International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 1, Issue 1 : Page No.64-66, September-October 2013
www.ijlrec.com

A Novel Network Coding Based Privacy Safeguarding Scheme against Traffic Analysis Attacks

G.P.Raja[1], Dr.S.Mangai[2], K.Sudhakar[3]
[1]Assistant Professor, IT, Sengunthar College of Engineering, Tiruchengode, India,
[2]Professor, ECE, Velalar College of Engineering & Technology, Thindal, Erode, India
[3]Asst Prof & Head, CSE, Sengunthar College of Engineering, Tiruchengode, India

Abstract: Wireless access networks have been extensively deployed due to their ease, portability, and low cost. For expanding the radio coverage range of the accessible wireless networks, a Multi-hop Wireless Networks (MWNs) are considered as extremely capable solution and they can also be used to get enhance the system reliability through multi-path packet forwarding. However, due to the open wireless medium, MWNs are vulnerable to a variety of attacks, such as eavesdropping, data alteration and node compromising. Due to the open wireless medium attacks the traffic analysis and flow tracing can be easily initiated by a hateful adversary as privacy hazard is one of the significant issues in multihop wireless networks. Since the network coding has the potential to prevent these attacks as the coding operation is encouraged at intermediate nodes. However, the simple consumption of network coding cannot accomplish the goal once adequate packets are collected by the adversaries. On the other hand, the coding nature averts the possibility of employing the available privacy safeguarding methods, such as Onion Routing. A novel network coding based privacy safeguarding scheme against traffic analysis in multi-hop wireless networks is proposed in this paper. The proposed scheme offers two important privacy preserving features with homomorphic encryption on Global Encoding Vectors (GEVs). The packet flow un-traceability and message content confidentiality are two features for resourcefully preventing the traffic analysis attacks.

Keywords: Privacy Safeguarding, Multi-hop Wireless Networks, Traffic Analysis Attacks, Onion Routing.

INTRODUCTION

The open wireless medium of Multi-hop Wireless Networks is susceptible to a variety of attacks such as data alteration node compromising and eavesdropping. The attacks may violate the security of multi-hop wireless networks, including privacy, reliability and accuracy and to compromise users' privacy some advanced attacks such as traffic analysis and flow tracing can also be launched by a hateful adversary, including source secrecy and traffic secrecy [1] [2]. Source anonymity is of special interest in Multi-hop Wireless Networks among all privacy properties which refers to communicating through a network without revealing the location of source nodes. For expanding the radio coverage ranges of the accessible wireless networks, and also to develop the system reliability through multi-path packet forwarding, Multi-hop Wireless Networks are regarded as an extremely capable solution [3].

For confidentiality aware Multi-hop Wireless Networks shown in fig1 averting traffic analysis or flow tracing and provisioning source secrecy are vital. It is very challenging to efficiently prevent traffic analysis/ flow tracing attacks and provide privacy protection in multi-hop wireless networks [5].

Considering a multicast communication in military ad hoc networks, where nodes can converse with each other through multi-hop packet forwarding and it may disclose some sensitive information such as the location of critical nodes, if an attacker can interrupt packets and trace back to the source through traffic analysis and then further it may damage the location confidentiality. Existing privacy preserving solutions, such as proxy based schemes and onion-based schemes which may either require a series of trusted forwarding proxies or result in severe performance degradation in practice. Network coding has been extensively acknowledged as a talented information distribution approach to progress network performance [4] [6].

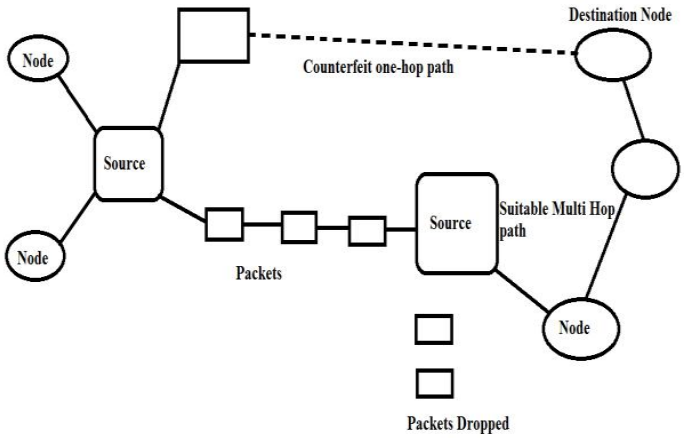

Fig 1: An overview of multi hop network.

At present, most important applications of network coding take account of distribution off file and multimedia streaming on peer to peer overlay networks. The haphazard coding makes network coding more realistic, while the linear coding is established to be adequate and computationally well-organized for network coding.

CONTRIBUTION TO THE IMPROVED CONFIDENTIALITY AGAINST TRAFFIC INVESTIGATION

The privacy of global encoding vector brings an implicative benefit, the confidentiality of message content because message decoding only relies on global encoding vector on the other hand, with random recoding on encrypted global encoding vector the coding feature of network coding can be exploited in a natural manner to satisfy the mixing requirements of privacy preservation against traffic analysis [7] [9].

Theoretical analysis demonstrates that the influence of homomorphic encryption functions on the invertible probability of global encoding vector is negligible. Random network coding is feasible only if the prefixed global encoding vectors are invertible with a high probability. Message recoding at intermediate nodes can be directly performed on encrypted global encoding vector and determined messages, without knowing the decryption keys or performing expensive decryption operations on each incoming packet due to the Homomorphism of homomorphic encryption function [8] [10] [11].

The confidentiality of global encoding vector is efficiently assured with the employment of homomorphic encryption functions, making it difficult for attackers to get better with the plaintext of global encoding vector. An efficient privacy-preserving scheme for multi-hop wireless networks based on network coding and a homomorphic encryption function offers the enhanced Privacy against traffic analysis and flow tracing [13]. The adversaries still cannot decrypt the global encoding vector even if some intermediate nodes are cooperated, since only the sinks know the decryption key.

EXPANSION OF NETWORK CODING

Data transmission in sensor networks premeditated connections in military networks measure up to with conservative packet forwarding technologies, network coding suggests, by permitting and encouraging coding/mixing operations at transitional forwarders more than a few important advantages such as probable throughput development, communication energy minimization, and impediment diminution [12] [14]. An uncomplicated deployment of network coding cannot put off traffic analysis tracing in view of the fact that the explicit Global Encoding Vectors previously fixed to the programmed messages make available a back door for adversaries to conciliation the privacy of users. A naive solution to take in hand this vulnerability is to make use of link-to-link encryption [15] [18]. This explanation can prevent traffic analysis to an assured degree, but it introduces important computational overhead and thus consequences in significant performance deprivation of the entire network system. Once the adequate coded packets are collected, then the adversaries can with no trouble recover the unique packets and then carry out the attacks based on these packets [16].

The non amiability connecting incoming packets and outgoing packets, which is a significant privacy property for put off traffic analysis tracing, can be accomplished by integration of the incoming packets at intermediate nodes. On the other hand, the confidentiality offered by such a mixing feature is still susceptible, in view of the fact that the linear dependence connecting outgoing and incoming packets can be easily evaluated [20]. The exploitation of network coding in multi-hop wireless networks can not only bring the above presentation advantages but also make available a practicable way to efficiently frustrate the traffic analysis tracing attacks since the coding/mixing operation is confident at transitional nodes [17].

Network coding has been extensively acknowledged as a talented information distribution approach to progress network performance. At present, most important applications of network coding take account of distribution of file and multimedia streaming on peer to peer overlay networks. Consequently, two key system, random coding and linear coding gives the initial dispersed achievement additional promoted the expansion of network coding [19]. The haphazard coding makes network coding more realistic, while the linear coding is established to be adequate and computationally well-organized for network coding.

CONCLUSION

A resourceful network coding based privacy safeguarding method against traffic analysis and flow tracing in multi-hop wireless networks is proposed in this paper. The proposed scheme offers two important privacy preserving features with the lightweight homomorphic encryption on Global Encoding Vectors (GEVs), packet flow untraceability and message content confidentiality, which can efficiently prevent traffic analysis/flow tracing attacks. Moreover, by inverting the GEVs with a very high probability, the proposed scheme keeps the random coding feature and each sink can recover the source packets. The quantitative analysis and simulative evaluation on confidentiality improvement and computational overhead demonstrate the efficiency and effectiveness of the proposed scheme.

REFERENCES

1. X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," in *Proc. IEEE ICC'07*, pp. 1247-1253, 2007.
2. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *Proc. IEEE INFOCOM'08*, pp. 51-55, 2008.
3. M. K. Reiter and A. D. Rubin, "Crowds: anonymity for web transactions," *ACM Trans. Inf. and System Security*, vol. 1, no. 1, pp. 66-92, Nov. 1998.
4. C. Shields and B. N. Levine, "A protocol for anonymous communication over the Internet," in *Proc. ACM CCS'00*, pp. 33-42, 2000.
5. M. Rennhard and B. Plattner, "Introducing MorphMix: peer-to-peer based anonymous Internet usage with collusion detection," in *Proc. ACM Workshop on Privacy in the Electronic Society*, pp. 91-102, 2002.
6. G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: design of a type III anonymous remailer protocol," in *Proc. IEEE Symposium on Security and Privacy*, pp. 2-15, May 2003.
7. D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private Internet connections," *Commun. ACM*, vol. 42, no. 2, pp. 39-41, Feb. 1999.
8. X. Wu and N. Li, "Achieving privacy in mesh networks," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'06)*, pp. 13-22, 2006.
9. R. Ahlswede, 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.
10. 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 Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413-4430, 2006.