ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

SECURE NETWORK CODE AGAINST POLLUTION ATTACKS

Dr.S.Audithan

Principal, P.R.Engineering College, Vallam, Thanjavur, India

ABSTRACT

Network coding helps to multicast the information available at the source to all the destination. Network coding offers increased throughput and improved robustness against pollution attacks in network. The pollution attacks consists of injecting malicious packets in the network, it causes severe damage to the system, which breaks the network security. This paper presents an unconditionally secure authentication code that provides multicast network coding. In multicast network coding one sender and multiple receivers are available. A trusted key distribution centre initially computes a private keys and public keys, the required keys are send to the sender and the receiver. The sender computes an authentication tag using his private key and appends a tag to the message. This authenticated message is broadcast to all the receivers. Each receiver can verify the data origin and integrity of the message received without decoding, and thus to detect and discard the malicious packets that fail the verification. The sufficient number of uncorrupted messages received by the receiver to decode and obtain the original message sent by the source.

1. INTRODUCTION

Network coding helps to multicast the information available at the source to all the destination. It allows intermediate nodes between the source and the destination to store and forward the packets and also encode the packets before forwarding them. Network coding has various advantages such as maximizing the usage of network resources and robustness against packet losses. It also deals with change of topology and delays. Network coding has various applications such as file download and file distribution. Network coding helps to increase the throughput, but it suffer greatly from pollution attacks.

Pollution attacks consist of injecting malicious packets in the network, which break the network security. A more severe problem is pollution propagation, a small number of polluted messages can quickly propagate into the network and infect a large number of nodes in the network. In general, network security attacks are of two types. They are, 1. Passive

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

attack 2.Active attack.Passive attack: It makes use of information from the system, but does not affect the system resources. There are two types of passive attacks, release of message contents and traffic analysis.Release of message contents: To prevent an opponent from learning the content of the transmission.Traffic analysis: It masks the contents of the message, so the opponent could not extract the information from the message.

Active attack: Active attacks involve some modification of the data stream or the creation of a false stream. It cannot be prevented easily. Active attacks can be subdivided into four types. They are,Masquerade: One entity pretends to be a different entity. [6] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

Replay: The passive capture of a data unit and its subsequent retransmission produce an unauthorized effect.Modification of message: The modification of the original message

Denial of service: Disruption of entire network.

In our project mainly focuses on Impersonation attack and Substitution attack. The attacker tries to construct a valid tagged message without seen any previously transmitted message (impersonation attack). The attacker try to observe the message and altering the original message (substitution attack).This pollution attack problem is addressed by authentication technique. It checks both the origin and integrity of the data. With no integrity check performed, the honest intermediate node receive single malicious packet and perform the encoding of malicious packet with other packets. It causes severe damage in the network. To avoid this problem, we use three security services that provides authentication.

Data Integrity: Protecting the data from any modification by the malicious nodes.

Data origin authentication: validating the identity of the origin of the data.

Nonrepudiation: Guaranteeing that the origin of the data cannot deny having created and sent data.

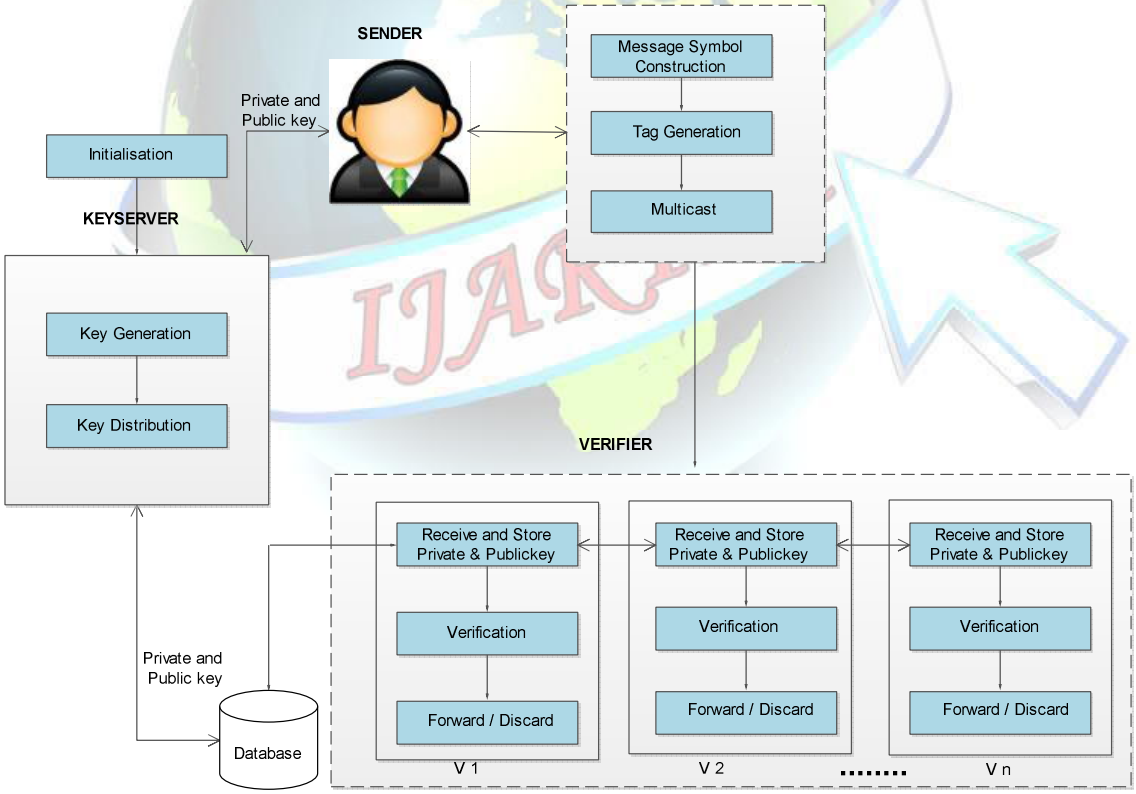
An unconditionally secure authentication scheme provides the multicast network coding with robustness against pollution attacks. In this scheme where one transmitter communicates to multiple receivers who cannot all be trusted. The transmitter first appends a tag to a common message and then it will be send to all the receivers, who can separately verify the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

authenticity of the tagged message using their own private secret key. In this there are a group of malicious receivers also available these malicious receivers can either perform impersonation or substitution attacks. Impersonation attack: If they try to construct a valid tagged message without having seen any transmitted message before. Substitution attack: If they first listen to atleast one tagged message before trying to fake a tag in such a way that the receiver will accept the tagged message. If the best chance of success in the attack is |1/T|, then the Perfect Protection is obtained. Where |T| is the size of the tag space.

We call a (k,V,M) network coding authentication code an authentication code for V verifying nodes, which is unconditionally secure against either impersonation or substitution attacks done by a group of at most k-1 advesaries, possibly belonging to the verifying nodes, where the source can use the same key at most M times. This is the definition of multicast network coding.

2.SYSTEM ARCHITECTURE



V 1,V 2,.....,V n=Verifiers

Figure(1) System Architecture

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

Figure(1) explains the overall Architecture of the system in which the Initialisation block who provides the values q, the polynomials $p_i(x)$ are of the degree k-1. The KeyServer initially compute and distribute Private and Public keys to the Sender and all the verifiers in the multicast network.The Sender first construct the messages as the symbols and then generate a Authentication tag , this tag is append to the message and then finally the packets are multicast to all the verifiers in the network.The verifier verify the Authenticity of the tagged message using their own private key.The verified message is correct then it will be forward message to the destination otherwise it will be discarded.

3. MODULES

3.1Key Generation

A trusted key distribution centre (KDC) randomly generates M+1 polynomials $P_0(x),.....,P_M(x) \in F_q^{l(x)}$. These polynomials are of degree k-1,

It is denoted by ,$P_i(x)=a_{i0}+a_{i1}x+a_{i2}x^2+....+a_{i,k-1}x^{k-1}$, i=0,....,M.

3.2 Key Distribution

A trusted key distribution centre (KDC) distribute the private keys and public keys to the sender and receiver.

($P_0(x),.....,P_M(x)$) are private keys and $x_1,....,x_V$ are public values.

3.3Authentication Tag Generation

The sender wants to send n messages $s_1,....,s_n \in F_q^l$ .The sender computes an authentication tag by using his private keys, it is denoted by

$As_i(x) = P_0(x)+s_i P_1(x)+s_i^q P_2(x)....+s_i^{q(M-1)} P_M(x)$, i=1,....,n.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

The sender sends the packets X_i are of the form

X_i=[1,s_i,As_i(x)] ∈ F_q^{1+l+kl} , i=1,.....,n.

3.4Verification

The receiver Y(R_i) verify the packets sent by the source.The received tagged vector

Y(R_i) ∈ $F_q^{h(i)*N}$ at a node R_i with h (i) incoming edges $e_{i,1}$,.....,$e_{i,h(i)}$ when the sender is sending X_j==[1,s_j,As_j(x)] ∈ F_q^{1+l+kl} , j=1,.....,n.

$$Y(R_i)=\begin{bmatrix} g_{1(e_{i,1})} & \cdots & g_{n(e_{i,1})} \\ \vdots & \cdots & \vdots \\ g_{1(e_{i,h(i)})} & \cdots & g_{n(e_{i,h(i)})} \end{bmatrix}\begin{bmatrix} 1 & s_1 & As_1(x) \\ \vdots & \ldots & \vdots \\ 1 & s_n & As_n(x) \end{bmatrix}$$

Whose *m*th row, m=1,....,h(i) is given by

$$Y(e_{i,m})=\left[\sum_{j=1}^{n} g_{j(e_{i,m})}, \sum_{j=1}^{n} g_j(e_{i,m})s_j, \sum_{j=1}^{n} g_{j(e_{i,m})}As_j(x)\right]$$

The below two computations are coincide then there is no alteration of the protocol.

$$\sum_{j=1}^{n} g_{j(e_{i,m})}As_j(x_i) = \sum_{j=1}^{n} g_{j(e_{i,m})}P_0(x_i)$$

$$+\sum_{j=1}^{n} g_j(e_{i,m})s_j P_1(x_i)+\ldots\ldots +\sum_{j=1}^{n} g_{j(e_{i,m})} s_i^{q(M-1)}P_M(x_i)$$

4. PERFORMANCE ANALYSIS

Tag or signature size	Kl
Communication cost	Kl+1
Tag or signature computational cost	n(M-1)l exp nkMlmult
Verification computational cost	((M-1)+k-2)lhexp ((M+1)+k-1)lhmult
Storage at the source Storage at the verifiers	(M+1)lk (M+1)l

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

5. REFERENCES

1. S.Agrawal and D.Boneh, "Homomorphic MACs: MAC- based integrity for network coding," in proc. Appl. Cryptography Netw. Security, 2009, pp. 292-305.

2. R.Ahlswede, N.Cai, S.R.Li, and R.W.Yeung, "Network information flow,"IEEE Trans. Inf. Theory, vol.46, no.4, pp.1204-1216, Jul 2000.

3. "Avalanche: File swarming with network coding", Microsoft Research, Cambridge, U.K. [Online]. Available: http://research.microsoft.com/en-us/projects/avalanche.

4. D.Boneh, D.Freeman, J.Katz, and B.Waters, "Signing a linear subspace: Signature schemes for network coding,"Rep. 2008/316, 2008 [Online]. Available: http://eprint.iacr.org/2008/316. Inf. Sci. Syst..2006

5. D.Charles, K.Jain, and K.Lauter, "Signature for network coding," in Proc. Conf. Inf. Sci. Syst., 2006. pp. 857-863.

6.Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

7. P.Chou, Y.Wu, and K.Jain, "Practical network coding," in Proc. Allerton Conf. Commun., Control, Comput., 2003, pp. 40-49.

8. Y.Desmedi, Y.Frankel, and M.Yung, "Multi-receiver/multi—sender network security: Efficient authenticated multicast/feedback,"in Proc. IEEE INFOCOM, 1992, vol.3, pp. 2045-2054.

9. A.G.Dimakis and P.B.Godfrey, M.J.Wainwright, and K.Ramchandran, "Network coding for distributed storage systems," in Proc. IEEE INFOCOM, 2007, pp. 2000-2008.

10. C.Gkantsidis, P.Rodriguez, "Network coding for large scale content distribution,"in Proc. IEEE INFOCOM, 2005, vol.4, pp. 2235-2245.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

11. C.Gkantsidis, J.Miller, and P.Rodriguez, "Comprehensive view of a live network coding P2P system,"in Proc. ACM SIGCOMM IMC, 2006, pp. 177-188.

12. C.Gkantsidis and P.Rodriguez, "Cooperative security for network coding file distribution," in Proc. IEEE INFOCOM, 2006, pp. 1-13.

13. G.Hanaoka, J.Shikata, Y.Zheng, and H.Imai, "Unconditionally secure digital signature schemes admitting transferability," in Proc. ASI-ACRYPT, 2000, vol.1976, LNCS, pp. 130-142.

14. S.Katti, H.Rahul, W.Hu, D.Kattabi, M.Medard, and J.Croweoft, "XORs in the air: Practical wireless network coding," in Proc. ACM SigCOMM. 2006, pp. 243-254.

15. R.Koetter and M.Medard, "An algebraic approach to network coding," IEEE/ACM Trans. Netw., vol.11, no.5, pp. 782-795. Oct. 2003.

16. R.Koetter and F.R.Kschischang, "Coding for errors and erasures in random network coding,"IEEE Trans. Inf. Theory, vol. 54, no. 8, pp. 3579-3591, Aug. 2008.

17. S.Y.R.Li and R.W.Yeung, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no.2, pp. 371-381, Feb. 2003.

18. F.Oggier and H.Fathi, "Multi-receiver authentication codes for network coding," in Proc. 46thAnnu. Allerton Conf. Commun., Control, Comput., 2008, pp. 1225-1231.

19. R.Safavi-Naini and H.Wang, "New results on multi-receiver authentication codes," in Proc. Eurocrypt, 1998, vol. LNCS 1403. Pp. 527-541.

20. D.Silva, F.R.Kschischang, and R.Koetter, "A rank-metric approach to error control in random network coding," IEEE Trans. Inf. Theory, Vol. 54, no.9, pp. 3951-3967, Sep. 2008.

21. D.R.Stinson, Cryptocraphy: Theory and Practice. Boea Raton, FL: CRC Press, 1995.

22. Z.Yu, Y.Wei, B.Ramkumar, and Y.Guan, "An efficient signature-based scheme for securing network coding against pollution attacks," in Proc. IEEE INFOCOM, 2008, pp. 1409-1417.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

23. Z.Yu, Y.Wei, B.Ramkumar, and Y.Guan, "An efficient scheme for securing XOR network coding against pollution attacks," in Proc. IEEE INFOCOM, 2009, pp. 406-414.

24. F.Zhao, T.Kalker, M.Medard, and K.J.Han, "Signatures for content distribution with network coding," in Proc. IEEE Int. Symp. Inf. Theory, 2007, pp. 556-560.