficient security is required [2], effective cryptographic and coding measures must be assured to provide adequate quality in the terms of end-to-end throughput and delay. Therefore, in this section, we briefly introduce current multi-homing architecture approaches in nowadays packet networks. Subsequently, we present enhancements towards secure, reliable and load-balanced packet delivery in future mobile systems.

2.1. Current IP-Related Multi-Homing Architectures

The network layer, as per the ISO/OSI reference model, or the so called the Internet layer, is widespread based on the Internet protocol (IPv4/IPv6) which relies on interconnection of independent network parts denoted as the autonomous systems (ASs). The natural dynamic behaviour is managed by border routers which utilize dynamic routing protocols, such as the border gateway protocol (BGP), to exchange the network topology modifications as the particular network availability changes. Even though the IPv4 and the IPv6 work in a different manner, they both rely on the AS principle and both are desired to provide redundancy and load-sharing [3]. However generally, the principles have not been completely resolved or standardized yet [4], and without proper end-to-end administrative control, the proportional load balancing (Fig. 1) is impossible to ensure for the returning path even while utilizing BGP [5].

In [1], the authors accomplished a complex survey of the bandwidth multiplexing methods in heterogeneous environment, such as the multiple radio access technology (Multiple-RAT), [6]. The contribution has been published lately thus we consider it comprehensive. Even though the analysed solutions do affect either the application layer, the transport layer, the network layer, or the link layer, none of them has been standardized, because none of them is universal enough to cover all heterogeneous networks (IP-, non-IP-based) and/or various physical connections under different application requirements while efficiently implementing load balancing with minimal header overhead, delay and providing adequate security. Therefore, we focus on a transparent approach that addresses them.

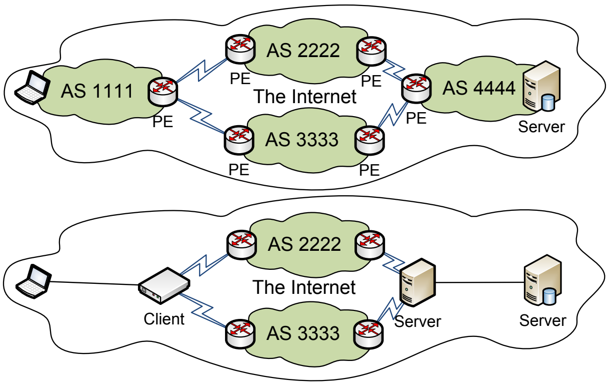

Fig. 1: BGP-based and non-BGP-based multi-homing example.

2.2. Transparent Transmission Environment Compliance

The elementary idea is to prevent congestion and deterioration of the transmission parameters due to classification of incoming packets according to current states of the individual outgoing interfaces the packet are about to be sent to, and to establish a stable data channel resistant to fluctuating transmission parameters, by which a wireless or a mobile environment is typically characterized. The solution adopts a packet (polyline) regulator principle that is based on inverse packet multiplexer [7].

However, the regulator principle does not address optimized reliability or security (Fig. 2). Therefore, within our approach, we focus on the network coding principles that reduce the overall processing delay and require a minimum buffers size while preserving adequate reliability in the terms of delivery of network packets.

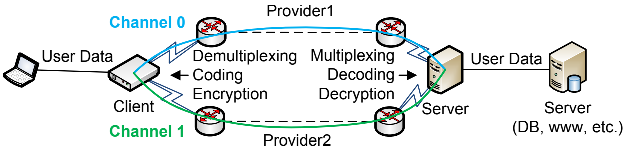

Fig. 2: Transparent transmission multi-homing principle.

Network coding is a novel technique introduced at the turn of the millennium with the intention to improve network throughput, robustness and wireless resources. In usual communication networks, every intermediate node works with an assumption that independent data streams may share resources, but the information itself is separate. Network coding breaks this assumption. Instead of simply forwarding data, nodes are enabled to recombine several messages from different input flows into one or several output packets [8]. The authors in [9] showed that we can allow intermediate nodes to process incoming streams, not just forward them. Benefits of network coding techniques in terms of throughput and robustness are described in e.g. [10], [11], [12].

Our system is based on the combination of network coding and path diversity principles. An appropriate linear combination of data, specifically with XOR logical function, produces an additional redundancy for the transmission that creates an option of setting the ratio of resistance and transmission rate. Channel 1 is used for the XOR combination of two consecutive messages. If a single message or more messages M_n get lost, is possible to reconstruct original data without any retransmissions in Channel 0 (Fig. 3(a)). Number of messages suitable for reconstruction is dependent on the size of buffer at the receiver side of transmission.

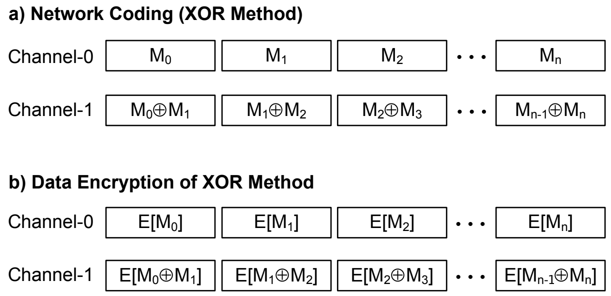

Fig. 3: Network encryption principle.

2.3. System Security Aspects

Undoubtedly, multiple transmission paths make a potential eavesdropping attack difficult. But on the other hand, considering that the attacker is able to intercept data on a single connection, most probably will be (technically) able to perform the same malicious activity on the rest of the links. Therefore, such measure cannot be considered as a data protection technique [13], hence we focus on a satisfactory security principle which does not affect the transmission parameters while preserves the system resources.

To be able to state that the system is secure, it is necessary to fulfil the three information security attributes: confidentiality, integrity and availability (CIA). The availability is assured by the network coding mechanism described in the previous section (referred to as reliability). To provide consistency of data, integrity mechanisms generally add redundant information to the original data. Therefore, considering that today's modern devices are endowed with HW support of block algorithm denoted as the Advanced Encryption Standard (AES), we utilized AES in Galois/counter mode of operation (AES-GCM), which is a confidentiality and authenticated encryption mechanism that includes integrity function while minimizing the extra information added to the user data thus minimizing latency and operation overhead [14]. Even though, stream ciphers are faster when implemented in HW, they are not considered in this case as they do not provide the integrity feature and vulnerable to the modification attacks. In [15] on the other hand, the authors outlined parameters (such as pipelined and parallelized implementations and minimal computational latency) which are requested that the mode must fulfil in order to be efficient for high-speed data rates. The counter mode has emerged as the best method.

Algorithm 1 Robustness increasing.

```
ASSUMPTION: a packet buffer $B$ exists
CREATE an empty queue $Q$
GET packet $P$ from $B$
ENQUEUE $P$ onto $Q$
GET packet $P$ from $B$
ENQUEUE $P$ onto $Q$
while $Q$ is NOT empty do
    $M_0 \leftarrow Q$.dequeue()
    $M_1 \leftarrow Q$.read()
    $E_0 = E[M_0]$
    $E_1 = E[M_0 \oplus M_1]$
    SEND $E_0$ via Channel 0
    SEND $E_1$ via Channel 1
    GET packet $P$ from $B$
    ENQUEUE $P$ onto $Q$
end while
```

The principle of securing the multiple encoded data stream (Alg. 1) is based on encryption (E[M_n]) of single messages (M_n) or encryption of coded pairs of consequent packets (E[$M_{n-1} \oplus M_n$]) by application of AES (see Fig. 3b). The AES-GCM is an algorithm providing encryption and hashing mechanism while it minimizes the overall data overhead of the original message and maximizes throughput, especially, when efficiently combined with dedicated HW resources such as the field-programmable gate arrays (FPGAs),[16].

3. Performance Evaluation

The purpose of this paper is to improve the architecture of heterogeneous multi-homed devices or networks with high probability of packet loss, such as the wireless communication systems. While preserving adequate security for the user data, the proposed approach aims at increasing reliability and robustness of the connection by optimizing the data coding. We utilized the open-source OMNeT++ network simulation framework to demonstrate the proposed mechanism behaviour.

3.1. Transmission Efficiency

In the first simulation, we focused on the transmission efficiency, which was assumed as number of received to the number of retransmitted messages ratio. Compared to a load-balancing mechanism utilizing both data channels for data transmission; based on its nature, the proposed XOR approach does not require as many messages to be resent as the original load-balancing mechanism. This is due to the feature, which enables the receiver to reconstruct specific amount of messages which were not delivered as a result of loss.

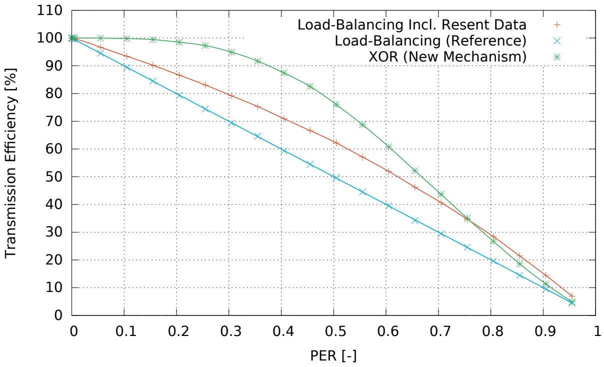

Fig. 4: Transmission efficiency.

The Fig. 4 demonstrates comparison of common load-balance method with and without retransmission with the proposed mechanism in terms of transmission efficiency. The load-balancing without resending lost data is the worst case in the entire monitored section because of the impact of packet error rate (PER) for both channels and the impossibility of any recovery. The XOR mechanism is very efficient up to packet error rate (PER = 0.8), where the load-balancing becomes more efficient. This is caused by various options for data reconstruction of the XOR mechanism. With the growing number of errors, the load-balance loses its natural advantage of two separate channels for the data transmission and the benefit of lost packet reconstruction in the new mechanism becomes more important. The efficiency turning point (PER = 0.8) describes situation where the new mechanism does not have enough data for the reconstruction because of extremely high error rate.

3.2. Effective Throughput

From the effective throughput perspective considering lossless environment, there is a clear benefit in utilizing both channels for data transmission in a load-balancing mode and not for redundancy as in the case of a new mechanism. Nevertheless with the increasing error rates (above PER = 0.25), it can be observed that the proposed mechanism becomes efficient.

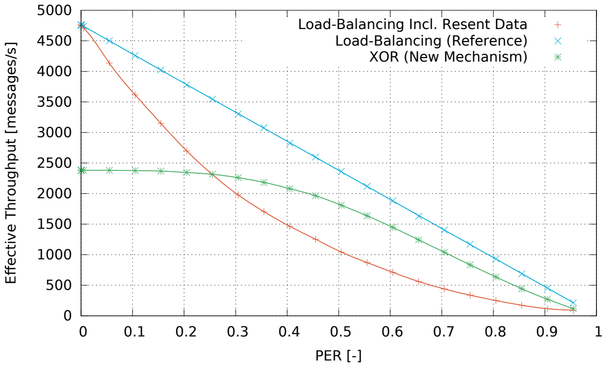

Fig. 5: Effective throughput.

Retransmissions of the data poses serious impact on effective throughput of the data; especially, shared wireless transmission technologies are sensitive to the amount of transmitted data and any data sent in addition has negative impact on the performance. In order to preserve generality of the result, we considered within the simulations that each lost message is resent only once and then assumed delivered. In other words, the probability a resent message will be lost again is put to zero. In a real world environment, such probability is not null, thus the effective throughput of the load-balancing mechanism with retransmissions would be far less effective (Fig. 5).

3.3. Practical Impact of Data Loss

By paying more attention to the fact, how does to lost data affects higher layer protocols, it can be seen that based on specific implementations of reliable protocols, such as the worldwide used transmission control protocol (TCP), can a single missing fragment of data cause retransmission of all consequent data or a more efficient method, such as the caching memory (buffer), is required to be implemented on both ends of the transmission path.

If the transmission systems operate in environment with higher value of error rate (PER), the size of the buffer is required to be increased with respect to the PER value. Otherwise with increasing PER value, the efficient throughput will further decrease as already received data will be required to be resent due to insufficient memory space in the buffer (Fig. 6).

The proposed XOR method utilizes buffers of a constant size. Therefore, it is unaffected by the actual PER value. Moreover, size of these buffers is given by a required number of messages correction possibility and its size is negligible compared to the neces-

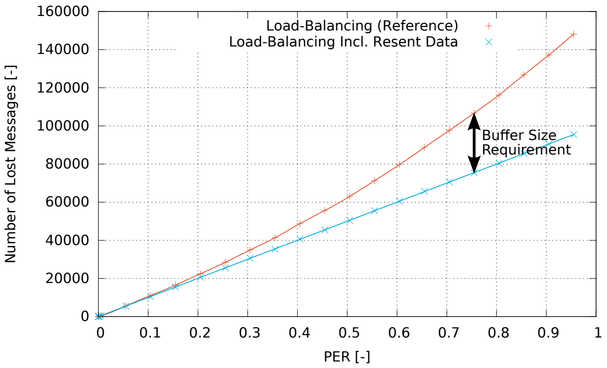

Fig. 6: Buffer size requirement.

sary buffer size in the case of the load-balance method including lost data retransmissions. Apparently, the extreme values of PER → 1 were evaluated for simulation and theoretical research purposes. We assume that the kind reader considers the practical aspects of using networks within such ranges.

4. Conclusion

The paper is focused on a novel secure transparent multi-homing architecture. We have evaluated standardized and non-standardized approaches, which are available, and have concluded that a secure and transparent solution for higher-level protocols is currently unavailable. Since our proposal is not based on dynamic routing protocols, it can be utilized not only for network connectivity backup, but also as an efficient solution used by the end devices. Moreover, the approach we have designed is high-performance in environments evincing variable parameters due to the proposed coding scheme, as it significantly reduces number of resent messages if these get lost as a result of increased packet error rate.

Currently, the solution utilizes two proprietary linux-based devices (a client and a server appliance) which can be considered as a relative disadvantage. On the other hand, the client-side is planned to be programmed as a software application (e.g. for mobile devices). We believe that its redesign and utilization of more than two physical interfaces can prepare such solution for standardization, without which it can hardly consider wider application.

Acknowledgment

This work was supported by the Grant of the Ministry of the Interior of the Czech Republic, No. VG20122014095, “Development of adaptable and data processing systems for high-speed, secure and reliable communication in extreme conditions”, and was researched in cooperation with CERTICON.

References

[1] HABAK, K., K. A. HARRAS and M. YOUSSEF. Bandwidth aggregation techniques in heterogeneous multi-homed devices: A survey. *Computer Science - Networking and Internet Architecture.* 2013, vol. abs/1309.0542. Available at: `http://arxiv.org/abs/1309.0542`.

[2] MACURA, L., J. ROZHON, F. REZAC, J. VYCHODIL and M. VOZNAK. Secured monitoring probe with highly redundant WAN connection. In: *Proceeding of the conference Knowledge in Telecommunication Technologies and Optics.* Ostrava: VSB–Technical University of Ostrava, 2010, pp. 118–121. ISBN 978-80-248-2330-0.

[3] ABLEY, J., B. BLACK and V. GILL. *Goals for IPv6 Site-Multihoming Architectures.* RFC 3582, 2003. Available at: `https://www.ietf.org/rfc/rfc3582.txt`.

[4] KUNTZ, R., J. MONTAVONT and T. NOEL. Multihoming in IPv6 mobile networks: progress, challenges, and solutions. *Communications Magazine.* 2013, vol. 51, iss. 1, pp. 128–135. ISSN 0163-6804.

[5] ABLEY, J., K. LINDQVIST, E. DAVIES, B. BLACK and V. GILL. *IPv4 Multihoming Practices and Limitations.* RFC 3582, 2005. Available at: `http://www.ietf.org/rfc/rfc4116.txt`.

[6] GHAMARI, S., M. SCHELLMANN, M. DILLINGER and E. SCHULZ. An approach for automated spectrum refarming for multiple radio access technologies. In: *Telecom World (ITU WT), 2011 Technical Symposium at ITU.* Geneva: IEEE, 2011, pp. 187–192. ISBN 978-1-4577-1148-0.

[7] KOCUR, Z., J. VODRAZKA, P. MACEJKO and V. MARIK. *Adaptive system for increasing the speed and reliability of data transmission in a packet network with optimized delay.* Utility Model no. 25772. August 2013.

[8] FRAGOULI, C., J. Y. LE BOUDEC and J. WIDMER. Network coding: An instant primer. *ACM SIGCOMM Computer Communication Review.* 2006, vol. 36, no. 1, pp. 63–68. ISSN 0146-4833. DOI: 10.1145/1111322.1111337.

[9] ALSHWEDE, R., N. CAI, S. R. LI and R. W. YEUNG. Network information flow. *IEEE Transactions on Information Theory.* 2000,

vol. 46, iss. 4, pp. 1204–1216. ISSN 0018-9448. DOI: 10.1109/18.850663.

[10] YEUNG, R., S. R. LI, N. CAI and Z. YHANG. Network coding theory. *Foundation and Trends in Communications and Information Theory*. 2005, vol. 12, iss. 4-5, pp. 241–381. ISSN 1567-2328.

[11] HO, T. and D. S. LUN. *Network Coding: An Introduction*. Cambridge: Cambridge University Press, 2008. ISBN 978-1-139-47018-6.

[12] KATTI, S., H. RAHUL, W. HU, D. KATABI, M. MEDARD and J. CROWCROFT. XORs in the Air: Practical Wireless Network Coding. *IEEE/ACM Transactions on Networking*. 2008, vol. 16, iss. 3, pp. 497–510. ISSN 1063-6692. DOI: 10.1109/TNET.2008.923722.

[13] LOU, W., W. LIU and I. FANG. Spread: improving network security by multipath routing. In: *Military Communications Conference*. Boston: IEEE, 2003, pp. 808–813. ISBN 0-7803-8140-8.

[14] DWORKIN, M. *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. U.S.: National Institute of Standards and Technology, 2006.

[15] MCGREW, D. A. and J. VIEGA. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In: *5th International Conference on Cryptology*. Berlin: Springer, 2005, pp. 343–355. ISBN 978-3-540-24130-0. DOI: 10.1007/978-3-540-30556-9_27.

[16] ABDELLATIF, K. M., R. CHOTIN-AVOT and H. MEHREZ. Efficient AES-GCM for VPNs using FPGAs. In: *56th International Midwest Symposium on Circuits and Systems*. Columbus: IEEE, 2013, pp. 1411–1414. ISBN 9781479900657. DOI: 10.1109/MWSCAS.2013.6674921.

About Authors

Matej ROHLIK received his M.Sc. and Ph.D. degree from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 2008 and 2012 respectively. His research is focused on security of future mobile networks and broadcast security. He is actively involved in projects focused on security of the next generation mobile networks and high speed mobile transmission optimization.

Petr CHLUMSKY received his M.Sc. from the Czech Technical University in Prague in 2010. Since 2010 he has been studying Ph.D. degree. His research interests include wireless transmission, network coding and network simulation.

Tomas VANEK received his M.Sc. degree in telecommunication engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 2000. In 2008 he received the Ph.D. degree in applied cryptography from Czech Technical University in Prague, Faculty of Electrical Engineering. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include cryptography, advanced network protocols and VoIP security.