Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Coding for Privacy Protection against Traffic Analysis in Multi-Hop Wireless Networks

Suini Paul
Department of Computer Applications
The Oxford College of Engineering

Priyadarshini K.R
MCA 3rd year
The Oxford College of Engineering
prdarshini345@gmail.com

Abstract—***Traffic analysis presents a serious threat to wireless network privacy due to the open nature of wireless medium.In multi-hop wireless network (MWN), the mobile nodes relay others' packets forenabling new applications and enhancing the network deployment and performence.Privacy threat is one of the critical issues in multi_hop wireless networks, where the involves such as traffic analysis can be easily launched by a malicious adversary due to the open air transmission .Network coding has the potential to traffic analysis attacks since the coding /maxing operation is encouraged at intermediate nodes. in this paper we propose a novel network coding based privacy preserving scheme against traffic analysis in multi_hop wireless networks.***

Keywords—***Homographic encryption,network coding, privacy preservation, traffic analysis.***

I. INTRODUCTION

Multi_hop Wireless Networks are regarded as such a promising solution for extending the radio coverage range of the existing wireless networks. There exist many security and privacy issues in MWN.Due to the open _air wirless transmission ,MWN's suffer from various kinds of attacks,such as eavesdropping,data modification /injection.and node compromising these attacks may breach the security properties of MWNs,includingconfidentiality,integrity,and authenticity.

Reputation-based mechanisms and incentive protocols [3] have been proposed to protect against packet drop by enforcing and stimulating the nodes' cooperation, respectively. For reputation-based mechanisms, each node usually monitors the transmissions of its neighbors to make sure that the neighbors relay others' traffics and thus the uncooperative nodes (malicious or selfish) can be identified and punished. Each node maintains a reputation value for each neighbor. A neighbor's reputation value is improved when the neighbor relays a packet and degraded when the neighbor drops a packet[2].

In this paper we focus on privacy preservation issues that is how to prevent traffic analysis/flow tracing and achive source anonymity in MWN's.Source anonymity is special interest in MWN's ,Source anonymity refers to communicating through a network without revealing the identity or location of the source node. Preventing traffic analysis/flow tracing and provising source anonymity is critical for securing MWNs.Where the nodes can communicate with each other through multi_hop packet forwarding.

Existing privacy preservation solution, such as proxy _based schemes, Chum's mix _based scheme, e.g. with an end_to_end delay of several minutes. In this paper based on network coding and homomorphism Encryption functions.

We propose an efficient privacy_prserving scheme for MWNs.Our objective is to achieve source anonymity by preventing traffic analysis and flow tracing attacks.

The proposed scheme offers the following attractive features

A. Enhanced Privacy against flow tracing and traffic analysis

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

B. Efficiency

Due to the homomorphism of HEFs, messages recoding at intermediate nodes can be directly performed on encrypted GEVs and encoded massages, 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 Inverible.

A. Network Coding Model

Unlike traditional packet-forwarding systems, network coding allows intermediate nodes to perform computation

on input messages, making output messages be the mixture of the input ones.

Whenever there is a transmission opportunity on an outgoing link, an outgoing packet is formed by taking a random combination of packets in the current buffer. Packet tagging and buffering are key for practical network coding. 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 only performed among the packets in the same generation .Packets with a generation need to be synchronized by buffering for the purpose of network coding at intermediate nodes.

For example consider an acyclic network(V, E.c) with unit capacity that is c(e)=1 for all e belongs to E meaning that each edge can carry one symbol per unit time.

II. FEATURE SELECTION ALGORITHMS

A. *Homomorphism Encryption Function*

Homomorphism Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating on corresponding cipher text. For example, suppose E(.) is a HEF .

It is easy to compute E(x+y)from e(x) and E(y) without knowing the corresponding plaintext x and y .to be applicable in the proposed scheme, a HEF E(.) needs to satisfy the following properties:

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

2) *Scalar Multilicativity:*Given E(x) and scalar t,there exist a computationally efficient algorithm Mul(.,.) such that E(t,X)=Mul(E(X),t).

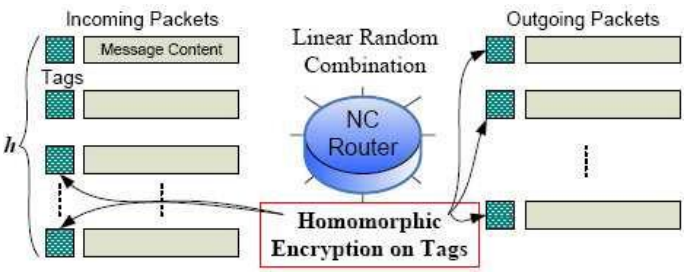

Figure 1.Homomorpic encryption on packet tags.

HEF is an intutive way to keep GEVs confidential to intermediate nodes by encrypting the GEVs in end-to-end manner, which can prevent compromised intermediate nodes from analyzing GEVs or recovering the original messages.

HEF is used to applay encryption to GEVs,HEFcannot keep the confidential of GEVs but also enable intermediate nodes to efficiently mix the coded messages.

In HEFs, intermediatenodes are allowed to directly perform linear coding/mixing operations on the coded messages encrypted tags.

The proposed scheme consists of three phases.

1) *Source encoding:* 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 .After tagging; thesource can choose a random LEV and then linear encoding operation on these messages.

2) *Intermediate Random Linear Recoding:*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 .

3) *Sink Decoding:*After receiving a packet, the sink first decrypts the packet tag using the corresponding decryption key dk.Once enough packets are received, a sink can decode the packets to get the original messages.

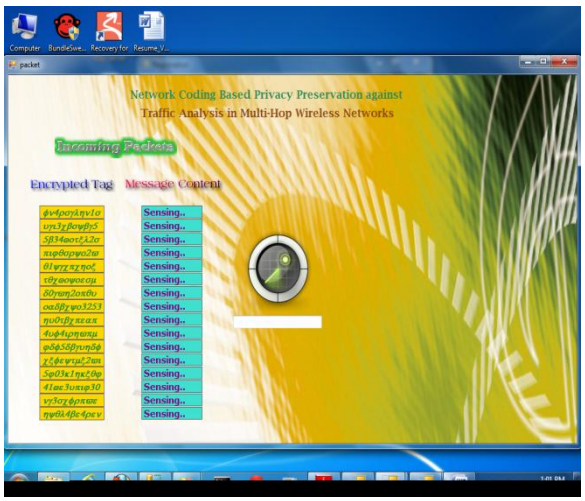

Figure 2.traffic analysis window

This window is used to prevent the traffic If the attacker can intercept the packet the packets and trace back to the source through traffic analysis sensor sensing the encryption messages.

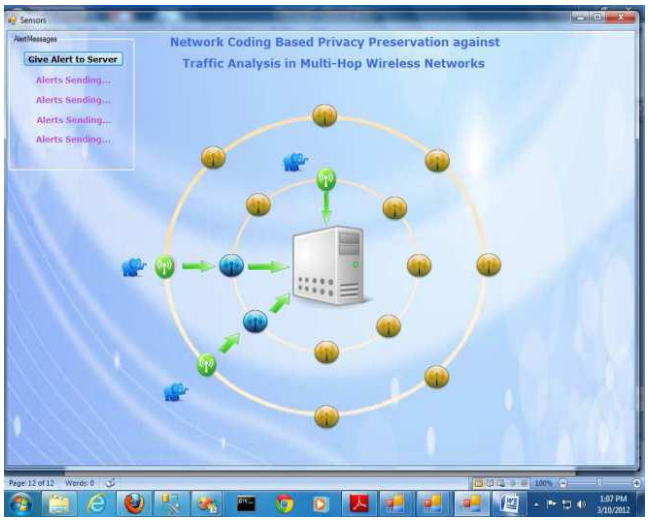

Figure 3.Attacker and server window

The appearance of an endangered animal (Attackers) in a monitored area is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and Hunter they are also can participate this wireless network. In the commander and hunter itself some intruders are there, our aim to capture the attackers before attempting the network.

III. Conclusion

This paper gives the clear view of the how to prevent the traffic analysis/flow tracing ,using network coding privacy preservation scheme with homomorpic encryption on global Encoding Vector functions/algorithum,using coding/mixing operation on intermediate nodes unlinkability between the source location.

I. References:

[1].YanfeiFan,YixinJiang,Haojin Chen Network Coding Based Privacy Preservation against TraficAnalysis in Multi_HopWirless Networks published in march 2011.

[2].Network Coding Based Privacy Preservation against Traffic Analysis in Multi_HopWirless Networks, www.vidhat.com/../base paper

[3] Yanfei Fan Network Coding based InformationSecurity in Multi-hop Wireless Networks, published on 2009.

[4] Yanfei Fan; Yixin Jiang; Haojin Zhu; XueminShen; An Efficient Privacy-Preserving Scheme against Traffic Analysis Attacks in Network Coding published in April 2009.

[5]by Kaikai Chi, Xiaohong Jiang, Baoliu Ye, Hnin Yu Shwe, Susumu Horiguchi Efficient network coding-based end-to-end reliable multicast in multi-hop wireless networks

[6]By Y Fan, Y Jiang, H Zhu, X Shen An Efficient Privacy-Preserving Scheme against Traffic Analysis Attacks in Network Coding,published in 2009

[7]Survey on Privacy Solutions at the Network Layer: Terminology, Fundamentals and Classification Pedro Moreira
da Silva1, Jaime Dias1, Manuel Ricardo1.

