ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Network Coding based Privacy Preservation Technique for Multi-Hop Wireless Networks

Prof. Santosh kumar Bandak, Jyoti Neginal

***Abstract*- Privacy is one of the critical issues in multi-hop wireless networks, where attacks such as traffic analysis and flow tracing can be easily launched by a malicious adversary due to the open wireless medium. Network coding has the potential to traffic analysis attacks since the coding/mixing operation is encouraged at intermediate nodes. On the other hand some other schemes are existing for privacy preservation such as mix based schemes, onion based schemes, proxy based schemes, but they all have some limitations. In this paper we propose a network coding privacy preservation technique in multi-hop wireless networks. This technique overcomes the limitations of the existing systems. With homomorphic encryption, the proposed technique offers three significant privacy preserving features, packet flow untracability and message content confidentiality. By using this technique we can detect how many hackers are trying to attack the network and also detect the target node to which node it's trying to attack.**

***Index Terms*— Network coding, homomorphic encryption, privacy preservation, traffic analysis.**

I. INTRODUCTION

Wireless Networks have been widely used due to their convenience, portability and low cost. But the limitation of wireless networks is its limited radio coverage's, poor system reliability, and lack of security and privacy. Highly promising solution for extending the radio coverage range of the existing wireless networks are multi-hop wireless networks, and they can also be used to improve the system reliability.

Due to the open wireless medium, MWNs are susceptible to various attacks, such as eavesdropping, modification /injection and node compromising [1]. These attacks may breach the security goals of MWNs, including confidentiality, integrity, and authenticity. In addition, some advanced attacks such as traffic analysis and flow tracing can also be launched by a malicious node to compromise user's privacy including source anonymity and traffic secrecy. In this paper we focus on the privacy issues such as traffic analysis/flow tracing, finding number of attackers and source anonymity in MWNs. Source anonymity refers to communicating through a network without revealing the identity or location of source nodes.

Manuscript received May, 2012.

***Prof. Santoshkumar.c.bandak,** Department of Comuter Science, Visveawaraiah Technology University, Belgaum / Poojya Doddappa Appa engineering College/ H.K.E Socity, (e-mail: santosh.bamdah@gmial.com), Gulbarga, India.*

***Miss Jyoti neginal department of Computer science,** Visvearaiah technology University, Belgaum/ poojya Daddappa Appa College of Engeneering Gulbarga, India 9986700546 e-mail: jyoti.c.neginal@gmail.com).*

We focus on the three fundamental information security issues in MWNs; efficient privacy preservation for source anonymity, which is critical to the information security of MWNs, the traffic explosion issue, which targets at preventing denial of service (DoS) and enhancing system availability. It is very challenging to efficiently thwart traffic analysis/flow tracing attacks and provide privacy protection in MWNs. Existing privacy-preserving solutions such as proxy based scheme[2], chaum's mix based schemes[3], and onion based shemes [4], may either require a series of trusted forwarding proxies or result in these schemes are low degradation in practice. Limitations of these schemes is low network performance, unpredictable delay, high computation cost and message transmission delay. Different from previous schemes, our research investigates the privacy preservation. Network coding technique overcomes the limitation of the existing scemes [5]. To secure Network coding some solutions have been produced. Information based schemes [6] can detect polluted messages at sinks. Cryptography based solutions include homomorphic hashing [7], homomorphic signature [8]. Another secure network coding based on hash functions are proposed in [9]. These solutions incur high computation overhead. And they all mainly focus on detecting and filtering out polluted messages. Little attention has been paid to the privacy issues, especially to protect the encoded messages from tracking or traffic analysis.

In this paper, based on network coding and homomorhic encryption functions (HEFs) [10],[11], we propose an efficient privacy preservation scheme for MWNs. My objective is to achieve source anonymity by preventing traffic analysis/flow tracing and also detecting number of hackers. To the best of my knowledge, this is the first research effort in utilizing network coding to thwart traffic analysis/flow tracing and realize privacy preservation. The proposed technique offers the following attractive features:

A. ***Enhanced Privacy against flow tracing and traffic analysis:***

The confidentiality of GEVs is efficiently guaranteed, which makes it difficult for hackers to recover the GEVs.

B. ***Efficiency:*** Due to the homomorphism of HEFs, message recoding at intermediate nodes can be directly performed on encrypted GEVs and encoded messages, without knowing the decryption key or performing the decryption operation on each incoming packet.

C. High Invertible GEVs:

Random network coding is feasible only if the prefixed GEVs are invertible.

II. NETWORK CODING MODEL

What is Network coding?

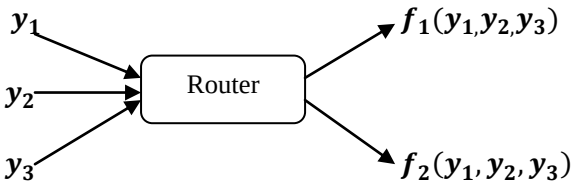

Fig. 1 Network coding: network nodes can compute functions of input messages.

Consider a router in a computer network. Today, a router can merely route, or forward messages. Each message on an output link must be a copy of a message that derived earlier on an output link Network coding, in contrast, allows each node in a network to perform some computation. Therefore in network coding, each message sent on a node's output link ca be some "function" or" mixture" of messages that arrived earlier on the input's link, as illustrated in Fig 1. Thus, network coding is generally the transmission, mixing (or encoding), and re-mixing (or re-encoding) of messages arriving at nodes inside the network, such that the transmitted messages can be unmixed (or decoded) at their final destinations.

Network coding was first introduced by Ahlswede et al [12] as shown in Fig.1. Subsequently, two key techniques, random coding [13] and linear coding [14] further promoted the development of network coding. The random codin makes network coding more practical, while the linear coding is proven to be sufficient and computationally efficient for network coding . currently, network coding has been widely recognized as a promising information dissemination approach to improve network performance.

Unlike other packet-forwarding systems, network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming ones. This elegant principle implies a random network coding [13], as shown in Fig. 2, where there is a transmission opportunity for an outgoing link, an outgoing packet is formed by taking a random combination of packets in the current buffer. An overview of network coding and possible applications has been given in [15]. In practical network coding, source information should be divided into blocks with h packets in each block. All coded packets related to the kth block belong to generation k and random coding is performed only among the packets in the same generation. Packets within a generation need to be synchronized by buffering for the purpose of network coding at intermediate nodes.

III HOMOMORPHIC ENCRYPTION FUNCTION

Homomorphic Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating cipher text as shown in Fig. 3.If *E(.)* is a HEF, *E(x+y)* can be plaintext x and y. To be applicable in the corresponding plain text scheme, a HEF (.) needs to satisfy the following properties.

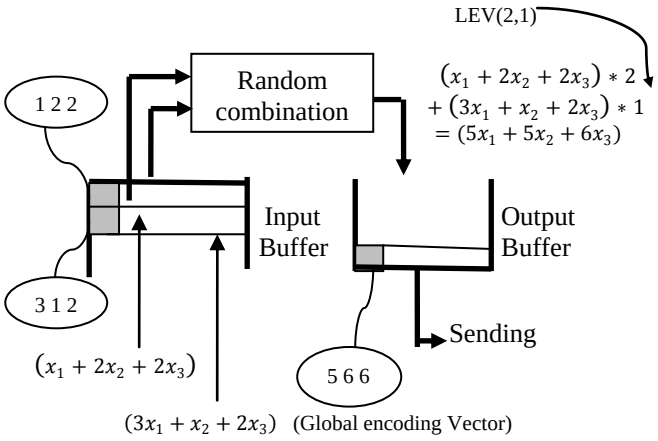

Fig. 2 Random network Coding

Additivity: Given the cipher text *(x)* and *(y)*, there exists a computationally efficient algorithm *Add(. , .)* such that *E(X+Y) = Add(E(x), E(y)).*

Scalar Multiplicity: Given *E(x)* and a scalar t, there exists a computationally efficient algorithm *Mul(. , .)* such that *E(x. t) = Mul(E(x), t).*

Benaloh [10] and Paillier[11] cryptosystems are of such an additive HEF, where the addition on plaintext can be achieved by performing a multiplicative operation on the corresponding cipher text, i.e, *E(x1 + x2) = E(x1) . E(x2).*

IV THE PROPOSED PRIVACY PRESERVATION TECHNIQUE

The proposed technique consists of three phases: Source encoding, intermediate node recoding and sink decoding. Without loss of generality, we assume that each sink acquires two keys, the encryption key *ek* and decryption key *dk*, from an offline Trust Authority (TA). For supporting multicast, a group of sinks are required to obtain from the TA. Then, the encryption key is published and the decryption key is kept secret.

Source Encoding: Block diagram of source encoding phase as shown in Fig.6. Consider that a source has h messages, say *X1, . , . , . ,Xh,* to be sent out. The source first prefixes h unit vectors to the h messages, respectively. After tagging as shown in Fig.5, the source can choose a random LEV and perform linear encoding on these messages, respectively. Then a LEV can produce an encoded message with GEV's are explicit. So any node can recover the original messages hence we are using homomorphic encryption functions to encrypt the GEV.

To offer confidentiality for the tags, homomorphic encryption operations are applied as follows:

$$Ci(e) = E_{ek}\big(gi(e)\big), \quad (1 \le i \le h)$$
$$C(e) = [C_1(e), C_2(e), \dots, ch(e)] \qquad (1)$$

Intermediate Recoding: Block diagram of this phase is as shown in Fig.7, After receiving a number of packets of the same generation, an intermediate node can perform random linear coding on these packets. To generate an outgoing packet, firstly, a random LEV[β1, . . . βh] is chosen independently; then a linear combination of message content

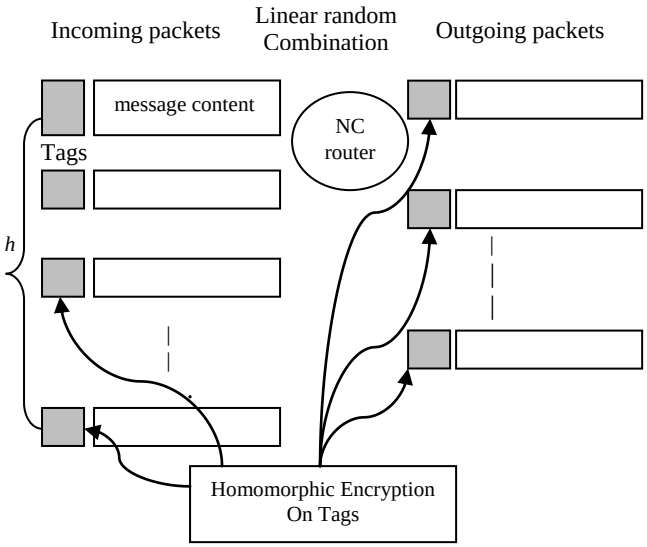

Fig 4. Homomorphic encryption on packet tags

of the outgoing packet, as shown in Fig 2. Since the tags of h incoming packets are in cipher text format, and an intermediate node gas no knowledge of the corresponding decryption keys, it is difficult for intermediate node to perform functions such as earliest decoding to get the original message content. However, due to the homomorphism of the encryption function, a linear transformation can be directly performed on the encrypted tags of the incoming packets to generate a new tag for the outgoing packet, namely,

$$g(e) = \sum_{i=1}^{h} \beta(e) g(e1_i) \qquad (2)$$

The GEV of a new outgoing packet can be calculated according to Eq. (2). By utilizing the homomorphic characteristic of the encryption on GEVs, the cipher text of the new GEVs for outgoing packets can be calculated as follows:

$$\begin{aligned} E_{ek}(g(e) &= E_{ek}\left(\sum_{i=1}^{h} \beta i(e) g(e_i^1)\right) \\ &= \pi_{i=1}^{h} E_{ek}\left(\beta_i(e) g\left(e_i^1\right)\right) \\ &= \pi_{i=1}^{h} E_{ek}^{\beta_i(e)}\left(g\left(e_i^1\right)\right) \end{aligned} \qquad (3)$$

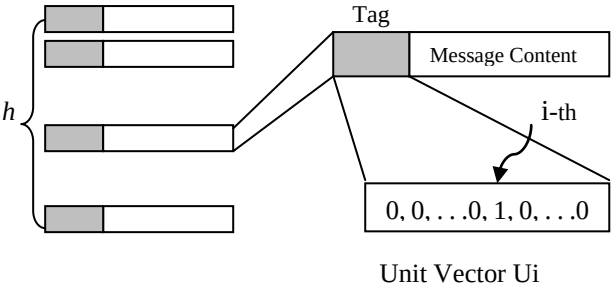

Fig 5. Packet tagging before source encoding

The cipher text of new GEVs can be computed from the cipher text of GEVs of incoming packets without the knowledge of the decryption key. Finally, the cipher text of a new GEV is prefixed to the corresponding message content to form a new outgoing packet, which is sent out to downstream nodes.

Sink Decoding: The sink decoding phase is as shown in Fig.9, After receiving a packet, the sink first decrypts the packet tag the corresponding decryption sent *dk.*

$$\begin{aligned} g_i(e) &= D_{dk}\left(c_i(e)\right) \ (1 \le i \le h) \\ g(e) &= [g_1 g_2(e), \ldots., g_h(e)] \end{aligned} \qquad (4)$$

Once enough packets are received, a sink can decode the packets to get the original messages. Then, the sink can decode the decoding vector, which is the inverse of the GEM, as shown in the following equations.

$$\begin{aligned} G^{-1}.G &= U \\ G &= [g(e_1), g(e_2), .., g(e_h)]^T \end{aligned} \qquad (5)$$

Finally, the sink can use the inverse to recover the original messages, shown as follows.

$$\begin{pmatrix} x1 \\ . \\ . \\ xh \end{pmatrix} = G^{-1} \begin{pmatrix} y(e_1) \\ . \\ . \\ y(e_h) \end{pmatrix} \qquad (6)$$

For random network coding, a key issue is the inevitability of a GEM.

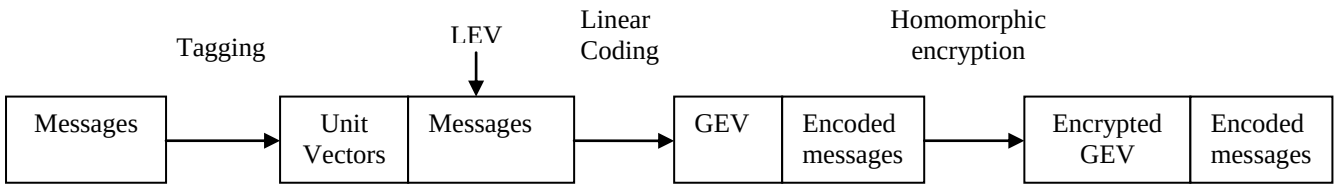

Fig 6. Source Encoding Phase

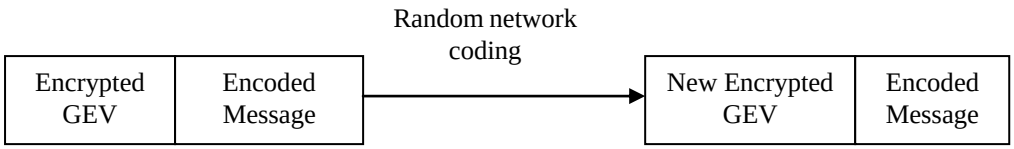

Fig 7 Intermediate Node Recoding Phase

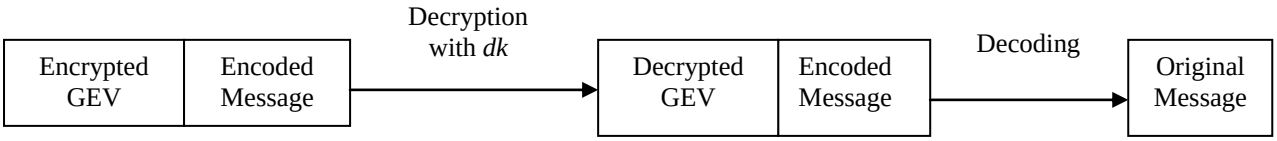

Fig 8 Sink Decoding Phase

V RESULT

The message encryption window is as shown in Fig.9, which is used to encrypt the message which we are sending from source to destination by using homomorphic encryption function with encryption key *ek*. First the message will split into number of paths after that message will encrypt by using encryption key *ek*. Without knowing the encryption key attackers cannot get the original message. If an attacker tries to obtain the message with guessed decryption key than they will get some other message. When we click simulate with routing button the traffic analysis window as shown in Fig.10 will appear.

The traffic analysis window is used to prevent traffic analysis/flow tracing by detecting number of attackers which are trying to hack the messages. First it will create the path from source to destination after creating path it will start transmission of packets. When we click the make intrusion button it will show which nodes are members and which are not members of path and also detect the number of attackers with their target node.

VI CONCUSION

In this paper we have proposed an efficient network coding based privacy preservation technique against traffic analysis and flow tracing in multi hop wireless networks. And we can detect how many attackers are trying to attack to hack the message. With homomorphic encryption on global encoding vectors (GEVs), the proposed technique offers two significant privacy preserving features packet flow untracability and message content confidentiality, with efficiently thwart traffic analysis/flow tracing attacks. With homomorphic encryption, the proposed technique keeps the essence of random linear network coding and each sink can discover the source message by inverting GEVs with very probability.

Network performance of the proposed technique is better than the previous schemes because of intrinsic feature; less computation cost because packets from the same session can be encoded together; maximize the throughput and consumes less energy.

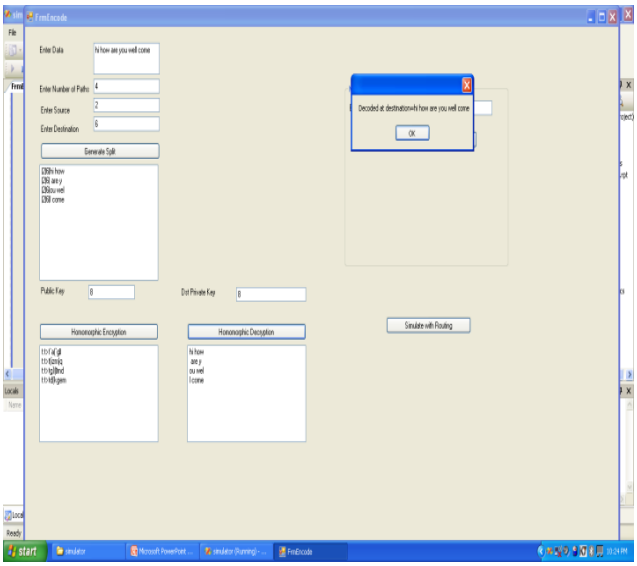

Fig. 9 Message Encryption window

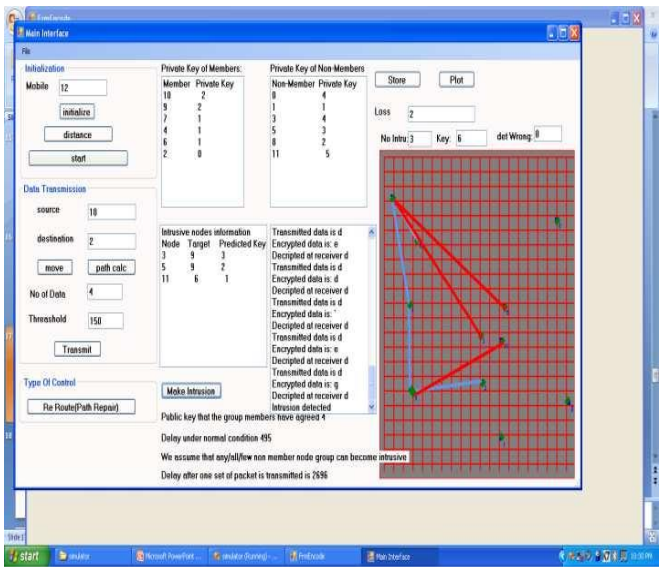

Fig. 10 Traffic Analysis Window

VII REFERENCES

[1] T.Zia and A.Zomaya "Security Issues in Wireless Networks".
[2] M.K.Reiter and A.D.Rubin, "Crowds: anonymity for web transactions" *ACMTrans.INF. and system security*, vol.1, no1, pp.66-92, Nov 1998.
[3] M.Rennhard and B.Plattner, "Introduction MorphMix:peer-peer based Anonymous Internet usage with collision detection," in *Proc ACM Work shop on privacy in the Electroni Society*, pp.91-102, 2002.
[4]D.Goldschlag, M.Reed and P.Syversion, "Onion routing for anonymous And private internet connections," *Commun. ACM*, vol 42, no.2, pp.39-41, Feb 1999.
[5] Z.Won, K.Xing, Y.Liu"Privacy-Code:Preserving privacy against traffic Analysis through network coding for Multi-hop wireless networks".
[6] K.Han, T.Ho,R.Koetter, M.Medard and F.Zhao, "Network coding for Security," in *Proc. IEEE MILCOM'*07, pp.1-6, 2007.
[7] C.Gkantsidis abd P.R.Rodridguez," Cooperative Security fot Network Coding File Distribution," in *Proc. IEEE INFCOM'* 06, pp.1-13, 2006.
[8] Z.Yu, Y.Wei, B.Ramkumar and Y.Guan, "An efficient Signature based Scheme for Securing Network Coding Against Pollution Attacks,"in *Proc IEEE INFCOM*, 2008.
[9] M Adeli and H Liu, "Secure Network Coding with Minimum Overhead based on Hash Functions," IEEE Commn. Lett, vol 13, no12, pp956-958, 2009.
[10] J.Benaloh, "Dense Probablistic Encryption," in Proc.Workshop on Selected Areas in Cryptogrgaphy, pp.120-128, 1994.
[11] P.Paillier, "Public-key Cryptosystem based on Composite Degree Resi-ducity Classes,"in *Proc EUROCRYPT'99*, vol1592, pp.223-238, 1999.
[12] R.Ashswede, N.Cai, S-Y.R Li and R.W.Yeung, " Network Information flow," *IEEE Trans. Inf.Theory*, vol.46, no.4, pp.1204-1216, July 2000.
[13] T.Ho, M.Medard, R.Koetter, D.R.Karger, M.Effors, J.Shi and B.Leong "A Random Linear Network Coding Approach to Multicast", *IEEE Trans. Inf.Theory*, vol.49, no.10, pp.4413-4430, 2006.
[14] S-Y, R.W.Yeung and C.Ning, " Linear Network Coding", *IEEE Trans Inf Theory*, vol.49, no.2, pp371-381, 2003.

Prof Santoshkumar Bandak received the B.E dgree in computer scince and engineering from Gulbarga. Karnataka, India in 1997., the M.Tech in information and technologyfrom AAIEDU Alhabad in the year 2005, perceiving Phd in computer science from CMJ University Meghalaya , workin as Asst.Prof in H.K.E Society Poojya Doddappa Engineering College Gulbarga.

Jyoti Neginal received the B.E degree in computer science from Visveswaraiah University Belguam , Karnataka, India in 2006, now doing M.Tech (4th sem) degree in compter science from Visveswaraiah university, Poojya doddappa appa college of engineering Gulbarga, Karnataka, India in 2012.