RESEARCH ARTICLE OPEN ACCESS

A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks

Mohammed Tarique [1], Rohan Raul [2], Khalil Pinjari [3], Pranay Patil [4], Rohit Shinde [5]

UG Students [1], [2], [4], & [5], Assistant Professor [3]
Department of Information Technology Engineering
Theem College of Engineering, Boisar
University of Mumbai
Maharashtra – India

ABSTRACT

Energy saving is very important matter of subject in Mobile Ad Hoc Networks (MANETs). Current studies show that network coding can help lessen the energy consumption in MANETs by providing less transmission. Apart from transmission cost, the other sources of energy consumption are data encryption/decryption. The studies show how to control network coding to reduce the energy that is consumed by the data encryption in MANETs. It is interesting that network coding has an agreeable property of key security, based on which encryption can be done quite well. In this paper, we have proposed P-Coding, a lightweight encryption scheme to provide confidentiality for network-coded MANETs in an energy-efficient way. The basic idea of P-Coding is to let the source randomly permute the symbols of each packet (which is prefixed with its coding vector), before performing network coding operations. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding, and thus cannot obtain any meaningful information.

Keywords :- Mobile ad hoc networks, energy saving, network coding, lightweight encryption

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET's) are significant wireless communication models. Mobile Ad Hoc Network (MANET) are infrastructure-less and dynamic network involving wireless mobile nodes that communicate with each other without use of any integrated authority. The mobile and infrastructure less nature of MANETs makes them fit for collecting alternative data in disastrous areas and performing mission-critical communication in battle fields. A serious matters in MANETs is how to reduce energy consumption and maintain a longer life time for mobile nodes. Some energy efficient scheme are proposed to determination this issue [2], [3], & [4]

Current studies that network coding [5] can help realize a lower energy consumption in MANETs [6], [7] & [8]. The energy savings arise from fact that less transmission are required when in-network nodes are assisted to encoded packets. Energy consumption can also come from encryption and decryption processes at each node, as most MANETs need some level of guard on their content. For model, in a battle field, the data communicated between soldiers with mobile devices can be very delicate, and should be kept confidential during transmissions. The easiest approach in providing confidentiality to a network-coded MANETs will be to encrypt the packet payload by using symmetric-key encryption algorithms. While this method is not that efficient reference [9] show that on a Motorola's "Dragon Ball" surrounded microprocessor ,it consumes around 13.9 micro to send a bit, while consumes another 7.9 MicroJ per bit when symmetric-key algorithms are used. Due to the homomorphic environment of HEFs, network coding can be performed straight on the encrypted coding vectors, without impacting the standard network coding operations. In this paper we propose a new encryption system which is a lightweight in totalling by leveraging network coding which makes it very beautiful in network-coded MANETs to further reduce energy consumption.

II. LITERATURE SURVEY

A. "P-CODING: SECURE NETWORK CODING AGAINST EAVESDROPPING ATTACKS"

In this paper [1], author focuses on basic privacy as network coding is still vulnerable to eavesdropping attacks, via which an enemy could compromise the confidentiality of message content. Fundamental studies mostly deal with eavesdroppers that could catch a limited number of packets. But, real situations often consist of more capable opponents, e.g., Global eavesdroppers, which can defeat these systems. In this paper, the author proposed P-Coding, a novel security scheme against eavesdropping attacks in the network coding. P-Coding can capably spoil global eavesdroppers in a clear way by using lightweight permutation encryption which is performed on each message and its coding vector. Moreover, P-Coding is very much highlighted in scalability and toughness, which enable it to be combined into practical network coded systems. Security analysis and simulation results showed the efficiency of the P-Coding scheme.

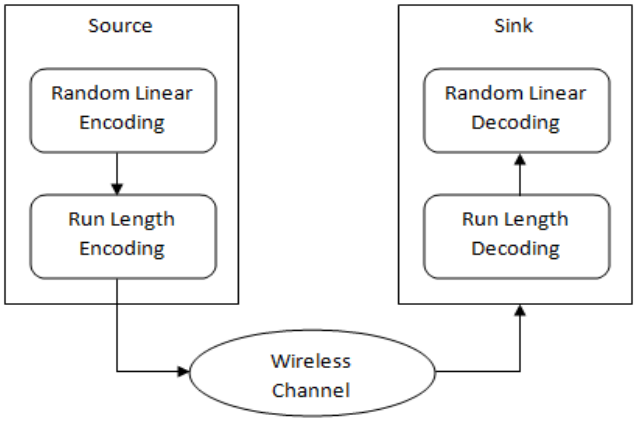

Figure2.1.1: Enhanced P-Coding

B. "Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks"

In this paper [3], the author had addressed the challenge of multicasting in ad hoc wireless networks from the perspective of energy efficiency. Here the author had discussed the impact of the wireless intermediate on the multicasting problem and the essential trade-offs that arise. Further the author proposed and evaluated several algorithms that defined multicast trees for session or connection-oriented traffic when transceiver resources are restricted. These algorithms selected the relay nodes and the corresponding transmission power levels, and realized different degrees of scalability and performance. Here author demonstrated the incorporation of energy considerations into multicast algorithms which could result in improved energy efficiency.

C. "Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding"

In this paper [6], author has proposed the minimum energy required for transmitting one bit of information through a network that represented the most economical way to connect in the network. Further author focused on the layered classic of a wireless network, the minimum energy-per-bit for multicasting in a mobile ad hoc network had been found by a linear program; the minimum energy-per-bit could be attained by acting network coding. When comparing with conventional routing solutions, the network coding not only allows a potentially lower energy-per-bit to be reached, but also enables the perfect solution that could be started in polynomial time, in sharp contrast with the NP-hardness that constructs the minimum-energy multicast tree which results in the optimal routing solution. Later author focused on how the minimum energy multicast preparation is equivalent to a cost minimization with linear edge-based rating, where the edge prices where the energy-per-bits that were the corresponding physical transmission links. Due to the linearity of the pricing arrangement, the minimum energy-per-bit for routing is achievable by using a single delivery tree. A categorization that consisted of tolerable rate region for routing with a single tree was presented. The minimum energy-per-bit for multicasting with routing was originated by an integer lined program. Author showed that the reduction of this integer linear program might now be assumed as the optimization for minimum energy multicasting with network coding. In short, the author presented a joining study of minimum energy multicasting with network coding and routing.

D. "Network Coding- Based Broadcast in Mobile Ad-Hoc Networks"

In this paper [8], author introduced Broadcast operation, which disseminates evidence network-wide, and is very important in multi-hop wireless networks. Owing to the broadcast nature of wireless media, not all nodes need to transmit in order for the note to reach every node. Prior work on broadcast support could be classified as probabilistic i.e. each node rebroadcasted a packet with a given probability or deterministic approaches i.e. nodes pre-selected a few neighbours for rebroadcasting. Further author showed how network-coding could be applied to a deterministic broadcast methods, resulting in significant reduction in the number of announcements in the network. author proposed two algorithms, that rely only on local two-hop topology information and made a wide use of

opportunistic attending to reduce the number of transmissions: 1) a simple XOR-based coding algorithm that provided up to 45% gained as compared to that a non-coding approach and 2) a Reed-Solomon based coding algorithm that determined the optimal coding gain achieved for a coding algorithm that trusted only on local confirmation, with gains up to 61% in the simulations result. Author also showed that the coding-based deterministic approach outclassed the coding-based probabilistic approach.

E. "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols"

In this paper [9], author focused on how safety is becoming an ordinary concern for a wide range of electronic systems that operate, communicate, and store complex data. Author focuses on an important and emerging group of such electronic systems which are battery-powered mobile applications, such as personal digital assistants (PDAs) and cell phones, which are strictly, constrained in the resources they possess, namely, CPU, cordless, and memory. This effort focuses on one important constraint of such devices-battery life-and inspects how it is impacted by the use of various security mechanisms. Author showed a study on the energy consumption supplies of the most popular transport-layer security protocol: Secure Sockets Layer (SSL). Also author examined the impact of various limitations at the protocol level such as authentication mechanisms, cipher suites, and transaction sizes, etc. and the cryptographic algorithm level (cipher modes, strength) on the overall energy consumption for secure data transactions. Author proposed a measurement-based experimental test bed that consisted of an iPAQ PDA which was connected to a wireless local area network (LAN) and running Linux, a PC-based data achievement system for real-time current measurement, the OpenSSL implementation of the SSL protocol, and the parameterizable SSL client and server test program. Based on results, author discussed various occasions for understanding energy-efficient applications of security protocols.

III. EXISTING SYSTEM

The straight approach to provide secrecy for network-coded MANETs is to encrypt the packet load using symmetric-key encryption algorithms. The information fraternization feature of network coding which provides an intrinsic security depending on which a more effective cryptographic scheme can be designed. Vilelaet al. [10] proposed such a scheme. In this scheme, the source performed arbitrary linear coding on the messages that are to be send and locks/encrypts the coding vectors by using the symmetric key which is shared between it and all sinks. Fanet al. [11] proposed encrypt coding vectors by using Homomorphic Encryption Functions (HEFs) in an end-to-end way.

F. Disadvantage of Existing System

Owing to the homomorphic nature of HEFs, network coding can be performed conventional on the encrypted coding vectors, without impacting the standard network coding operations. However, the above two approaches have large above with respect to either computation or galaxy, and may not be suitable for MANETs.

IV. PROPOSED SYSTEM

The proposed system attempts to design a new encryption scheme that can fully adventure the security property of net-work coding. The coding vectors and the message content are both necessary for decoding, arbitrarily reordering/mixing they will generate significant confusion to the eavesdropping challenger. In specific, we propose P-Coding which is a lightweight encryption scheme to fight against eavesdroppers in network-coded MANETs. In a nutshell, with the help of permutation encryption, P-Coding randomly mixes symbols of each packed which is a coded packet (packet prefixed with its coding vector), so as to make it harder for eavesdroppers to locate coding vectors for package decoding.

1) Advantages of Proposed System

A fresh encryption scheme which is lightweight in control by leveraging network coding, which makes it very gorgeous in network-coded MANETs to further reduce energy consumption.

We present here an analysis on the inherent weak security which is more accurate by network coding,

4.2 Proposed System Architecture

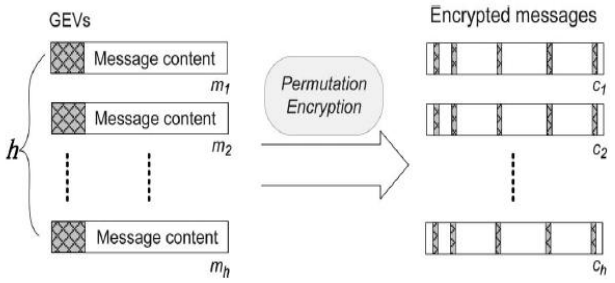

Figure 4.2.1: Encrypted and Decrypted Permutation

V. CONCLUSION

This project involved the education of energy saving problem in MANETs based on the technique of network coding. Preceding studies demonstrated that network coding can shrink energy consumption with less transmission in MANETs. P-Coding, a lightweight encryption scheme on top of network coding, reduces energy consumption in MANETs by decreasing the security cost. P-Coding events the intrinsic security stuff of network coding, and uses simple permutation encryptions to generate great mistake to eavesdropping adversaries. It is publicised that P-Coding is efficient in calculation, and incurs less energy consumption for encryptions/decryptions. Extending the Application of P-Coding to other communication.

FUTURE WORK

The future work includes the application of Enhance P-Coding to other statement networks, e.g. Vehicular Ad Hoc networks

REFERENCES

[1] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, ‘‘P-coding: Secure Network Coding Against Eavesdropping Attacks,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1-9.

[2] S. Singh, C. Raghavendra, and J. Stepanek, ‘‘Power-Aware Broadcasting in Mobile Ad Hoc Networks,’’ in Proc. IEEE PIMRC, 1999, pp. 1-10.

[3] J. Wieselthier, G. Nguyen, and A. Ephremides, ‘‘Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks,’’ Mobile Netw. Appl., vol. 6, no. 3, pp. 251-263, June 2001.

[4] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, ‘‘Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks,’’ Wireless Netw., vol. 8, no. 5, pp. 481-494, Sept. 2002.

[5] 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.

[6] Y. Wu, P. Chou, and S. Kung, ‘‘Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding,’’ IEEE Trans. Commun., vol. 53, no. 11, pp. 1906-1918, Nov. 2005.

[7] C. Fragouli, J. Widmer, and J. Boudec, ‘‘A Network Coding Approach to Energy Efficient Broadcasting: From Theory to Practice,’’ in Proc. IEEE INFOCOM, 2006, pp. 1-11.

[8] L. Li, R. Ramjee, M. Buddhikot, and S.Miller, ‘‘Network Coding-Based Broadcast in Mobile Ad-Hoc Networks,’’ in Proc. IEEE INFOCOM, 2007, pp. 1739-1747.

[9] N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, ‘‘AStudy of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,’’ IEEE Trans. Mobile Comput., vol. 5, no. 2, pp. 128-143, Feb. 2006.

[10] J.P. Vilela, L. Lima, and J. Barros, ‘‘Lightweight Security for Network Coding,’’ in Proc. IEEE ICC, May 2008, pp. 1750-1754.

[11] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, ‘‘An Efficient Privacy-Preserving Scheme Against Traffic Analysis in Network Coding,’’ in Proc. IEEE INFOCOM, Apr. 2009, pp. 2213-2221.

[12] K. Bhattad and K.R. Narayanan, ‘‘Weakly Secure Network Coding,’’ in Proc. NetCod, Riva del Garda, Italy, Apr. 2005.

[13] T. Ho, M. Me´dard, 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, Oct. 2006.

[14] C.E. Shannon, ‘‘Communication Theory of Secrecy Systems,’’ Bell Syst. Tech. J., vol. 28, no. 4, pp. 656-715, Oct. 1949.

[15] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, Oct. 1996.

[16] N. Cai and R.W. Yeung, ‘‘Secure Network Coding,’’ in Proc. IEEE ISIT, June 2002, pp. 323-329.

[17] A. Dimovski and D. Gligoroski, ‘‘Attacks on the Transposition Ciphers using Optimization Heuristics,’’ in Proc. Int’l Sci. Conf. Inf., Commun. Energy Syst. Technol., Oct. 2003, pp. 1-4.

[18] C. Gkantsidis and P. Rodriguez, ‘‘Network Coding for Large Scale File Distribution,’’ in Proc. IEEE INFOCOM, Mar. 2005, pp. 2235-2245.

[19] J. Daemen and V. Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.

[20] L.C. Washington and W. Trappe, Introduction to Cryptography: With Coding Theory. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[21] J. Giddy and R. Safavi-Naini, ‘‘Automated Cryptanalysis of Transposition Ciphers,’’ Comput. J., vol. 37, no. 5, pp. 429-436, 1994.

[22] M.D. Russell, J.A. Clark, and S. Stepney, ‘‘Making the Most of Two Heuristics: Breaking Transposition Ciphers with Ants,’’ in Proc. Congr. Evol. Comput., 2003, pp. 2653-2658.

[23] P. Paillier, ‘‘Public-Key Cryptosystems based on Composite Degree Residuocity Classes,’’ in Proc. EUROCRYPT, May 1999, pp. 233-238.

[24] The OpenSSL project. [Online]. Available: http://www.openssl.org/

[25] D.W. Carman, P.S. Kruus, and B.J. Matt, ‘‘Constraints and approaches for distributed sensor network security (Final),’’ NAI Labs, Glenwood, MD, USA, DARPA Proj. Rep., 2000.

[26] K. Aoki and H. Lipmaa, ‘‘Fast Implementations of AES Candidates,’’ in Proc. 3rd AES Candidate Conf., 2000, pp. 13-14.

[27] [27] M. C ˇ agalj, J. Hubaux, and C. Enz, ‘‘Minimum-Energy Broadcast in All-Wireless Networks: Np-Completeness and Distribution Issues,’’ in Proc. ACM MobiCom, 2002, pp. 172-182.

[28] [28] L. Lima, M. Me´dard, and J. Barros, ‘‘Random Linear Network Coding: A Free Cypher?,’’ in Proc. IEEE ISIT, June 2007, pp. 546-550.

[29] J. Wang, J. Wang, K. Lu, B. Xiao, and N. Gu, ‘‘Optimal Linear Network Coding Design for Secure Unicast with Multiple Streams,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1-9.

[30] J. Benaloh, ‘‘Dense Probabilistic Encryption,’’ in Proc. Workshop Sel. Areas Cryptogr., Aug. 1994, pp. 120-128.

[31] A.-F. Chan, ‘‘Distributed Symmetric Key Management for Mobile Ad Hoc Networks,’’ in Proc. IEEE INFOCOM, 2004, pp. 2414-2424.

[32] J.V.D. Merwe, D. Dawoud, and S. McDonald, ‘‘A Survey on Peerto- Peer Key Management for Mobile Ad Hoc Networks,’’ ACM Comput. Surveys, vol. 39, no. 1, pp. 3-45, 2007.

[33] M. Wang and B. Li, ‘‘R2: Random Push with Random Network Coding in Live Peer-to-Peer Streaming,’’ IEEE J. Sel. Areas Commun., vol. 25, no. 9, pp. 1655-1666, Dec. 2007.

[34] Y. Hu, H.C. Chen, P.P. Lee, and Y. Tang, ‘‘NCCloud: Applying Network Coding for the Storage Repair in a Cloud-Of-Clouds,’’ in Proc. USENIX FAST, 2012, p. 21.

[35] S. Ross, Introduction to Probability Models, 9th ed., New York, NY, USA: Academic, 2007.