Security vulnerabilities of network coding

Journal:	*IEEE Communications Magazine*
Manuscript ID:	Draft
Topic or Series:	Open Call Article
Date Submitted by the Author:	n/a
Complete List of Authors:	Gholibegi, Mozhdeh; Tampere University of Technology, Department of Communications Engineering Karimzadeh, Morteza; Tampere University of Technology, Department of Communications Engineering Moltchanov, Dmitri; Tampere University of Technology, Department of Communication Engineering Koucheryavy, Yevgeni; Tampere University of Technology, Department of Communications Engineering
Key Words:	network coding, security

Security vulnerabilities of network coding

M. Gholibegi[1], M. Karimzadeh, D. Moltchanov, Y. Koucheryavy
Department of Communications Engineering
Tampere University of Technology
E-mail: mozhdeh.gholibegi@tut.fi

Abstract. It is already around ten years since the network coding paradigm has been introduced as a new communication approach with the aim of improving the performance of network protocols by breaking the rule of traditional store and forward approach and allowing intermediate nodes to encode received packets before forwarding them out. As of today, the concept is still immature and demands more extensive research in many areas with security being one of the most important and critical aspects due to the specific characteristics of network coding such as packet mixing and increased redundancy. The matter is even more challenging in environments such as wireless multi-hop networks which are inherently vulnerable and suffer from intrinsic security drawbacks due to unstable shared wireless communication medium, dynamic communication environment, possibly limited memory space and computing capabilities, etc. These and additional weak points including severe vulnerabilities against different type of attacks like eavesdropping and corrupted data injection make the existing security solutions intended for traditional wired networks or even one-hop wireless networks non-applicable to wireless multi-hop networks. Hence, there is a high demand for new security solutions complying with the specific requirements of these networks. The purpose of this article is review security vulnerabilities and challenges of network coding and to present and discuss possible solutions and countermeasures.

Keywords: network coding, security, wireless multi-hop networks

1. Introduction

The concept of network coding is not ripe yet as it has been emerged approximately ten years ago and there are only few limited practical applications aimed for testing the functionality and efficiency of the concept (see e.g. [1,2]). Thus, the search for possible practical applications is nowadays complemented with analysis of the network coding techniques identifying challenges and vulnerabilities at the early stages of development when it is still not applied extensively. As performance improvement has been the main objective of network coding, not enough attention has been paid to the security aspects resulting in design proposals having multiple security drawbacks.

[1] Corresponding author's e-mail: mozhdeh.gholibeigi@tut.fi

According to the basic principle of network coding, intermediate nodes of a network are allowed to perform special coding operations on the received data packets while in the traditional store and forward approach they simply forward them unchanged. In other words, a node can act as an encoder encoding the received data packets from input links into one or more packets before sending them to output links. As a result, network coding can be implemented as an extension of the classic store and forward approach.

Network coding is a promising approach improving throughput, reliability and robustness of a network against failures and erasures. In both wired and wireless environment it may fully utilize the capacity of a network allowing getting close to its theoretical limit. As a result, it has attracted a lot of interest from the research community over the recent years. Most studies published over this time span almost exclusively focused on developing various encoding strategies for network performance improvement. However, for these schemes to be ready for practical implementation, other aspects of network coding must also be addressed.

Security as one of the main aspects may hamper network coding implementation and adumbrate performance improvements as its basic design goal. The random mixture of data packets as the main feature of network coding leads to severe security drawbacks, i.e. allowing intermediate network nodes to encode received packets simply turns them to potential attackers. In wireless systems this matter is even more challenging and security policies must be stricter to address inherent weaknesses of communication medium. Our main goal is to introduce and discuss security vulnerabilities and possible countermeasures proposed for network coding so far. We believe that our work can be helpful for both newcomers to the field looking for a point to start from and experienced scientists in the area of network coding looking for up-to-date review of the work that has been done so far in context of security.

The rest of this paper is organized as follows. Section 2 gives a bit more detailed description of network coding. In Section 3 security aspects of network coding are discussed. We also give two general classifications of general coding schemes from the security point of view. Security vulnerabilities for both intra-flow and inter-flow network coding are discussed in Sections 4 and 5, respectively. Conclusions are provided in the last section.

2. Network coding gains

The concept of network coding-based information delivery has been introduced in the seminal paper of Ahlswede *et al* [3]. It was originally developed to improve capacity of wired networks operating in multicasting mode. For detailed introduction to the network coding we refer to e.g. [4]. Here, we mainly concentrate on gains network coding can provide.

Network coding concept allows intermediate relay nodes to act as a special encoder mixing incoming packets instead of simply replicating them to one or a set of output interfaces. This scheme is illustrated in Fig. 1 using the well-known butterfly network example. In this example node *N3* after *XOR*ing the *X* and *Y* messages forwards the resulting message to the end nodes *N5* and *N6* through the node *N4*. Then, the nodes *N5* and *N6* can decode *Y* and *X* by *XOR*ing the received messages. Usage of *XOR* coding in this network allows channels to be used just once instead of twice when messages are delivered separately.

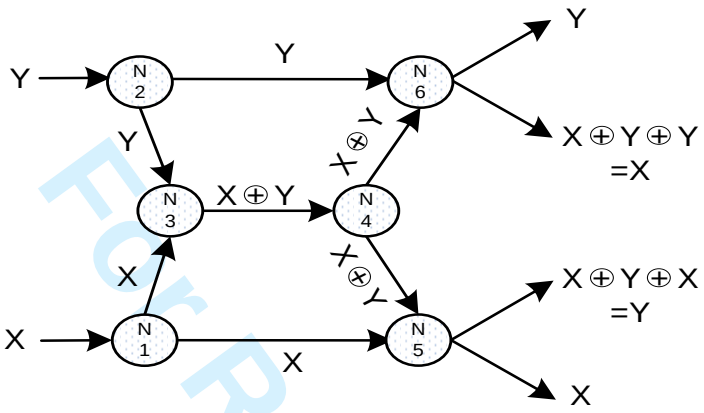
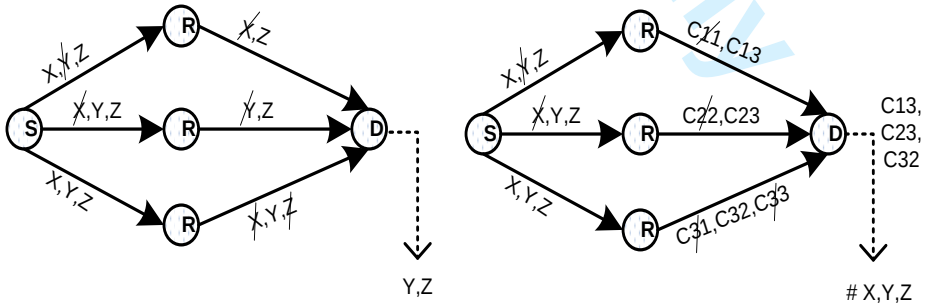


Fig. 1. Example of network coding in multicasting scenario.

In networks without intermediate coding, destination nodes need to receive a specific amount of successive packets sent by the source node to decode the information correctly. As it is demonstrated in Fig. 2, usage of network coding provides the receiver the ability to decode and exploit all sent information by receiving a reasonable number of independently encoded packets. Therefore, a lossy network (e.g. wireless multi-hop networks such as wireless sensor systems) could be made more reliable by using network coding mechanisms.



Network without coding *Network with coding*

Fig. 2. Improving reliability using network coding.

Benefits of network coding makes it a perfect choice for broadcast-based wireless multi-hop networks, where nodes are often subject to resource limitations in terms of power, buffer and link

capacity. In various special cases such as sensor, mesh and vehicular networks links between end systems are inherently intermittent due to dynamic network topology. To enable efficient communication, intermediate mobile or stationary nodes are responsible for acting as relays using the store-and-forward mechanism. If the buffer of a node is filled up and new data arrives before delivery of the stored messages, the node may drop them or delete the old messages to store new ones. As shown in Fig. 3, usage of network coding makes it possible to encode newly arrived and old data in the buffer and generate new encoding vectors as a function of all received data without deleting any packet in the buffer or dropping new ones.

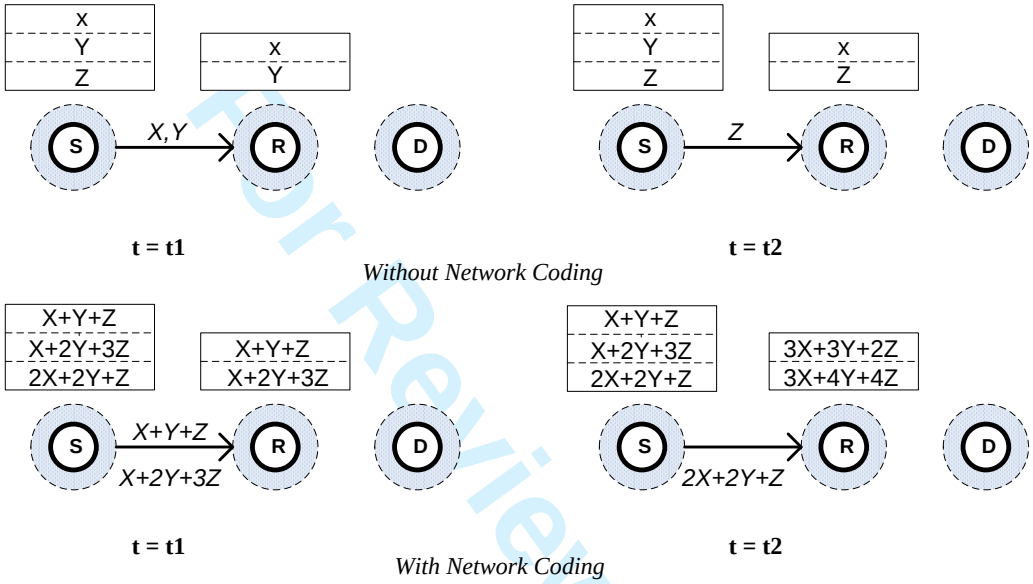


Fig. 3. Improving buffer performance using network coding.

Implementing network coding imposes additional processing overhead due to encoding at intermediate nodes and decoding at the destination nodes. In general, more complex coding offers better performance at the expense of higher processing overhead. As a result, in those environments, where processing power is a scarce resource simple network coding algorithms such as *XOR* or linear random permutations need to be used.

- **XOR coding**

In this method, the intermediate relay nodes broadcast *XOR*ed version of messages to all nodes after receiving them from the source nodes. Corresponding destination nodes should be able to decode the sent messages by *XOR*ing the received messages once again. It is important to note that only those nodes knowing one of two elements of the encrypted messages can recover the sent messages. Therefore, this property improves the security of wireless transmission as malicious nodes do not have access to any of the elements of the encrypted messages.

- **Linear coding**

As the name suggests, mixing the received messages at intermediate nodes is carried out using linear combinations. The coefficients of this combination are taken from a finite field that needs to be the same for all nodes. If the received packets and their combinations are denoted by x_i and g_i respectively, the linear combination of the packets is given by $\sum_i g_i \times x_i$. The destination nodes can decrypt the encrypted data by receiving n combinations out of N sent messages provided that the rank of combinations equals to n. If the coefficients are set randomly at intermediate nodes receiving more combinations of messages results in higher probability of correct decoding. To achieve this random linear network coding can be used. In this mechanism each node combines input packets using random coefficients in a random linear manner. Gaussian elimination algorithm can be used at destination nodes to solve the matrix with n equations to retrieve N unknown parameters that represent the sent messages.

3. Security in network coding

Network coding suffers from multiple weak points, especially, in context of security. The matter becomes entitled to more emphasis if we talk about wireless environment that has a lot of inherent vulnerabilities, e.g. easily accessible shared communication medium, dynamic network topology, limited processing and energy resources of mobile nodes, etc. Due to the packet mixing property of network coding, the destructive impact of attacks is more drastic, as for instance, only one corrupted packet injected by a malicious intermediate node during the encoding procedure corrupts all encoded packets forwarded by that node and the nodes receiving these corrupted packets encode and forward them and so on, resulting in pervasive distribution of corrupted packets and significant performance degradation. Besides avoiding message recovery by destinations, such attacks may also exhaust the network and nodes resources which is a critical challenge for resource-constrained wireless communication.

There are various network coding schemes based on the techniques used to encode multiple input packets together into one or more output packets. From the security point of view they could be classified into two general schemes. The first classification is based on dependency of packets contributing in one mixing process to one or more separate flows. These are *intra-flow* and *inter-flow* network coding. The principle difference is illustrated in Fig. 4 using two simple communication scenarios. As one can see, the encoded packets belong to the same flow in case of intra-flow coding or to multiple flows in case of inter-flow coding.

Similarly to intra-flow network coding, inter-flow approach utilizes opportunistic listening and coding at intermediate nodes to reduce the amount of redundant transmissions and improve

performance. It is inherently more secure than intra-flow network coding against passive attacks such as eavesdropping. The reason is that in this case it is more difficult for a malicious node to exploit meaningful information from the encoded packets belonging to separate flows. On the other hand, inter-flow network coding is more fragile against active attacks such as pollution attack. Indeed, by combining packets from different flows a single corrupted packet may result in several flows to be polluted. By increasing the number of flows contributing to a coding session, the impact of pollution would be much more drastic and network-wide. Moreover, employing some special schemes such as coding-aware routing metrics to increase the level of contribution in coding sessions results in more severe effect of pollution attacks.

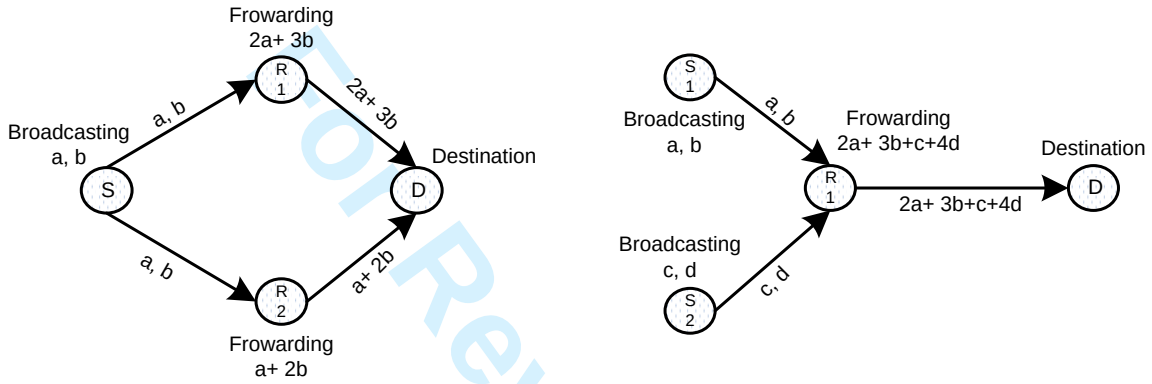


Fig. 4. Example of intra-flow and inter-flow network coding.

Another classification of network coding schemes is based on the information used to make encoding and routing decisions. We distinguish between *stateless* network coding that does not use state information to decide when and how to encode input packets and *stateful* network coding that need to be partly or even completely aware of state information such as network topology, neighboring links and nodes capacities to be able to make encoding decisions. Random linear network coding (RLNC) is an example of stateless network coding which is a distributed scheme for combining separate data flows. As an example of stateful network coding we can refer to COPE protocol in which a coding layer between the IP and MAC layers is relied upon to detect encoding opportunities and then utilize them to forward several packets in one transmission [5]. It could be shown that the stateful approach is more vulnerable against malicious nodes, as a malicious node can easily inject wrong state information and misconduct encoding and routing decisions. For example, a malicious node could impersonate itself as another node or introduce itself being only a hop distant from the destination.

4 Intra-flow network coding

In intra-flow network coding batches (or so-called generation) of multiple packets from the same flow are transmitted by the source node. Intermediate nodes carry out linear encoding on the packets belonging to a batch and send these encoded packets. Linear combinations of packets of the current batch are regularly broadcasted by the source node till receiving an acknowledgement for that batch from the receiver. Then, the source node carries out the same process for the next batch. Intermediate nodes, known as forwarders, forward encoded packets throughout the network to deliver them to the destination nodes. Linearly independent packets overheard by each forwarder are stored in its buffer. Then, the forwarder node forwards new encoded packets by linearly mixing packets stored its buffer. The receiver node is able to decode all packets of the current batch by receiving sufficient number of linearly encoded packets of that batch. Then, the receiver sends an acknowledgement for it and the source node broadcasts the next batch.

Operation of intra-flow network coding can be classified into four phases. These are forwarding mode selection and rate assignment, data forwarding, delivery of acknowledgement packets and coding/decoding phases. Below we describe these phases identifying their major steps, possible attacks and countermeasures.

4.1 Forwarding node selection and rate assignment

This phase is intended for determining the group of forwarder nodes and the rate of forwarding encoded packets for each of them. Factors such as interference among nodes, relative distances of intermediate nodes to the source and destination nodes, measured via a routing metric such as expected transmission count (ETX [6]), and fairness among separate flows must be taken into account to choose forwarding nodes and forwarding rates optimally. To carry out these calculations a centralized scheme utilizing a link state graph stored at each node can be used by intra-flow network coding protocols. Generally, these centralized computations are carried out and sent by the source node to intermediate nodes along with data packets. Link state graph is the main input of this phase. Each node regularly floods the information regarding the quality of its local links throughout the network. Some security vulnerabilities, such as those ones mentioned below, may lead to network nodes having improper link state graphs. This false information affects selection of forwarders and associated rates negatively.

- *Link quality modification/falsification*

Incorrect quality metrics are introduced by malicious nodes for their neighbor links. Since the scope of this information is local restraining these attacks is difficult. A reactive scheme that detects and separates the attacker has been proposed in [7]. A special case of this attack is when

link qualities introduced by other nodes are altered by an attacker during the flooding. Message authentication techniques such as digital signatures can be utilized to cope with these attacks.

- *Wormhole*

Attackers belonging to this category introduce bogus links between network nodes and negatively affect the topology and link state knowledge of these nodes. Although the traditional security schemes such as packet leases and connectivity-based solutions can be used as countermeasures, their high computation and communication overheads make them inappropriate for network coding-based systems. Simply put, they decrease throughput of such systems absorbing the most important advantage of network coding. Designing security schemes to counter wormhole attackers ensuring proper link state and network topology information is quite challenging labor to overcome. To the best of our knowledge, security schemes that would be well-suited for wireless networks have not been proposed yet.

4.2 Data forwarding

Forwarding nodes and the receiver nodes overheard and store linearly independent encoded packets. The random linear mixings of buffered packets are sent by the forwarder nodes at the rate computed in the first phase. By overhearing sufficient number of linearly independent encoded packets from a batch, the receiver node is able to decode all packets of that batch by solving a set of linear equations. This phase is mostly threatened by packet pollution and packet dropping.

- *Packet pollution*

According to the basic rule of network coding intermediate nodes are allowed to encode the received packets to form new encoded packets rather than just forwarding them. This principle makes the network coding scheme inherently vulnerable against pollution attacks as even a single polluted packet may epidemically affect the whole network and degrade the performance significantly. Proposed solutions for countering pollution attacks generally incur high computation and communication overheads affecting performance improvement as the basic design objective of network coding. The solution proposed in [8], which is based on simple linear checksum and time asymmetry, is rather light compared to other schemes.

- *Packet dropping*

Due to intrinsic redundancy and opportunistic listening network coding systems have a level of intrinsic security. However, as a result of attempts to optimize the forwarding node selection and rate assignment with the aim of decreasing interference and the number of retransmissions,

recent schemes are generally more fragile against node misbehaviors such as packet dropping. Since the number of packets transmitted by a node and transmission times depends on opportunistic packet receptions at that node, conventional solutions for countering packet dropping attacks such as Watchdog [9] are not applicable to systems based on network coding.

4.3 Acknowledgements delivery

To ensure reliably communication acknowledgements are sent from the destination to the source through the highly qualified paths. The source node starts to broadcast the next batch after receiving the acknowledgement for the current batch. To timely deliver acknowledgements intermediate nodes assign high priorities to acknowledgement packets and force the next hops to send an explicit acknowledgement. This phase of intra-flow network coding is subject to ACK injection and modification, ACK dropping and ACK delay attacks.

- *ACK injection/modification*

In this type of attacks the attacker node injects fictitious acknowledgements or modifies an acknowledgement packet making the source node moving to the next batch of packets untimely. Delivery of partial batches makes the receiver node unable to decode all packets in batches. Message authentication techniques such as digital signatures can be used to cope with these attacks.

- *ACK dropping*

Malicious nodes in the acknowledgement delivery paths may simply drop ACK packets. As a result, the source node continues to send the same batch repeatedly. Attackers may also alter path metrics or use wormhole links to increase the probability of being in the acknowledgment delivery route. General techniques identifying malicious nodes based on the amount of dropped ACK packet can be used.

- *ACK delay*

Unlike the previous attacks, in this case attacker nodes do not drop acknowledgement packets but delay the delivery of them. These attacks are more furtive compared to the ACK dropping attacks and significantly decrease the system performance by lengthening batch transmission times. This attack is more complicated to deal with compared to ACK injection/modification or ACK dropping. The reason is that delays in the ACK delivery process are not always signatures of malicious node behavior and may happen naturally as a result of computational constraints. Thus, no effective mechanisms are expected to appear to deal with this type of attacks.

4.4 Packet coding and decoding

This is the main phase of intra-flow network coding. In this phase the source node encodes plain packets of a generation (*n* packets) as linear combinations using elements of a random coding vector as coefficients and sends them to forwarder nodes. Forwarder nodes form new encoded packets by computing random linear combinations of the received encoded packets and using elements of a random coding vector as coefficients of this mixing. By receiving *n* linearly independent encoded packets and solving *n* linear equations, the destination node is able to decode all packets of that generation.

- *Traffic injection/flooding*

A malicious node may purposely flood the network with useless traffic. Even if the number of such nodes is fairly small this type of attack may affect performance of the whole network. Since intermediate nodes serve as encoders and relays, network resources and computational resources of nodes are affected. Nodes authentication procedures are required to deal with these attacks.

5 Inter-flow network coding

According to the basic principle of inter-flow network coding a node that has packets from a number of flows intended to be forwarded to different next hops does not separately unicast packets to proper next hops. Instead, it mixes the packets together and broadcasts the new mixed packet to all intended next hops at once. Inter-flow network coding contains the following phases: discovery of coding opportunities, packet forwarding, routing integration and packet coding/decoding.

5.1 Discovery of coding opportunities

Coding opportunities at a node implies finding appropriate packets to encode together such that the encoded packets are decodable at downstream nodes. Based on the scope of coding opportunities inter-flow network coding protocols can be divided into *localized* (single-hop) and *global* (multi-hop) coding protocols. In the localized protocols (e.g. COPE [5]) only adjacent neighbors are considered for possible coding opportunities, while in the second case all nodes of the network are considered as candidates. In both cases the search for candidates is performed via discovery process that can be implemented using a certain routing protocol such as dynamic source routing (DSR, [10]) distributing information about coding opportunities. Below we mention attacks that modify the information about coding opportunities threatening this phase for both localized and global inter-flow network coding.

- *Misreporting packet reception information*

In localized inter-flow network coding an attacker can report an untrue packet reception information by impersonating honest nodes. This type of attacks may result in sending packets that are non-decodable by the next hop. These unusable packets are not acknowledged. Thus, the source node continues to send non-decodable packets repeatedly. Message authentication mechanisms can be used to cope with these attacks. As packet reception reports are sent frequently these techniques must be extra light. Notice that ACK aggregation mechanisms may not be a viable alternative due to various attacks targeting the ACK delivery process.

- *Link state pollution*

Localized inter-flow network coding systems use link state information to derive packet reception situations at other nodes. Hence, attacks affecting link state graphs of nodes may result in improper packet reception information leading to transmission of encoded packets that are not decodable. Node authentication is to be used to deal with this type of attacks.

- *Neighbor set pollution*

In global inter-flow network coding systems the neighbor nodes set information collected during the route discovery procedure is used to determine coding opportunities by a node. Modifying route request packets or introducing bogus links via wormholes may result in collection of false neighbor nodes set information. As a result of this untrue information a node loses coding opportunities or sends non-decodable packets to other nodes. Authenticating neighbor node set information can be achieved using secure routing protocols such as Ariadne [11]. Notice that securing neighbor node set information is essential for countering wormhole attacks too.

5.2 Packet forwarding

In inter-flow network coding each intermediate node must send encoded packets to several next hops instead of sending them only to one next hop as is in the traditional routing. To ensure a certain level of reliability, especially, in wireless networks with random channel access such as IEEE 802.11, the transmitting node must ensure that all next hops have received a certain encoded packet. To address this issue a *pseudo-broadcast* mechanism has been proposed in [12]. Using this mechanism the source node transmits the encoded packets using the next hops as the MAC receiver. The packet retransmissions will be continued several times until the specified MAC receiver receives and acknowledges the packet. There are multiple specific attacks associated with this phase.

- *Packet pollution*

In this case an attacker node injects polluted packet into the network. According to inter-flow network coding, packets from different flows are encoded together and an encoded packet k is referred to as polluted packet if it is marked as encoded using $b_1,b_2,\ldots,b_m$ (each one from a separate flow), but k is not equal to $b_1 \oplus b_2 \oplus \ldots \oplus b_m$. Pollution attack results in epidemic propagation of corrupted packets that may affect the whole network. As a result of complicated inter-flow dependencies and epidemic propagation of polluted packets across several flows the effect of pollution attack is much more destructive compared to intra-flow network coding. Solutions proposed to cope with pollution attack in intra-flow network coding systems target identifying and dropping corrupted data packets. Since packets from different flows contribute to a single encoded packet solutions such as homomorphic signatures proposed for countering pollution attacks in intra-flow network coding do not work in this case. Notice that in the case of intra-flow network coding several paths between source and destination are used to route data packets, while in inter-flow network coding systems often a single path is used to route data packets form source to destination. To the best of our knowledge, there is only one solution proposed to cope with pollution attacks in inter-flow network coding systems [13], where the authors proposed a countermeasure mechanism named CodeGuard. It uses proactive node confirmation and reactive bit-level traceback to detect attackers. In addition, digital signatures are used by nodes to authenticate messages. It is assumed that there are authenticated communication channels between neighboring nodes that is implemented using either digital signatures or message authentication codes (MAC). The bit-level traceback introduced in this scheme traces the history of polluted packets to detect the attacker.

- *Packet overcoding*

This type of attacks is specific to inter-flow network coding systems. According to the discovery of routing opportunities, packets contributing to an encoded packet are determined such that these new encoded packets are decodable by downstream nodes. As a result of overcoding attack, more packets than assumed are encoded together by a malicious node. Consequently, decoding operation cannot be performed properly at downstream nodes. Since overcoded packets transmitted by malicious nodes do not conform to the format of general corrupted packets these types of attacks are extremely difficult to cope with. Particularly, solutions proposed for countering pollution attacks are not directly applicable in this case. Using information obtained at the discovery of coding opportunities phase and ensuring that selected opportunities are conformant are important points to be taken into account when designing effective security solutions in this case.

- *Packet underdecoding*

This type of attack is similar to the previous one. The difference is that in the previous case the attacker is an encoding node, while in this case attack is performed by a decoding node. According to the discovery of coding opportunities, decoding nodes make use of specific number of overheard packets to decode received encoded packets. Using fewer overheard packets by a malicious decoder node may make downstream nodes unable to decode forwarded packets.

- *Packet dropping*

In inter-flow network coding systems there is an exhortation to path sharing with the aim to increase coding opportunities. A malicious node can misuse this property to have more chances to be chosen for multiple routes. Then, the attacker can drop packets from a lot of flows and disturb their communication. Packet dropping can be carried out by a forwarding node or an encoding/decoding node. The difference is that, if dropping is performed by a forwarding node it is detectable using conventional solutions for packet dropping attacks such as Watchdog [9]. However, this mechanism does not work when an encoding/decoding node performs packet dropping.

- *ACK injection or modification*

An attacker may inject fictitious acknowledgements or modify correct ones. As a result, packet retransmission sessions can be untimely halted. Thus, packets cannot be received properly at next hops. Due to highly frequent acknowledgement packets, the message authentication mechanisms used for countering ACK injection/modification attacks must be extra light in terms of computation and communication overheads.

5.3 Routing integration

To improve throughput, instead of relying on conventional routing protocols characterizing coding opportunities based on episodic route interlacing, inter-flow network coding can use specific coding-aware routing protocols. According to these protocols paths are selected such that encoding gain is maximized. These protocols operate based on coding-aware metrics that describe the cost of links allowing encoding. Choosing the optimal paths based on these coding-aware metrics can be carried out in central or distributed manner. In addition to checking link and path metrics validity, as is in conventional routing protocols, coding-aware routing protocols need to ensure the validity of reported coding opportunities too. A malicious node may hamper the functionality of protocols by modifying coding opportunities reports. For example, a malicious node may report high coding opportunities to increase the probability of being selected to multiple paths and disturb a lot of data

flows. Since in addition to topology information coding opportunities rely on the current flow structures in the network, development of mechanisms for ensuring the validity of reported coding opportunities is expected to be more challenging compared to development of mechanisms for ensuring security of topology metrics such as link and path qualities.

5.4 Packet coding and decoding

In intra-flow network coding all forwarding nodes may encode the received packets while only receivers are able to perform decoding. In the case of inter-flow network coding systems encoding could be performed only at nodes sitting in the crossroad of flows of interest and any such node having overheard required packets may carry out decoding process. Other nodes of the network forward packets without encoding them.

- *Traffic injection/flooding*

  Similarly to intra-flow network coding injection of malicious traffic is the main security threat at this phase. Notice that in the case of inter-flow network coding the effect could be much more profound as encoding and decoding is now performed over multiple flows. Thus, development of nodes authentication schemes is even more important for this case.

6 Conclusions

Since network coding is relatively new communication approach and performance improvement has been almost exclusively considered as the main and only design goal of it, various aspects of network coding are rather unsought with security as one of the most important of them. The basic rule of network coding not only results in new security threats, but also makes coded-enabled systems more vulnerable to existing attacks. Due to inherent vulnerabilities of wireless media the matter is even more critical in one of the most important foreseeable application area of network coding – wireless multi-hop networks. Table 1 summarizes common security attacks in network coding environment. Since some of these attacks are inherent for any network environment (e.g. traffic analysis, replay), they have not been specifically addressed them in the text.

To make proposing security solutions easier, we classified network coding approaches proposed so far into two general categories, intra- and inter-flow network coding techniques. For both categories we specified security attacks and discussed possible countermeasures. In order to have practically secure network coding systems offering both performance improvement and security the trade-off between the level of security and performance must be taken into account. For example, developing a system for space communications the security level can be compromised in favor of increased throughput. One the other hand, systems for military applications needs to incorporate the

highest possible security level while still ensuring adequate performance. Thus, the security must be addressed at the system development phase. Most existing network coding security schemes do not conform to this requirement and lead to complex systems incurring large processing overhead.

Table 1. Common security attacks, description and impact.

Attack	**Description**	**Impact**
Fabrication	Injecting messages with wrong information	Increasing path lengths, prevention of flows
Impersonation	Masquerading as another node	Misrouted traffic flows
Replay	Retransmitting old messages	Misrouting based on the outdated messages
Wormhole	Tunneling between malicious nodes	Increased path lengths, prevention of flows
Blackhole	Relying on other nodes' control traffic	Communication reduction, loss of connection
Eavesdropping	Exploiting data not intended for that node	Disclosure of information
Modification	Altering data packets maliciously	DOS, undecodable packets, traffic obviation
Packet dropping	Dropping data packets purposely	Loss of data flows
ACK altering	Dropping acknowledgements	Misdirecting the source node
Pollution	Injecting corrupted packets	Undecodable packets
Traffic analysis	Analyzing the network traffic patterns	Compromising user privacy

Packet pollution is the most common and destructive attack in network coding systems due to the nature of network coding. As a result, it has been studied more comprehensively compared to other threats. However, there is a wide range of various security threats that still remain completely or partially unaddressed resulting in exciting future work for network coding security. The current research in this field needs to be concentrated on proposing lightweight security solutions for a particular application area and also introducing countermeasures for threats that are not covered yet.

References

[1] M. Wang, B. Li, "Lava: a reality check of network coding in peer-to-peer live streaming," In Proc. IEEE Infocom, Anchorage, US, pp. 1082-1090, 2007.

[2] H. J. Kang, A. Yun, E.Y. Vasserman, H. T. Lee, J. H. Cheon, Y. Kim, "Secure Network Coding for a P2P System," In Proc. ACM Conference of Computer and Communications Security (CSS), pp. 1-3, 2009.

[3] R. Ahlswede, N. Cai, S.Y.R. Li, and R.W.Yeung, "Network information flow," IEEE Trans. Inf. Theory, V.46, N.4, pp. 1204-1216, July 2000.

[4] R. Yeung, S.-Y. Li, N. Cai, Z. Zhang, "Network Coding Theory," Foundations and Trends in Communications and Information Theory, V.2, N.5, NowPublishers, 2005.

[5] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft. "XORs in the air: practical wireless network coding," In Proc. ACM SIGCOMM, Pisa, Italy, pp.243–254, 2006.

[6] D. S. J. D. Couto, D. Aguayo, J. C. Bicket, R. Morris, "A high-throughput path metric for multi-hop wireless Routing," In Proc. of ACM MOBICOM'03, pp. 134–146, 2003.

[7] J. Dong, R. Curtmola, C. Nita-Rotaru, "On the pitfalls of using high-throughput multicast metrics in adversarial wireless mesh networks," In Proc. SECON'08, pp. 224–232, June 2008.

[8] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks," In Proc. 2nd ACM Conference on Wireless network Security, Zurich, Switzerland, 2009.

[9] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In Proc. MOBICOM, August 2000.

[10] D. B. Johnson, D. A. Maltz, J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," edited by Charles E. Perkins, Ch. 5, pp. 139–172, Addison-Wesley, 2001.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," Wireless Networks, pp.21–38, 2005.

[12] J. Le, J. C. S. Lui, and D. M. Chiu, "DCAR: distributed coding-aware routing in wireless networks," In Proc. IEEE Trans. Mob. Comp, V.9, N.4, pp. 596-608, Apr. 2010.

[13] J. Dong, R. Curtmola, C. Nita- Rotaru, D. Yau, "Pollution attacks and defenses in wireless inter-flow network coding systems," In Proc. IEEE Wireless Network Coding Conference (WiNC), Boston, US, pp. 1-6, 2010.