Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 85-90 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Secure Network Coding Schemes: Comparsions and Broader Perspective

M. I.Nazeer[1] and M. S. Shaikh[2]

[1] Center for Research in Ubiquitous Computing, FAST-NUCES, Karachi, Pakistan
[2]Department of Electrical Engineering, FAST-NUCES, Karachi, Pakistan
irshad.nazir@nu.edu.pk , shahid.shaikh@nu.edu.pk
cor
rec

Abstract: In this paper we compare various schemes of Secure Network Coding proposed so far. With the goal to find an efficient approach toward secure Network Coding, we classify and analyze different schemes used to secure Network Coding enabled networks in terms of confidentiality, authentication and level of the security strength they provide. Based upon comparative study of different schemes we come across the conclusion that a generalized model for secure network coding may work in broader perspective.

Keywords: Netwrk Coding; secure network coding; wireless networks.

INTRODUCTION

The roots of Network Coding theory lies in classical graph theory as one of the major applications of graph theory is representation of data communication networks. In a network graph *G(V,E), V* is the set of all vertexes that represent communicating nodes and E is set of all edges that represent the communication links between pairs of vertexes *(u,v)* where *u* and *v* belongs to *V*. These nodes can be of three types: nodes that originate data are called source nodes, nodes for which the transmitted data is intended are called sink nodes while nodes that neither act as source nor as sink are called intermediate nodes. Associated with each link e belonging to E is its capacity *C(e)* which represents the maximum data rate supported by the link *e*. Given a network graph with a source or a number of sources, a sink or number of sinks and capacities of all its edges, in general, there exist many paths that can carry data from source to sink. The path that carries largest amount of data in a given amount of time as compared to all other paths is known as maximum flow path. In graph theory, there are many well known methods, for example, Ford Fulkerson and Bellman Ford Algorithms, to find maximum flow in a given network. Finding maximum flow in a particular network helps planning, better resource utilization, and makes operations cost effective. However, unfortunately, our traditional communication networks do not provide the rate of communication as an order of this maximum flow. This is due to the obvious fact that routing mechanisms follow store and forward approach that do not take link capacities into account. To incorporate maximum flows in data communication networks, Network Coding is a new paradigm that bridges this gap.

The earlier work on network coding is of theoretical nature (Yeung, *et al.,* 2007) which is why many of the earlier schemes do not meet the practical requirements. The later work eliminates those constraints. The proponents and opponents have made their points on network coding. The most obvious issue related to network coding is data security. As intermediate nodes have access to the information being transmitted to a particular sink so these nodes may inject false data or modify the received data or may perform any other malicious activity. So a node can be compromised or link data can be eavesdropped. The security issue of network coding has been considered by many researchers and developments as a result of these efforts have given birth to the paradigm of Secure Network Coding (Cai, *et al.,*2002).

In this work, we select various Secure Network Coding Schemes and analyze them in terms of different security requirements and other related parameters such as security strength. According to our knowledge this the first work that provides an in-depth comparative study of nine different Secure network Coding sachems and suggest for a combing two schemes to meet the desired security using network Coding. The next section provides the literature review. The details comparison of the schemes studied is given in section II. Second part of the same section provide the trade-offs of

The first is sponsored by HEC through Indigenous fellowship program.

different requirements. The last section provides result analysis and concludes our work.

MATERIALAND METHOD OR EXPERIMENT

A. Literature Review

Initial literature on network coding elaborated the advantages of coding over routing (Ho, *et al.,* 2003). Later, Network Coding was successfully tested at various layers of OSI stack and in various domains. Some schemes incorporated network coding at physical layer (Zhang, *et al.,*2009) some at network layer (Chou, *et al.,* 2003) some at application layer for example (Gkantsidis, *et al.,* 2005 and Dimakis, *et al.,* 2004) while a cross-layer implementation is also given in (Katti *et al.,* 2009). As an example of different domains, coding can improve the throughput in application layer overlay networks (Li, *et al.,* 2003).

The first approach to construct network codes using network coding was the linear network codes (Li, *et al.,* 2003). The construction of such codes that are optimal for single source and meet the maximum flow bound is presented in (Li *et al.,* 2003), but this construction of linear codes does not take care of security of the associated links. In order to ensure secure transmission of the data over publicly accessible links, threshold cryptography is useful (Desmedt *et al.,* 1989). In threshold cryptography, the secret key to access transmitted data is distributed among *n* participating nodes instead of a single node, as, for a single node there are more chances of being compromised than that of all the nodes at the same time. Using Shimmer's secret sharing (Shamir, 2007), *k* out of *n* shares are required to recover the secret key from the distributed shares. The model presented in (Li *et al.,* 2003) was modified to incorporate a security condition for a single source on the principle of threshold secret sharing if an adversary has access to a limited number of links of the network (Cai, *et al.,* 2002). This security condition is then extended to the case of multiple sources in the extended work by the same authors (Cai, *et al.,* 2002). While traditional secret sharing challenges an adversary to get *k* out of *n* shares, some schemes to secure network coding are suggested on filtered secret sharing (Feldman *et al.,* 2004) that challenges an adversary with k out of all linear combination of n shares. The capacity analysis of the approach presented in (Cai, *et al.,* 2002) is given in (Feldman, *et al.,* 2004) that put a question mark on the field size required for the construction of linear network codes. Another obvious observation of the above work (Cai *et al.,* 2007) is that it considers only the network security and no consideration is given to the network cost which is sum of costs (a number that quantifies the overhead to setup a link *e* of capacity *C(e)*) associated with each connection involved in the communication. To address both, the network security and network cost in the same problem, different approaches have been suggested. For example, using rank matrix codes network cost can be decreased [D. Silva et al., D. Silva et al. 2008]. Rank matrix codes can also provide security without modifying the underlying network code even if the adversary has access to arbitrary subset of the links (Silva *et al.,* 2009). In contrast to rank matrix codes, a heuristic based approximate solution of the problem takes care of both the network security and network cost for linear network codes (Tan *et al.,* 2006).

As far as theoretical foundations are concerned, Network Coding theory is sufficiently mature. However, practical difficulties still remain as far as the implementation is concerned. One way to make Network Coding practical is to choose the encoding coefficients randomly (Lima, *et al.,* 2003). A security protocol is also proposed in (Vilela, *et al.,* 2008) that uses random linear network codes. This protocol is good to provide confidentiality of data by locking the encoding coefficients but has poor performance against any arbitrary modification from nodes that mimic as the trusted nodes but are in fact compromised. This sort of attack is called Byzantine attack. An approach to deal with Byzantine attacks is suggested in (Ho, *et al.,* 2004).

Another way of secure network coding is purely based upon cryptography. As a compromised node can harm the network traffic so a signature based scheme can detect and filter these un-authenticated packets in Network Coded transmissions (Yu, *et al.,* 2008). Another approach for modification attacks based on signature is described in (Oggier, *et al.,* and Han 2007). Hash function homomorphism can be applied to make the Network Coding computationally strong against modifications and eavesdropping, if the number of nodes to be accesses by adversary is equal to at most the capacity of the network (Zhou, *et al.,* and Katz, *et al.,* 2006). Despite the fact that the Network Coding is itself vulnerable to security, some researchers proved Network Coding to be beneficial in distributing the secret key (Oliveira *et al.,* 2006).

The recent work on secure network coding (Cui *et al.,* 2003) considers the problem in comparatively wider perspective, assuming adversary can access an arbitrary subset of links which are not constrained to be of equal capacity. Flaws in several schemes that claim to be secure are reported in (Wang, *et al.,* 2008). For example, schemes based on threshold cryptography will remain no more secure if an adversary is able to compromise a node that has *k* outgoing edges (Wang, *et al.,* 2008).

B. Classification, Comprisons and Trad-offs

We studied a number of schemes of secure network coding as described in Section II. **(Table 1)** contains the names of those with an English letter Identity (ID). A particular scheme shall later be identified with this letter for simplicity.

Table I. Schemes Under Study

Sr.	Schemes	ID
1	Byzantine Modification Detection in Multicast Networks (T. Ho *et al.*,)	A
2	Secure Network Coding with a Cost Criterion [J. Tan et al.]	B
3	Signature-based Scheme (Z. Yu *et al.*,)	C
4	Security for Wiretap Networks via Rank-Metric Codes (D. Silva *et al.*,)	D
5	Universal Secure Network Coding via Rank-Metric Codes (D. Silva *et al.*,)	E
6	SPOC (Secure Practical Network Coding) (J. P. Vilela *et al.*,)	F
7	Secure Network Coding Against the Contamination and Eavesdropping Adversaries (Y. Zhou *et al.*,)	G
8	Secure Network Coding via Filtered Secret Sharing (Y. Desmedt *et al.*.)	H
9	A Network Coding Approach to Secret Key Distribution (P. F. Oliveira *et al.*,)	I

We observe that there is need to classify these schemes on the basis of fundamental security requirements, i.e. schemes that provide Confidentiality only, schemes that provide Authorization only, and schemes that provide both Confidentiality and Authorization. **(Fig. 1)** shows the classification in this regard.

There are two ways to make a Network Coding scheme secure. One is to modify the existing Network Coding Schemes to incorporate security requirements called inner codes and second is to append another code to existing network coding scheme without modification called outer codes. We classify the schemes under study on the basis of this, in **(Table 2)**.

Table 2. Classification On Basis Of Inner Or Outer Codes

Inner Codes	Outer Codes
A, B, G	C, D, E, F

The types of attacks expected during Network Coding enabled transmission and the ability to counter one or more of these attacks by a Secure Network Coding schemes is summarized in **(Table 3)**.

We note that almost all Secure Network Coding schemes under study have some limitations. These limitations are listed in **(Table 4)**.

In the end we pay our attention to the security strength of each scheme under our study that is given in **(Table 5)**.

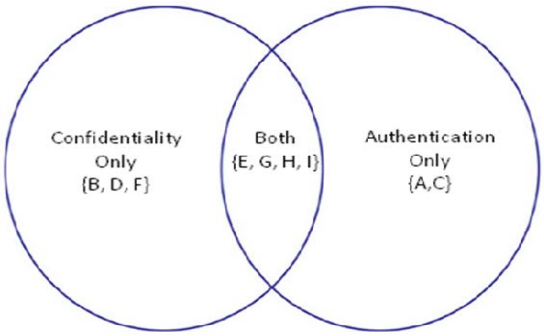


Fig. 1. Classification of selected schemes

Table. 3. Attacks Counterd By Schemes Under Study

Sr.	Attacks	Schemes
1	Byzantine Modification	A
2	Disclosure	B, F
3	Pollution	C, E, G, H
4	Wiretapping	D, E
5	Evesdropping	G, H
6	All of above	I

Table 4. Limitations Of Schemes Under Study

Scheme	Limitations
A	At detination one or more unmodified packets still may arrive.
B	A wiretapping adversary has interest for a known subset of transmitted messages.
C	Adversaries may come in a position to fully control the compromised forwarders.
D	Whitepaper has access to a subset of arbitrary chosen links.
E	Some information can be leaked but this is of no use for an adversary.
F	Inermediate nodes have access to the identifiers of the sinks and intermediate nodes have limited computational power.
G	The number of independent packets available to the eavesdropper is less than the multicast capacity of the network.
H	Filtered secret sharing is unsolvable in certain cases.
I	Immune to single point of failure.

Table. 5. Limitations Of Schemes Under Study

Scheme	Security Strength
A	Information Theoretic
B	Average; probability of eavesdropping as low as 0.01
C	Equivalent to RSA
D	Information theoretic
E	Information theoretic
F	Equal to the strength of cryptographic algorithm
G	Not information theoretically secure but secure enough for the application
H	Information theoretic
I	Information theoretic

Ideally a good secure network coding scheme should consume less time and resources of the network, not be vulnerable, have ease of implementation and have good security strength. But during our study of a number of such schemes, we find some tradeoffs. First, both the network cost and the network vulnerability, if network cost is decreased this would result in increased vulnerability. Second, computational overhead and the strength of security, if computational overhead is decreasing this may reduce the security strength. Last, outer and inner code, *i.e* either the network code has to be modified to provide security or the outer code has to be designed based on the specific network code used.

RESULTS DISCUSSION AND CONCLUSIONS

We may get almost desired results if we combine some of the suitable candidate proposed protocols. The idea that comes to our mind is to use a layered approach as shown in **(Fig. 2)**.

For example we use the scheme suggested in (Oliveira *et al.,* 2007) for key distribution while scheme proposed in (Vilela *et al.,* 2008) as an outer code to provide secure network Coding enabled transmissions. As a result of this we can get the desired results.

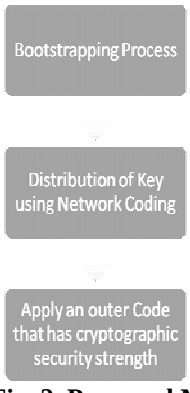


Fig. 2. Proposed Model

To, conclude, we presented a detailed comparison of different Network Coding security protocols in terms of their capabilities. We found that none of these serves to give benefits approximately equal to the benefits of network coding alone however we saw that we may trade off network capacity, bandwidth or network cost with security. A combination of good candidates from the available pool of security scheme may serve our purpose with throughput not equal to the throughput of network coding itself but conceivably greater than the throughput of traditional communication networks.

ACKNOWLEDGEMENT

This is the extended version of our own paper presented and published as Conference proceedings in "International Conference on Computers & Emerging Technologies" (ICCET 2011) held on 22-23 April 2011 at Shah Abdul Latif University, Khairpur, Sindh, Pakistan.

REFERENCES

Cai, N. and R. W. Yeung, (2002) "Secure Network Coding," in *Proc. IEEE ISIT*, Lausanne, Switzerland,

Cai, N. and R. W. Yeung, (2007) "A Security Condition for Multi-Source Linear Network Coding," in *Proc. IEEE International Symposium on Information Theory 2007*, Nice, France.

Cai, N. and R. W. Yeung, (2002) "Secure network coding," in *Proc. IEEE International Symposium on Information Theory 2002*, Lausanne, Switzerland, 323Pp.

Chou, P. Y. Wu, and K. Jain, (2003) "Practical network coding," *in Proc. Allerton Conference on Communication, Control, and Computing*, Allerton, USA.

Cui, T., T. Ho, and J. Kliewer, (2009) "On Secure Network Coding Over Networks With Unequal Link Capacities," CoRR, abs/0911.0467.

Dimakis, A. G., P. B. Godfrey, M. J. Wainwright, and K. Ramchandran, (2007) "Network coding for distributed storage in peer-to-peer systems," in *Proc. IEEE INFOCOM*, Anchorage, Alaska.

Desmedt, Y. and Y. Frankel,(1989) "Threshold cryptosystems," *Advances in Cryptology CRYPTO 89*, Springer-Verlag, 307-315.

Feldman, J., T. Malkin, C. Stein, and R. A. Servedio,(2004) "Secure network coding via filtered

secret sharing," in *Proc. 42nd Annual Allerton Conf. Commun., Control and Comput.*, Monticello, Illinois.

Feldman, J., T. Malkin, R. A. Servedio, and C. Stein, (2004) "On the Capacity of Secure Network Coding," in *Proc. 42nd Annual Allerton Conference on Communication, Control and Computing*, Monticello, Illinois.

Gkantsidis, C. and P. Rodriguez, (2005) "Network Coding for large scale content distribution," in *Proc. IEEE INFOCOM*, Miami, USA.

Han, K., T. Ho, R. Koetter, M. Medard, and F. Zhao, (2007) "On network coding for security", in Proc. Military Communications Conference, 2007 MILCOM 2007, Orlando, Florida .

Ho, T., R. Koetter, M. Medard, D. R. Karger, and Michelle Effros, (2003) "The Benefits of Coding over Routing in a Randomized Setting," in *Proc. IEEE International Symposium on Information Theory 2003*, Yokohama, Japan,.

Ho, T., B. Leong, M. Medard, D. R. Karger, R. Koetter, and Michelle Erosz, (2004) "Byzantine Modification Detection in Multicast Networks using Randomized Network Coding," *ISIT 2004. Proceedings. International Symposium Information Theory*, Chicago, Illinois.

Katz, J., D. Boneh, D. Freeman, and B. Waters, (2009) "Signing a Linear Subspace: Signatures for Network Coding," in *Proc. Public-Key Cryptography (PKC).*

Katti, S., H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, (2006) "XORs in the air: practical wireless network coding," in *Proc. SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, New York, NY, USA: ACM Press, 243–254.

Lima, L., M. Medard, and J. Barros, (2007) "Random Linear Network Coding: A free cipher,?" in *Proc. IEEE ISIT'07*, Nice, France.

Li, S.Y.R. (2003) "Linear Network Coding," *IEEE Trans. on Information Theory*, vol. 49, No. (**2**): 23-43.

Oggier, F. and H. Fathi ,(2009) "An Authentication Code against Pollution Attacks in Network Coding," CoRR, abs/0909. 3146Pp.

Oliveira, P. F. and J. Barros, (2007) "Network Coding Protocols for Secret Key Distribution," in *Proc. On the Move to Meaningful Internet Systems 2007,* ISOTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007, LNCS, Vilamoura, Portugal, November 25-30.

Shamir, A. (2007) "How to share a secret", *Communications of the ACM*, vol. 22, No. (**2**): 612–613.

Silva, D. (2008) "Universal Secure Network Coding via Rank-Metric Codes," in *Proc. IEEE International Symposium on Information Theory 2008*, Toronto, Ontario, Canada.

Silva, D. and F. R. Kschischang, (2008) "Security for Wiretap Networks via Rank-Metric Codes," in *Proc. IEEE ISIT 2008*, Toronto, Ontario, Canada.

Tan, J. and Muriel Medard, (2006) "Secure Network Coding with a Cost Criterion," in *Proc. 4th International Symposium Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, (WiOpt'06)*, Boston MA.

Vilela, J. P., L. Lima, and J. Barros, (2008) "Lightweight Security for Network Coding," in *Proc. IEEE International Conference Communications ICC '08*, Beijing, China.

Wang, Y. (2008) "Insecure "Provably Secure Network Coding" and Homomorphic Authentication Schemes for Network Coding," unpublished available: http://www.sis.uncc.edu/~yonwang/papers/ncattack.pdf
Y. Zhou, H. Li, and J. Ma, "Secure Network Coding Against the Contamination and Eavesdropping Adversaries," CoRR, abs/0805.2286, .

Yu, Z., Y. Wei, B. Ramkumar, and Yong Guan, (2008) "An Efficient Signature-based Scheme for Securing Network Coding against Pollution Attacks," in Proc. IEEE INFOCOM 2008 The 27th Conference on Computer Communications, Phoenix, AZ.

Yeung, R. W., S.-Y. R. Li, N. Cai, and Z. Zhang, (2006) *Network Coding Theory*. Boston-Delft: now Publishers Inc.

Zhu, Y., B. Li, and J. Guo, (2004) "Multicast with Network Coding in Application-Layer Overlay Networks," IEEE Journal on Selected Areas in Communications, vol. 22, No. (**1**): 88-94.

Zhang, S. and S. C. Liew, "Applying Physical-layer Network Coding in Wireless Networks,"CoRR, abs/0910.2604.