Anonymous Communication Scheme for Wireless Mesh Network Based on Network Coding

Nan Guo, Shuang Yu*, and Tianhan Gao
Northeastern University, Shenyang, Liaoning 110000 China
guonan@mail.neu.edu.cn, yushuangneu@foxmail.com, gaoth@mail.neu.edu.cn

Abstract

Wireless Mesh Network, holding the features of self-organization, strong scalability, low deployment cost, is considered to be the most competitive technology for broadband wireless access service. However, the security and privacy issues become the bottleneck for WMN's rapid popularization. Network coding, which can improve both network throughput and anonymity, is adopted for the communication security in WMN recently. However, the related network-coding based anonymous communication schemes suffer from the efficiency and security issues. In this paper, an efficient anonymous communication scheme for WMN is proposed, which combines the opportunistic routing protocol and network coding approach. The global coding vector is protected with the lightweight permutation encryption mechanism. In addition, the security and performance analysis demonstrate that the proposed scheme can provide strong privacy protection for WMN communication with high network throughput.

Keywords: wireless mesh network, anonymous communication, network coding, permutation encryption

1 Introduction

With the rapid development of wireless communication technology and wireless network equipment, the demands for wireless network service are becoming more and more urgent. Wireless Mesh Network (WMN), as one of the ideal technologies to solve the last mile access problem, has become the best communication technologies for wireless broadband access backbone networks with the features of self-simple configuration, strong scalability, robustness, and low deployment cost [1]. As wireless multi-hop network, security is the main obstacle for the wide spread of WMN. And as individuals increasingly emphasize privacy preservation, anonymous communication has become an important research topic of WMN security [8].

In WMN, the use of network coding can effectively optimize data forwarding, and ensures anonymity and high network throughput [13]. ANOC [14] presents a method based on cooperative networking to remove the conflict between traditional anonymous routing protocol and network coding. [15] and [3]transmit the encoded routing information and packets through different paths to grantee security and anonymity. PRIV-CODE [9] tries to achieve communication unlinkability based on packet delay techniques. A-WEOR [7] borrows the core idea from MORE [2] to combine network coding and opportunity routing, which increases the network throughput and anonymity. Even though the above schemes are able to guarantee the anonymity of communication in WMN, large amount of encryption and decryption operations are involved, that greatly reduces the network performance. HEFs [4] employs the homomorphic encryption (HEFs) to encrypt the Global Encoding Vector (GEV) at source node, the intermediate nodes

Research Briefs on Information Communication Technology Evolution (ReBICTE), Vol. 3, Article No. 7 (October 15, 2017)
*Corresponding author: Department of Software College, Northeastern University, Shenyang, Liaoning 110000 China, Tel: +86-186-4030-1601

do not need to decrypt the encoded packet to obtain GEV, which ensures the security of the packets. Zhang Peng et al. propose a secure network coding scheme P-Coding [12], depending on classical permutation encryption to protect the GEV and the message on the source node. The computational cost of P-Coding is far less than HEFs. ALNCODE [11] encrypts the packets at the intermediate nodes of the multiple streams. The correlation between the uplink GEV and the downlink GEV of each stream is eliminated to against anti-flow analysis. In 2015, Jin Wang et al. proposed a wireless network anonymous communication program ULNC [10] for mobile devices in terms of ALNOCDE. Unfortunately, these schemes assume that a secure anonymous routing protocol is existed to determine the routing path on the source, while the traditional anonymous routing protocols fail to exploit the advantages of network coding to improve network throughput.

In this paper, an efficient anonymous communication scheme for WMN is proposed, which combines the opportunistic routing protocol and network coding. The GEV is protected with the lightweight permutation encryption mechanism. In addition, the security and performance analysis demonstrate that the proposed scheme can provide strong privacy protection for WMN communication with high network throughput.

The rest of the paper is organized as follows. Section 2 briefly describes the relevant technologies involved in our scheme. Section 3 elaborates the network-based WMN anonymous communication scheme. Section 4 provides a security and performance analysis of the proposed scheme. Section 5 concludes the paper and presents the future research works.

2 Related technologies

2.1 Network Coding

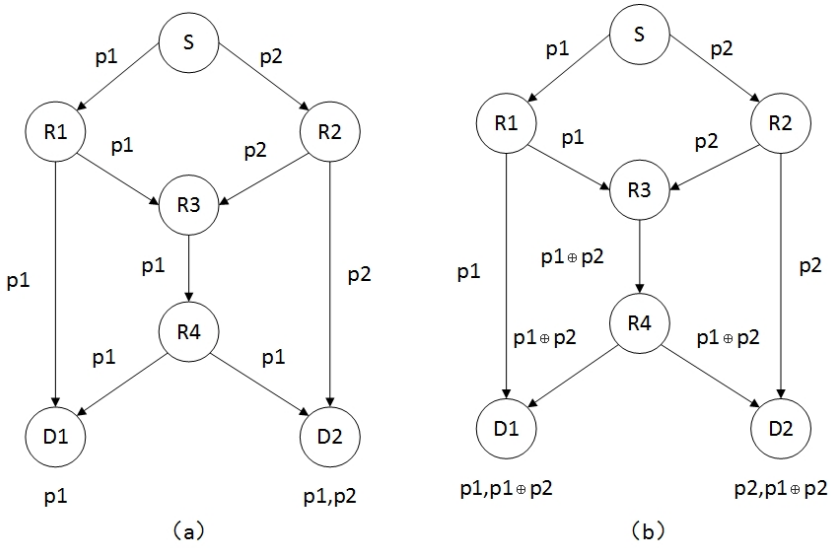


Figure 1: The Butterfly Network of Single Source

Taking the typical butterfly network as an example, the basic principle of network coding is shown in Figure 1. Assuming that the source node S wants to send 1-bit data to the destinations D1 and D2, and the link is unicast only 1-bit data can be transmitted at a time. Figure 1 (a) illustrates the traditional routing method, where R3 can only transfer 1-bit data to R4, and R4 relay the data to the destination D1, D2. Figure 1 (b) shows the network coding scenario. R3 encodes p1, p2 and then scents the encoding

Table 1: Notation and Definition

Notation	Definition
GEV	Global encoding vector
IRSP	Initial routing setup packet
MAP	Message acknowledgment packet
p_i	Raw packet
P_i	Encoded packet
R_i	Node identification
key_i	Symmetric encryption key
S_New	New data flow ID
S_Old	Old data flow ID
flag1	Node type flag(R for forwarding node, D for destination node)
flag2	Packet type flag(0 for IRSP, 1 for MAP)
padding	Padding part
P_key	The key of permutation encryption

results(p1 $\oplus$ p2) to R4. R4 then forwards the result to the destination. Due to the radio network broadcasting characteristics, D1 and D2 are able to receive p1 $\oplus$ p2. Then D1 decodes p1 $\oplus$ p2 according to p1 from R1 to obtain p2. Similarly, D2 decodes p1 $\oplus$ p2 according to p2 from R2 to obtain p1. In this case, R3 and R4 achieve a 2-bit transmission rate that greatly improves the network throughput.

2.2 Permutation Encryption

P-Coding [10] proposes a lightweight security network coding scheme (PE), which adopts traditional permutation encryption mechanism to protect the encoded packets and GEV. The original information is replaced by the permutation result while the contents are not changed. As a result, the corresponding linear operation on each bit is exchangeable and holds the following properties:

(1) Additivity: $E_k(m+n) = E_k(m) + E_k(n)$

(2) Scalar Multiplicativity: $E_k(t \cdot m) = E_k(t) \cdot E_k(m)$

3 The proposed scheme

3.1 Adversary model

We assume that the adversary is a passive attacker who can passively monitor network traffic but can not modify, discard, or insert any packets in the communication. The main goal of the adversary is to infer the communication relationships between the source nodes and the destination nodes.

In order to facilitate the follow-up description, Table 1 is given to show the relevant notations.

3.2 The anonumouys communication scheme based on network coding

Before the communication starts, each node in WMN pre-generates its own public-private key pair and shares its public key. Moreover, every node shares a broadcast key with its neighbors, which is used for point-to-point encryption on some information such as flow ID. The anonymous communication scheme (NC-WMN) is divided into five stages: initial route establishment, source encoding, intermediate forwarding, destination decoding, anonymous message acknowledgment.

3.2.1 Initial route establishment

The primary purpose of the initial route establishment phase is to determine the forwarding node list and to notify the relevant nodes. Unlike traditional routing protocols, there is no explicit next hop address in the opportunistic route. All nodes that are closer to the destination node are potential next hop nodes. In NC-WMN, we employ a similar approach to [2] to judge the closer node from the destination node and add them to the forwarding_list.

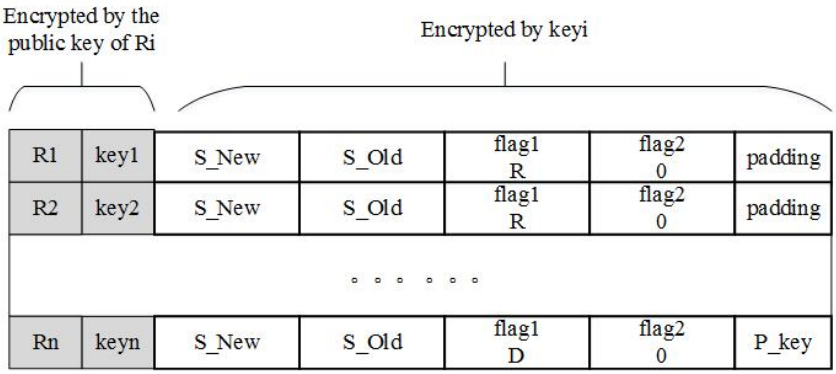


Figure 2: Initial Routing Setup Package

The source node then constructs the IRSP based on the forwarding_list. As shown in Figure 2, IRSP is composed of many sections whose descriptions are shown in Table 1. Each section is encrypted with the symmetric key key_i, which is generated by the source node for the corresponding node R_i. The key_i and R_i are carried at the head of each section and are encrypted using the public key of the node R_i.

After the IRSP is generated, the source node broadcasts the packet through flooding. When a node receives an IRSP, it first decrypts each section header in the packet with its own private key. If the node can successfully decrypt the header, it is the forwarding node of this session. Afterwards, the node uses key_i to decrypt the subsequent part of each section to get the relevant information, stores the flow ID (S_new) and forwards the packet. Otherwise the node forwards the packet directly.

3.2.2 Source Encoding

At this stage, the source node encodes the data and sends them. The linear random network coding scheme [5] is used in our scheme because it does not need to consider the entire topology of the network, that is suitable for WMN.

Firstly, the source node divides the data into h slices $\{p_1, p_2, p_3, \ldots, p_h\}$ and appends the unit vector (header GEV) to each data slice header. In order to ensure the confidentiality of the encoding vector, PE is used to encrypt the entire packets as shown in Figure 3. The key used by PE is the key (P_key) shared with the destination node during the initial route establishment phase. After that, the coding coefficients are randomly selected to linearly encode the data slices to generate h coded packets P_i. When the encoding completes, the source node adds flow ID to the header of P_i and encrypts it with its broadcast key. Then the source node continuously broadcasts these encoded packets until the Message Acknowledgement Packets (MAP) is received.

3.2.3 Intermediate Forwarding

After receiving a data packet broadcasted by a neighbor node, the intermediate node decrypts the flow ID of the packet using the shared broadcast key with the neighbor node. If the flow ID is stored in the node

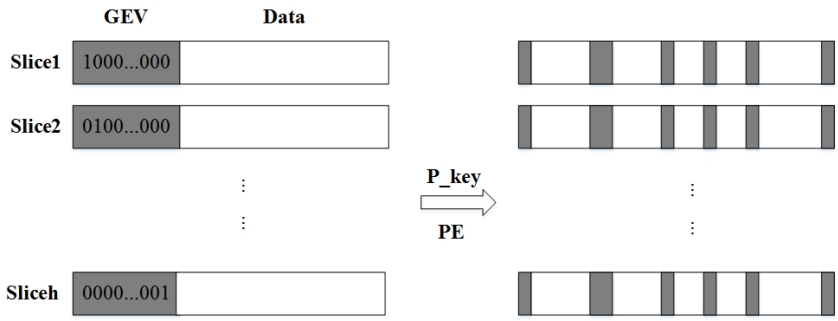


Figure 3: PE Instructions

list, it indicates that the node is a forwarding node of the flow. Then the intermediate node randomly selects the coding coefficients to encode the packet with the previously received packets from the same flow to form a new encoded packet. The intermediate node uses its own broadcast key to encrypt the flow ID of the message and then broadcast the encoded packet. Since PE encryption is transparent to the intermediate node, the intermediate node does not need to decrypt the GEV before encoding.

3.2.4 Destination Decoding

After receiving the encoded packets, the destination node decrypts the encoded packet through the pre-established replacement encryption key (P_key) to obtain the encoded packet and the GEV. After receiving h linearly encoded packets, the GEV of the h packets are composed of a matrix G of $h \times h$, thus the destination node can use Gaussian elimination method [6] to obtain the inverse matrix G^{-1} of G and then decoding to get the original data.

3.2.5 Anonymous Message Acknowledgment

In order to ensure the reliable transmission of the message, it is necessary for the destination node to return the MAP after receiving the data from source node. The destination node constructs MAP as the same format as IRSP. When the forward node receives the MAP, the packets associated with the old flow ID (S_old) are cleared, the new flow ID (S_new) is stored.

Through the anonymous message acknowledgment, the destination node declares a new flow identifier to each forwarding node, and negotiates the new P_key with the source node. After receiving the MAP, the source node encrypts the next message with the new P_key and the new flow ID(S_new).

4 Security and Performance Analysis

4.1 Security Analysis

During the initial route establishment phase and anonymous message acknowledgment phase, the source node uses the forwarding nodes public key to encrypt the message which prevent the forwarding node from judging the identity of the source node in terms of the key. The IRSP and MAP are broadcasted over the network that does not contain information about the source node and the sink node. Since all messages are encrypted, the external attackers cannot get any useful information. Moreover, even if the internal node is compromised, it doesn't know the identity of the source/destination node as well as other intermediate nodes. NC-WMN adopts PE to protect the contents of the encoded packets and GEV, [12] points out that PE provides sufficient computational security. At the same time, since the message is

broadcasted and the flow ID is encrypted, the attacker can not carry out the flow analysis attack. And because of network coding's characteristic of confusion, some methods such as content connection and time correlation are invalid. In summary, NC-WMN is able to provide security and anonymity protection.

4.2 Performance analysis

NC-WMN depends on lightweight PE to protect packet and GEV. Since the permutation function and the linear combination operation are exchangeable, the re-encoding of the intermediate node can be performed transparently on the encrypted packet. Obviously, this mechanism can greatly improve the efficiency of the system, since there is no need for any additional operation on the intermediate node. The computational overhead required by the source node to protect the GEV of each encoded packet is $O(n)$ memory copy operations. The computational cost required for a random linear network coding is $O(n^2)$ multiplication operations. Compared to the computational overhead of network coding, the overhead of a memory copy operation is negligible. Therefore, the computational cost of our scheme is approximately equal to the computational cost of network coding. No additional computational overhead is introduced during the anonymous communication.

5 Conclusion

Aiming for the anonymous communication issues in WMN, an anonymous communication scheme based on network coding is proposed in this paper. Opportunity routing and network coding are combined to achieve anonymous communications and protects the packet and the GEV through a lightweight permutation encryption scheme. The security and performance analysis show that NC-WMN is robust and effective.

In the future research work, we will focus on faster network coding mechanisms in WMN and explore more efficient anonymous communication solutions based on network coding.

Acknowledgments

This work was supported by National Natural Science Foundation of China under [Grant Number 61402095].

References

[1] I. F. Akyildiz and X. Wang. A survey on wireless mesh networks. *IEEE Communications Magazine*, 43(9):S23–S30, 2005.

[2] S. Chachulski, M. Jennings, S. Katti, and D. Katabi. Trading structure for randomness in wireless opportunistic routing. *Acm Sigcomm Computer Communication Review*, 37(4):169–180, 2007.

[3] G. H. Duan, W. P. Wang, J. X. Wang, and L. M. Yang. Anonymous communication mechanism with multi-paths network coding. In *Proc. of the 2009 IEEE Global Telecommunications Conference (GLOBECOM'09), Honolulu, Hawaii, USA*, pages 1–6. IEEE, November 2010.

[4] Y. Fan, Y. Jiang, H. Zhu, J. Chen, and X. S. Shen. Network coding based privacy preservation against traffic analysis in multi-hop wireless networks. *IEEE Transactions on Wireless Communications*, 10(3):834–843, March 2011.

[5] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, September 2006.

[6] D. S. Lun, T. Ho, N. Ratnakar, and R. Koetter. *Network Coding in Wireless Networks*. Springer Netherlands, 2006.

[7] N. Shah and D. Huang. A-weor: Communication privacy protection for wireless mesh networks using encoded opportunistic routing. In *Proc. of the 2010 IEEE Conference on Computer Communications Workshops (INFOCOM'10), San Diego, California, USA*, pages 1–6. IEEE, March 2010.

[8] H. Silva, A. Santos, and M. Nogueira. Routing management for performance and security tradeoff in wireless mesh networks. *International Journal of Information Security*, 14(1):35–46, 2015.

[9] Z. Wan, K. Xing, and Y. Liu. Priv-code: Preserving privacy against traffic analysis through network coding for multihop wireless networks. *Proc. of the 2012 IEEE Conference on Computer Communications Workshops (INFOCOM'12), Orlando, Florida, USA*, 131(5):73–81, March 2012.

[10] J. Wang, K. Lu, J. Wang, J. Zhu, and C. Qiao. Ulnc: An untraceable linear network coding mechanism for mobile devices in wireless mesh networks. *IEEE Transactions on Vehicular Technology*, 65(9):7621–7633, November 2016.

[11] J. Wang, J. Wang, C. Wu, and K. Lu. Anonymous communication with network coding against traffic analysis attack. In *Proc. of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM'11), Shanghai, China*, pages 1008–1016. IEEE, April 2011.

[12] P. Zhang, Y. Jiang, C. Lin, and Y. Fan. P-coding: Secure network coding against eavesdropping attacks. In *Proc. of the 2010 IEEE Conference on Computer Communications Workshops (INFOCOM'10), San Diego, California, USA*, pages 1–9. IEEE, March 2010.

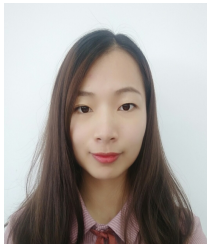
[13] P. Zhang and C. Lin. *Anonymous Routing for Wireless Network Coding*. Springer International Publishing, 2016.

[14] P. Zhang, C. Lin, Y. Jiang, P. P. C. Lee, and J. C. S. Lui. Anoc: Anonymous network-coding-based communication with efficient cooperation. *IEEE Journal on Selected Areas in Communications*, 30(9):1738–1745, October 2012.

[15] W. U. Zhenqiang and M. A. Yalei. A novel anonymous communication model:coding mix. *Journal of Wuhan University*, 57(5):401–407, 2011.

Author Biography

Nan Guo received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. Her research interests are security and privacy in social network and digital identity management.



Shuang Yu received the BE degree in Software College from Northeastern University in 2016. Currently she is taking a master's course at Graduate School of Software College, Northeastern University. Her research interests include anonymous communication and privacy protection for wireless mesh network security.

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.