Content Security Scheme for Content Centric Networks

Fawad Khan[1], Sarmad Ullah Khan[2(✉)], and Inam Bari[1]

[1] Electrical Department, Fast Nuces, Peshawar, Pakistan
{fawad.khan, inam.bari}@nu.edu.pk
[2] Electrical Department, Cecos University, Peshawar, Pakistan
sarmad@cecos.edu.pk

Abstract. Content Centric Networking (CCN) is a recently proposed internet paradigm that is based on content abstraction rather than host abstraction. People nowadays are interested in content and it does not matter from which locations they get the required content. Content requesting node has to make sure while receiving content from content publisher that whether the publisher and its content is trustable or not. To validate the authenticity of content on each node, an effective security scheme should be developed. In this paper we propose a content security scheme for CCN. We analyzed the performance of proposed scheme using ccnSim simulator and its security validation using AVISPA tool.

Keywords: Authentication · Content security · Validation

1 Introduction

Content Centric Networking (CCN) is proposed by Van Jacobson and his team [1]. CCN is built on the fact that today's networking is more oriented towards contents rather than hosts. It is the key reason for a radical revision of the current internet architecture (TCP/IP), named hosts to named data. Content by itself can be addressed, routed and secured over the network; making the revision a necessity for effective networking.

In the proposed scheme, each small network has its own unique identity which distinguishes it from other networks over the internet. The rest of the paper is organized as follows. In Sect. 2, we provide some related work followed by our proposed content security scheme in Sect. 3. Section 4 evaluates the performance of the proposed scheme using ccnSim simulator. In Sect. 5, we validate the security of the proposed scheme using AVISPA tool and Sect. 6 concludes the paper.

2 Related Work

Recent research work in cryptography is based on PKI [3]. In [2], Smetters proposed the use of PKI for CCN. In this approach each node has a pair of private key and public key. Public keys are used to encrypt data and private keys are used for decryption. For a

J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 546–550, 2015.
DOI: 10.1007/978-3-319-23829-6_41

recipient to validate the authenticity, it has to get services from a Certification Authority (CA).

Identity based Public Key Generator (ID-PKG) [4] was proposed by Khalili and Katz for ad-hoc mobile networks. They eliminate the need of services of third party for certification and utilize the user identity for generating its public key. The scheme imposes several problems when used are: (1) How do the nodes identify the PKG. (2) How to update master secret key of system.

Identity based Public Key Cryptography (ID-PKC) is proposed by Deng [5] for cryptographic management and certification. However performance of this scheme is poor in case of compromise on any of key generating nodes.

Key Management Scheme (KMS) for CCN [6] is proposed by Sarmad and Thaibault. The major problem with this scheme is overhead. For each chunk of content; keys are evaluated and distributed over the network leading to large key shares, bandwidth and memory management issues.

3 Proposed Scheme

The existing key management schemes are ill suited for securing the content in CCN due to its content abstraction because locations do not matter. Hence the content needs to be secured, not the path over which the content travels.

3.1 Network Architecture and Deployment

Since internet is a combination of many small sized networks, we consider each network being handled by its own Network Manager (NM) which is a powerful node to look for all management and security related issues of network. Each of the networks is assigned a unique Network Identity (NI) through which that network is distinguished from other networks over the internet.

Initially all the nodes who want to join the network sent a joining request to a network manager. After receiving joining requests, network manager sends back Secret Key (SK) parameters, Network Identity (NI), a unique node Identity (ID) and Security Algorithm (SA) to each joining node. All these parameters are assigned to each node offline. Secret key parameters are used by node to generate its asymmetric key i.e. a pair of public and private key. Network identity is for distinguishing this network from other networks over the internet. Node identity is to make a node distinguished from other nodes in the network and security algorithm is used for defining how to calculate signatures, components of data packet, role of intermediate nodes and final content requesting node on receiving a data packet.

3.2 Network Security Management

After network is deployed, the node publishing the content will calculate two types of signatures as shown in Fig. 1. Signature1 (Sig1) is for ensuring validity of content as it moves between the intermediate nodes while Signature2 (Sig2) is for ensuring the

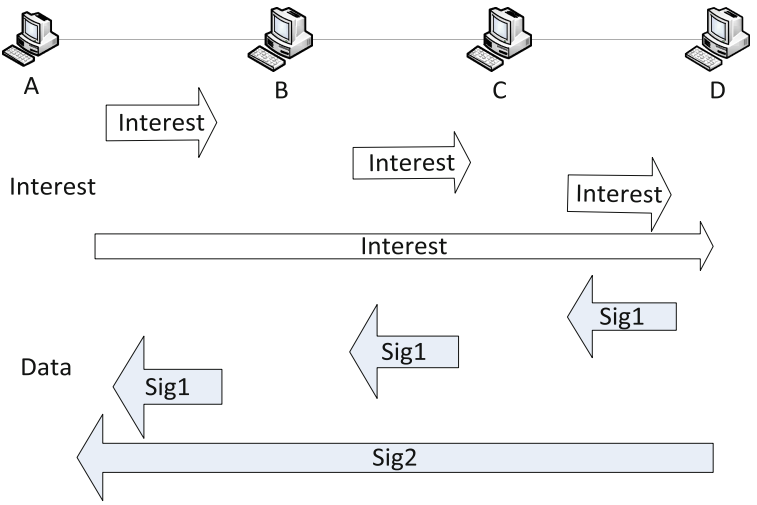

Fig. 1. Signature Types

validity as well as provenance of the content by the final content requesting node. The first one named Signature1 will be validated on each intermediate node till the content reaches the actual content requesting node. The second one named Signature2 will be validated only by the final node that actually generated the interest request for content. Signature2 can also be validated by intermediate node if it wants to store a copy of that content for future use. By validating Signature2 a node can built its trust on content publisher because identity of the publisher is part of Signature2. The publisher publishing the content will calculate M = f (Content) where f is a standard one-way hash function. After then Sig2 by g (M, ID, NI) where g is an arbitrary function. Finally it will calculate Sig1 by encrypting (M, Sig2, NI) by the public key of the node from which it received the request for the content.

$$\mathrm{M} = \mathrm{f}\ (\mathrm{Content}) \tag{1}$$

$$\mathrm{Sig2} = \mathrm{g}\ (\mathrm{M},\ \mathrm{ID},\ \mathrm{NI}) \tag{2}$$

$$\mathrm{Sig1} = (\mathrm{M},\ \mathrm{Sig2},\ \mathrm{NI})\ \mathrm{Kp} \tag{3}$$

The data packet sent back is composed of (Content, Sig1, Sig2, ID) and each intermediate node on receiving the packet will validate Sig1 (decrypt using its private key) to ensure validity of content and once ensured it will again encrypt (M, Sig2, NI) by the public key of the node from which it received the request for the content. The process of validating Sig1 (decrypting using its private key) and again encrypting it by the public key of adjacent nodes continues till the actual content requesting node has reached. When the actual content requesting node has received the packet, it will validate Sig1 by its private key and after then it will validate Sig2 by g (M, ID, NI). Since Sig2 contain the publisher ID as part of it; hence correct authentication of Sig2

builds trust on the publisher by content seeker. Figure 1 shows node D when publishing content will calculate both signatures and send those signatures along with content in packet. Node C and node B are intermediate nodes hence they will validate Signature1 using their private key and re-encrypt using adjacent nodes public key. Node A which is actual content requesting node will validate both signatures for ensuring trust on publisher and validity of content.

3.3 Intruder/Attacker Scenario

An attacker has only the knowledge of public keys of the nodes to which it is directly connected in the network. An attacker node on receiving the packet has three options. First one is forwarding the packet directly to content seeker node; content seeker will be unable to validate Sig1 because Sig1 was encrypted using public key of attacker by publisher node, hence content seeker node will discard the packet. The second option of attacker node is to evaluate Sig1 using content seeker Public key; which it fail to because it do not have Network Identity (NI) and Security Algorithm (SA), hence content seeker will fail to authenticate the Sig1 and will discard the packet. The last option will be modifying the packets which leads to failure of authentication of both the signatures hence packet is discarded.

4 Performance Analysis

In this section we show the analysis of our proposed scheme using ccnSim simulator [7]. We have modified the behavior of node '1' in Abilene topology as an attacker node. When node '1' receives a packet for node '0' it modifies the packet contents. Node '0' sends an interest request for content. The corresponding data packet to Node '0' can be delivered only from two paths either form Node '10' or from Node '1'. The packets sent by node '0' are discarded by node '1'. Table 1 shows the results.

Table 1. CCNSim Results

Total Packets Received By Node '0'	Total Packets sent by Attacker Node '1'	Malicious Packets Detected by Node '0'	Attackers Success
40384	3187	3187	0

5 Security Validation

To validate the security of proposed scheme; we have implemented our proposed scheme in AVISPA tool to check its strength against attackers who act as man in the middle and act maliciously on the data in order to modify the data. We checked out its security using OFMC (On the fly model checker) and CL-Atse (Constrained Logic Based Attack Searcher) [8]. OFMC builds an infinite tree based on the protocol analysis problem and uses number of techniques to represent the state space. CL-Atse provides

translation of the security protocol into a set of constraints to find attacks on protocols. The results are shown in the Table 2.

Table 2. AVISPA Tool Results

Technique	Summary
OFMC	SAFE
CL-AtSe	SAFE

6 Conclusion

Our proposed scheme proves effectively with respect to all schemes discussed in Sect. 2. Main features we took into consideration are: (1) Effective memory management i.e. the nodes in the network will have to remember only the public keys of adjacent nodes in the network. (2) Eliminated centralized certification authority. (3) Trust establishment between content seeker and content publisher. (4) Ensuring validity of content at intermediate nodes and also at final content requesting node.

References

1. Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., Braynard, R.L.: Networking named content. In: CoNEXT 2009: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, pp. 1–12. ACM, New York (2009)
2. Smetters, D., Jacobson, V.: Securing Network Content, PARC, Technical report, October 2009
3. Capkun, S., Buttyan, L., Hubaux, J.-P.: Self-organized public-key management for mobile ad hoc networks. IEEE Trans. Mob. Comput. **2**(1), 52–64 (2003)
4. Khalili, A., Katz, J., Arbaugh, W.: Toward secure key distribution in truly ad-hoc networks. In: 2003 Symposium on Applications and the Internet Workshops, pp. 342–346, January 2003
5. Deng, H., Mukherjee, A., Agrawal, D.: Threshold and identity-based key management and authentication for wireless ad hoc networks. In: International Conference on Information Technology: Coding and Computing 2004, ITCC 2004, vol. 1, pp. 107–111, April 2004
6. Khan, S.U., Cholez, T., Engel, T., Lavagno, L.: A key management scheme for content centric networks. In: IFIP/IEEE Integrated Network Management Symposium (IM 2013), Ghent, Belgium, 27–31 May 2013
7. Rossini, D.R.G.: Caching performance of content centric networks under multi-path routing (and more), in Technical report, Telecom ParisTech (2011)
8. http://www.avispa-project.org/