Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.5, No.6, 2014
www.iiste.org

Lightweight Encrytion Scheme against Flow Analysis in Multi-Hop Wireless Network Based on Network Coding

SHRIVANI. N, SRINIDHI. K, MANJULA DEVI T. H
Department of Telecommunication Engineering, Dayananda Sagar College of Engineering, Visvesvaraya Technological University, Bangalore-560078

ABSTRACT:
Traffic analysis is a major issue faced in multi-hop wireless networks (MWN) in the case of privacy preservation. Network coding is essential in achieving greater capacity for any network and we extend this network coding for privacy preservation in multi-hop networks as it offers coding and mixing functions at intermediate nodes. Certain existing privacy preserving methods like onion routing can be employed here. Applying homomorphic encryption on Global Encoding Vectors(GEV's), our method offers confidentiality and privacy preserving features. Only the sink has capability of decrypting the message content by inverting the GEV. Here, we focus on the privacy issue in order to prevent traffic analysis and flow tracing and achieve source anonymity in MWNs. Source anonymity refers to carrying the communication through the network maintaining the secrecy of the source node. Energy consumption when compared with the existing system was found to be reduced. Simulative evaluation by NS2 shows the efficiency of the system.
Keywords: *MWN, Privacy preservation, NS2, GEV.*

INTRODUCTION

Communication is the important part in any type of network for making it possible to transfer data from one node to another. Communication needs quality and security for better performance and for acceptance of users and client companies.

Security has become more important to personal computer users, organizations, and the military. Security became a major concern with the advent of internet and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The modified architecture of the internet can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Data integrity is quite a issue in security and to maintain that integrity we tends to improve as to provides the better encryption processes for security.

In traditional wireless networks there is only one source and destination and the source broadcasts and destination receives. Here it is difficult for an attacker to decrypt the message because there is only a source point from which the attacker can decrypt the message. But there are many disadvantages like less radio coverage i.e. the distance of coverage is very less and this system is not much reliable.

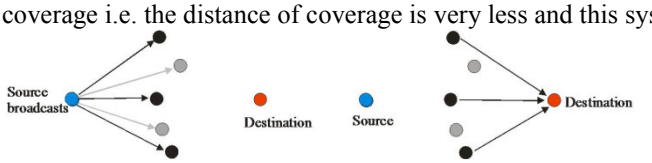


Fig 1.1: Traditional wireless networks

In multi-hop wireless networks there are multiple intermediate nodes between the source and the destination . In other multi hop systems the intermediate nodes decrypt the message and then it is sent to the sink but in our proposed system only the sink is capable of decrypting the message and hence the attacker cannot retrieve the message and confidentiality is maintained and even privacy. And source anonymity is maintained i.e. the source identity is kept as a secret.

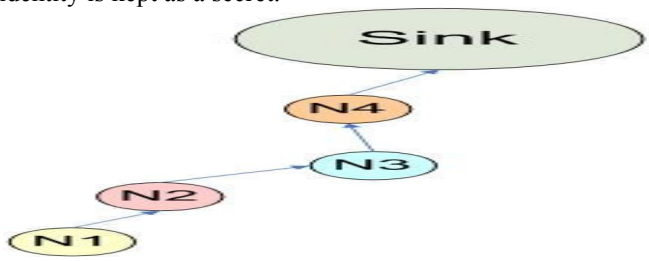


Fig 1.2: Multi-hop wireless network

A source node has a packet that it wishes to deliver to a distant destination. Between the source and destination are other wireless nodes willing to participate in Ex-OR. The source broadcasts the packet. Some sub-set of the nodes receive the packet. The nodes run a protocol to discover and agree on which nodes are in that sub-set. The

node in the sub-set that is closest to the destination encrypts and broadcasts the packet. Again, the nodes that receive this second transmission agree on the closest receiver, which again encrypts and broadcasts the packet. This process continues until the destination has received the packet and the sink decrypts it.

PROPOSED MODEL:

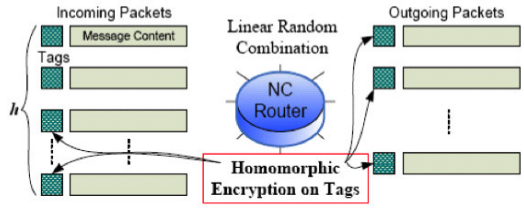


Fig. 1. Homomorphic encryption on packet tags.

Source Encoding:

Consider that a source has h messages, say $x1, \cdots, xh$, messages. The unit vectors are prefixed to h known messages. LEV is chosen for encryption. Then, a LEV can produce an encoded message with the GEV. Homomophic encryption used to provide confidentiality, *ek* is the encryption key. We adopt strategy of applying HEF to GEVs after linear encoding.

Intermediate Recoding:

After packets are received intermediate node performs recoding. To generate an outgoing packet- a random LEV $[\beta 1, \cdots, \beta h]$ is chosen and it is independent, then, a linear combination of message content of the incoming packets is computed as the message content of the outgoing packet.

Tags of the h incoming packets are in ciphertext format, and an intermediate node doesn't know of the corresponding decryption keys, it is difficult for the intermediate node to perform decoding to get the original message content. However, due to the HEF, a linear transformation can be directly performed on the packets which contain encrypted tags to generate a new tag for the outgoing packet.

By utilizing the homomorphic characteristic of the encryption on GEVs, the ciphertext of the new GEVs for outgoing packets can now be calculated.

The ciphertext of new GEVs can be computed from the ciphertext of GEVs of incoming packets with no knowledge of the decryption key. Finally, the ciphertext of a new GEV is prefixed to the corresponding message content to form a new outgoing packet, which may be sent out to other nodes.

5.1.3 Sink Decoding:

After receiving a packet, the sink first decrypts the packet tag using the corresponding decryption key dk and then packet is decrypted.

RESULT

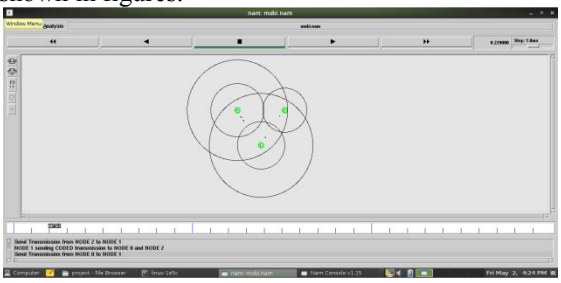
Figure: normal transmission.

For LES=0, nomal transmission, the transmission energy consumed is found to be 80 J and transmission between nodes is shown in figures.

First Transmission: node 0 to node 1 as indicated from dotted lines.

Second Transmission: node 0 to node 2 as indicated from dotted lines.

Third Transmission: node 2 to node 0 as indicated from dotted lines.
Fourth Transmission: node 2 to node 1 as indicated from dotted lines.
Hence four transmissions are required for node 1 to code the data and send back to node 0 and node 2.
For LES=1, the Transmission energy consumed is found to be 60 J and transmission between nodes is shown in figures.



First Transmission: node 0 to node 1 as indicated from dotted lines.
Second Transmission: node 2 to node 1 as indicated from dotted lines.
Third Transmission: coded data, that is node 1 performs ex-or operation between data sent from node 2 and node 0 is performed and sent to both node 0 and node 2 simultaneously as indicated from dotted lines.
The results inferred are:

- Energy consumed compared to normal transmission is reduced.
- One Transmission is reduced compared to normal transmission which in turn reduces traffic and network resources.
  The same application is showed for 6 nodes in simulation and link failure is indicated.

LINK FAIURE:
We have also indicated link failure in the nodes this is done by taking 6 nodes . Node 5 is out of coverage, and later it is include in

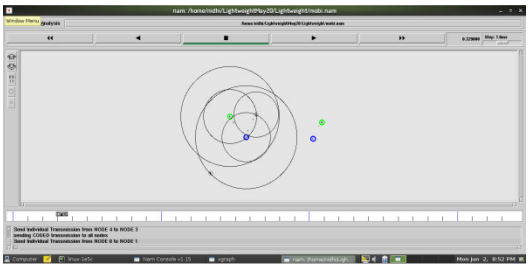


Figure: shows node 5 is out of radio coverage.
coverage area and later it is brought into coverage area. And two clusters each of three nodes are formed and coded transmissions are sent.

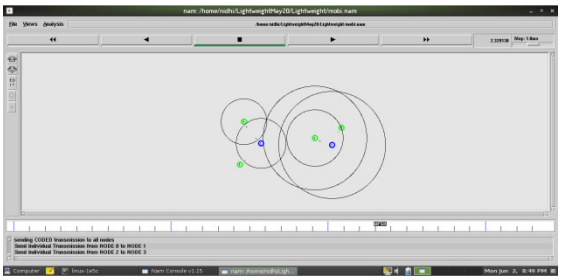


Figure: shows node 5 included in radio coverage and link failure is prevented.

APPLICATIONS:

- Can be used in mobile computing whenever the mobile station reaches out of coverage area.
- Military applications.
- Confidentiality is improved.
- Electronic voting and electronic cash.
- Expansion can be provided to network coding.

CONCLUSION:
A resourceful network coding based privacy preservation technique against traffic analysis and flow

tracing in multi-hop wireless networks is proposed in our scheme. This scheme offers three important features with the lightweight homomorphic encryption on Global Encoding Vectors (GEVs), packet flow confidentiality and message confidentiality, which can efficiently prevent traffic analysis attacks and also the energy consumed in LES system is found to be less than the normal method. Moreover, by inverting the GEVs, each sink or destination can recover the source packets.
It also provides:
1) Network coding packet mixing, along with homomorphic encryption.
2) we have a scheme for embedding the information into the network coding GEV using a simple mapping function and encryption with minimal impact on the decoding probability.
3) We show the efficiency of the proposed system by carrying out simulations, secrecy and security analysis.

FUTURE WORK:
Several privacy-preserving schemes have been proposed, and they can be classified into three categories: proxy-based, mix-based, and onion-based. Proxy-based schemes include Crowds and Hordes . The common characteristic of these schemes is to employ one or more network nodes to issue service requests on behalf of the originator. In Crowds, for example, servers and even crowd members cannot distinguish the originator of a service request, since it is equally likely originating from any member of the crowd.
These schemes commonly apply techniques such as shaping, which divides messages into a number of fixed-sized chunks, and mixing, which caches incoming messages and then forwards them in a randomized order. These techniques can be used to prevent attacks such as size correlation and time correlation. Onion-based schemes include Onion Routing and Onion Ring . The common feature of these schemes is to chain onion routers together to forward messages hop by hop to the intended recipient. Therefore, every intermediate onion router knows only about the router directly in front of and behind itself, respectively, which can protect user privacy if one or even several intermediate onion routers are compromised. Network coding has privacy-preserving features, such as shaping, buffering, and mixing.

REFERENCES:
[1] Zhiguo Wan, Kai Xing, Yunhao Liu *"Preserving Privacy Against Traffic Analysis through Network Coding for Multihop Wireless Networks*" ,IEEE Trans.2011.
[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "*Network Information Flow*", *IEEE Trans. on Information Theory*, vol. 46, no. 4, pp. 1204- 1216, Jul. 2000.
[3] M. Wang and B. Li, "*Network Coding in Live Peer-to-Peer Streaming*", IEEE Trans. On Multimedia, Vol. 9, No. 8, pp. 1554-1567, 2007.
[4] Philip A. Chou and Yunnan Wu "*Network coding for Internet and wireless network*" June 2007 MSR-TR- 2007-70.
[5] P. Venkitasubramaniam and L. Tong, "*Anonymous Networking with Minimum Latency in Multihop Networks*", *Proc.IEEE Symposium on Security and Privacy*, pp. 18-32, 2008.
[6] Ralf Koetter, Member, IEEE, and Muriel Médard, Senior Member, IEEE, "*An Algebraic Approach to Network Coding"*, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 11, NO. 5, OCTOBER 2003.

BIOGRAPHY
1. .Ms. Srinidhi. K is pursuing Bachelors Degree in
Telecommunication Engineering from Dayananda Sagar College of Engineering.
2..Ms. Shrivani. N is pursuing Bachelors Degree in
Telecommunication Engineering from Dayananda Sagar. College of Engineering.
3.Mrs. Manjula Devi T H is working as an Associate
Professor in Dept of Telecommunication Engineering, Dayananda Sagar College of Engineering, and Bangalore. She has Bachelors Degree in Electronics and Communication Engineering from Bangalore University, Bangalore and Masters Degree in Electronics and Communication Engineering from BU, Bangalore. Presently she is pursuing PhD from JNTU, Hyderabad.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar