IJRRECS/July 2014/Volume-2/Issue-7/2719-2724 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# AN EXPOSURE TOWARDS PRIVACY MANAGEMENT IN WIRELESS NETWORKS

**Patil Mahesh Balbhim[1], C.Deepa[2]**

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

## ABSTRACT:

Multi-hop Wireless are considered as an extremely capable solution for expanding radio coverage range of existing wireless networks, and they are used to get better system consistency all the way through multi-path packet forwarding. Among all confidentiality properties, source anonymity is of special attention in multi-hop wireless networks. Network coding put forward, through encouraging coding or mixing procedure at intermediate forwarders and can effort as erasure codes to improve the dependability of a dispersed data storage system. We put forward a resourceful privacy-preserving system for Multi-hop Wireless networks. The projected Privacy-Preserving Scheme although providing an inherent integration method, the unique network coding cannot make available privacy assurance due to unambiguous Global Encoding Vectors, because an adversary can get well original messages so long as sufficient packets are collected. The proposed system offers features. Improved Privacy against traffic analysis as well as flow tracing: With service of Homomorphism Encryption Functions, privacy of Global Encoding Vectors is successfully assured, making it not easy for attackers to get better plaintext of global encoding vectors. The projected scheme can make available privacy preservation by resisting traffic examination or flow tracing attacks for instance size correlation as well as message content correlation. It can be seen that projected system can uphold an extremely high invertible likelihood, which is comparable to those of random coding system; additionally, the projected scheme can recommend additional privacy enhancement, which is extremely crucial in realistic applications.

***Keywords: Network coding, Privacy-preserving, Multi-hop Wireless networks, Global encoding vectors.***

## 1. INTRODUCTION:

Preventing traffic analysis or flow tracing as well as provisioning source anonymity are crucial in support of privacy aware multi-hop wireless networks, for instance wireless sensor or tactical networks. Existing solutions of privacy-preserving, for instance proxy-based methods along with onion-based schemes might moreover necessitate a succession of trustworthy forwarding proxies or effect in rigorous performance deprivation in practice [4]. At present, network coding has been extensively acknowledged as a capable information dissemination technique to get better network performance. Quite a lot of methods of privacy-preserving were projected, and they are classified into three groupings such as: proxy-based, mix-based, as well as onion-based. Network coding has privacy-preserving characteristics, for instance shaping, mixing and buffering [8]. Network coding suffers from two most important types of attacks, such as pollution attacks as well as entropy attacks. Pollution attacks are launched by untrusted nodes or else adversaries all the way through injecting fake messages or adjusting genuine messages, which are serious to complete network due to rapid transmission of pollution. In entropy attacks, adversary falsifies non-innovative packets that are linear combination of "stale" ones, consequently reducing the general network throughput [1]. The vulnerabilities of inter or intraflow network coding structure are recognized, and wide-ranging guidelines are provided to accomplish security purpose of network coding systems. Distributed polynomial-time rate-optimal network codes are bring in against Byzantine adversaries by different attacking potential [11]. Cryptography-based solutions comprise homomorphic hashing, homomorphic signatures, as well as secure random checksum either requires an additional secure channel or acquire high computation transparency. Among all confidentiality properties, source anonymity is of special attention in multi-hop wireless networks [3]. Source anonymity refers to communicating all the way through a system devoid of revealing individuality or position of source nodes.

## 2. METHODOLOGY:

Multi-hop Wireless as shown in fig1 are considered as an extremely capable solution for expanding radio coverage range of existing wireless networks, and they are used to get better system consistency all the way through multi-path packet forwarding [14]. Several advanced attacks, for instance traffic analysis as well as flow tracing, can moreover be launched by a malevolent adversary to compromise users' confidentiality, consist of source anonymity as well as traffic secrecy [6]. **W**ireless access networks; have been extensively deployed due to their expediency, as well as low cost. They still undergo inherent shortcoming for instance restricted radio coverage, deprived system dependability, and lack of protection as well as privacy [9]. Key techniques such as random coding as well as linear coding additionally promoted expansion of network coding. The random coding build network coding more realistic, while linear coding is confirmed to be adequate and computationally well-organized for network coding. Network coding put forward, through encouraging coding or mixing procedure at intermediate forwarders [7]. Network coding can effort as erasure codes to improve the dependability of a dispersed data storage system. We put forward a resourceful privacy-preserving system for Multi-hop Wireless networks. Our objective is to attain source anonymity by put off traffic analysis as well as flow tracing. This is the initial research attempt in utilizing network coding towards thwart traffic analysis or flow tracing as well as understand privacy preservation [2]. The projected Privacy-Preserving Scheme although providing an inherent integration method, the unique network coding cannot make available privacy assurance due to unambiguous Global Encoding Vectors, because an adversary can get well original messages so long as sufficient packets are collected. Link-to link encryption is susceptible to inside attackers as they might previously have compromised quite a lot of intermediate nodes and get hold of secret keys [16]. An intuitive method to determine this problem is to remain global encoding vectors secret to intermediary nodes by encrypting global encoding vectors in a lengthwise method, which can put off compromised intermediate nodes from analyzing global encoding vectors or recovering unique messages. Such an instinctive approach, on the other hand, cannot put off the adversaries from tracking

message ciphertext as mixing characteristic of network coding might be disabled by lengthwise encryption [12]. The proposed system offers features. Improved Privacy against traffic analysis as well as flow tracing: With service of Homomorphic Encryption Functions, privacy of Global Encoding Vectors is successfully assured, making it not easy for attackers to get better plaintext of global encoding vectors [5]. Even if several intermediary nodes are compromised, adversary's still cannot decrypt Global Encoding Vectors, as only sinks recognize decryption key. Efficiency: Due to Homomorphism of homomorphic encryption functions, message recoding at intermediary nodes can be unswervingly executed on encoded messages, devoid of knowing decryption keys or performing costly decryption procedure on every incoming packet [15]. The performance assessment on computational difficulty demonstrates competence projected scheme. High Invertible Probability: unsystematic network coding is possible only if prefixed global encoding vectors are invertible with an elevated likelihood. Theoretical analysis shows that the influence of homomorphic encryption functions on invertible probability of global encoding vectors is insignificant [10]. Thus, random coding characteristic can be kept in network coding basis privacy-preserving system.

## 3. RESULTS:

The projected scheme can make available privacy preservation by resisting traffic examination or flow tracing attacks for instance size correlation as well as message content correlation. Size correlation can be obviously not permitted as every message is trimmed to be of similar length in network coding based system. Time correlation is efficiently resisted by intrinsic buffering method of network coding. It can be observed that, compared with preceding network coding system, the projected scheme considerably augment privacy preservation in terms of computational intricacy, which makes the attacks of traffic analysis approximately not possible. It can be seen that projected system can uphold an extremely high invertible likelihood, which is comparable to those of random coding system; additionally, the projected scheme can recommend additional privacy enhancement, which is extremely crucial in realistic applications.

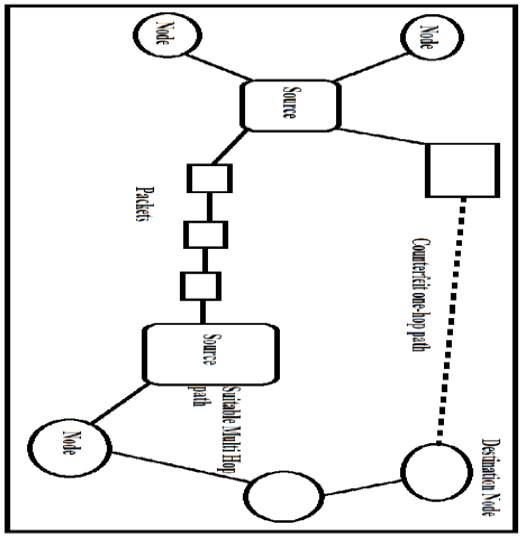


Fig 1: An overview of multi hop network.

## 4. CONCLUSION:

**W**ireless access networks; have been extensively deployed due to their expediency, as well as low cost. Network coding suffers from two most important types of attacks, such as pollution attacks as well as entropy attacks. Source anonymity refers to communicating all the way through a system devoid of revealing individuality or position of source nodes. Quite a lot of methods of privacy-preserving were projected, and they are classified into three groupings such as: proxy-based, mix-based, as well as onion-based. Network coding has privacy-preserving characteristics, for instance shaping, mixing and buffering. Several advanced attacks, for instance traffic analysis as well as flow tracing, can moreover be launched by a malevolent adversary to compromise users' confidentiality, consist of source anonymity as well as traffic secrecy. The random coding build network coding more realistic, while linear coding is confirmed to be adequate and computationally well-organized for network coding. Our objective is to attain source anonymity by put off traffic analysis as well as flow tracing. It can be observed that, compared with preceding network coding system, the projected scheme considerably augment privacy preservation in terms of computational intricacy, which makes the attacks of traffic analysis approximately not possible.

## REFERENCES:

[1] Network Coding Based Privacy Preservation againstTraffic Analysis in Multi-Hop Wireless NetworksYanfei Fan, Yixin Jiang, Haojin Zhu, Jiming Chen, and Xuemin (Sherman) Shen,2011

[2] M. Riemensberger, Y. E. Sagduyu, M. L. Honig, and W. Utschick,"Training overhead for decoding random linear network codes in wireless networks," IEEE J. Sel. Areas Commun., vol. 27, no. 5, pp. 729-737,2009

[3] P. Venkitasubramaniam and L. Tong, "Anonymous networking withminimum latency in multihop networks," in Proc. IEEE Symposium on Security and Privacy, pp. 18-32, 2008

[4] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B.Leong, "A random linear network coding approach to multicast," IEEETrans. Inf. Theory, vol. 52, no. 10, pp. 4413-4430, 2006

[5] Y. Wu, P. A. Chou, and S.-Y. Kung, "Minimum-energy multicast inmobile ad hoc networks using network coding," IEEE Trans. Commun.,vol. 53, no. 11, pp. 1906-1918, Nov. 2005.

[6] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, andM. Effros, "Resilient network coding in the presence of Byzantineadversaries," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2596-2603,2008

[7] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "ASRPAKE:an anonymous secure routing protocol with authenticated key exchangefor wireless ad hoc networks," in Proc. IEEE ICC'07, pp. 1247-1253,2007

[8] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: design ofa type III anonymous remailer protocol," in Proc. IEEE Symposium on Security and Privacy, pp. 2-15, May 2003

[9] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy-preservingscheme against traffic analysis attacks in network coding," in Proc. IEEE INFOCOM'09, Rio de Janeiro, Brazil, Apr. 2009.

[10] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure network coding forwireless mesh networks: threats, challenges, and directions," ComputerCommun. (Elsevier), vol. 32, no. 17, pp. 1790-1801, Nov. 2009.

[11] P. Sanders, S. Egner, and L. Tolhuizen, "Polynomial time algorithms fornetwork information flow," in Proc. 15th ACM Symposium on ParallelAlgorithms and Architectures (SPAA'03), pp. 286-294, 2003.

[12] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and securesensor data storage with dynamic integrity assurance," in Proc. IEEEINFOCOM'09, Rio de Janeiro, Brazil, Apr. 2009

[13] M. Rennhard and B. Plattner, "Introducing MorphMix: peer-to-peerbased anonymous Internet usage with collusion detection," in Proc. ACMWorkshop on Privacy in the Electronic Society, pp. 91-102, 2002.

[14] E. Ayday, F. Delgosha, and F. Fekri, "Location-aware security servicesfor wireless sensor networks using network coding," in Proc. IEEEINFOCOM '07, pp. 1226-1234, 2007.

[15 M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strongsource anonymity for sensor networks," in Proc. IEEE INFOCOM'08,pp. 51-55, 2008

[16] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature-basedscheme for securing network coding against pollution attacks," in Proc.
IEEE INFOCOM, 2008