Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.239 – 243

RESEARCH ARTICLE

Avoiding Pollution Attacks in Network Coding using Authentication Code

Mangesh N. Bhandare[1], Ravindra C. Thool[2], Gurdeep Singh Wahi[3]
[1]Department of Information Technology, SGGSIE &T, Nanded, India
[2]Department of Information Technology, SGGSIE &T, Nanded, India
[3]Department of Computer Engineering, Gramin Polytechnic, Nanded, India

[1] mangeshbhandare@gmail.com; [2] rcthool@gmail.com; [3] guru_wahi@yahoo.com

Abstract— When packets are transferred they suffer from the different pollution attacks by injecting malicious packets in the network. When pollution attacks occurs that provides greater damage in the network routing. In this paper, we address this issue by designing a secure authentication code that is computed by using different key generation functions and the key is distributed to the intermediate nodes and to the destinations. The proposed scheme allows verifying the integrity of receiving packets not only at destination nodes, but also at intermediate nodes. The packets which fail the verification those are detected and discarded by considering they are malicious packets or polluted packets in the network. In this way, the pollution in the network is removed before packets reaching to the destinations. This will reduce the pollution attacks from the outsiders and increase the throughput and performance of the data transmission in the coding based network.

Key Terms: - Network coding; Pollution attacks; Authentication code; Authentication key generation

I. Introduction

In traditional routing scheme data were transferred through intermediate nodes by simply store and forward technique, where in network coding scheme intermediate nodes not only switch the packets coming from sender to receiver but also check the data packets for their authentication and if the data packets fails to authenticate, that packets are discarded from the network and thus the pollution is removed from the network. Network coding provide various advantages like avoiding the packet loss in the network, maximize the usage of resources, increase the data transmission capacity and provide security the user data.

In the network when data is transferred from source to destination, malicious packets may be added by the malicious intermediate nodes. Also outsiders can inject malicious messages in the network and transferred to the destination called impersonation attack or original messages can be altered at intermediate nodes called substitution attack and these attacks cannot be detected at destination. So to identify these attacks and for secure data transmissions the digital signatures, MAC, authentication code are appended to messages at source.

To prevent the pollution attacks, we do not need all the functionalities provided by the digital signatures and by the message authentication code but the packets coming at the intermediate node or at the intermediate devices are coming from the same source and if yes, only those packets are combined together and forwarded towards the destinations. Also digital signature finds where from the data packets are coming and who is the source [9]. The digital signature scheme can be used for secure data transmission using public and private key but the key generation and checking the digital signature is quite time consuming and to minimize the data transmission time we are using the network coding scheme.

We present our experiences in the implementation of system using Network Coding. We say that the transmission time is minimizes as the pollution (malicious) packets are removed from the network. In particular, we show that network coding is feasible and minimizes the processing overhead at the sender and at the receiver by using the intelligent intermediate devices by increasing their workload.

II. RELATED WORK

Several authentication schemes have been recently proposed to detect the polluted packets at intermediate nodes based upon cryptographic functions with computational assumptions [1].

The scheme proposed in [2] for network coded content distribution allows intermediate nodes to detect malicious packets injected in the network and to alert neighboring nodes when a malicious packet is detected. It uses hash function to generate the hash values of the encoded data blocks that are then sent to the intermediate nodes and destinations before the data is encoded. The distribution of these hash values is done over a pre-established secure channel.

The scheme proposed in [3] is based on RSA algorithm in which intermediate nodes can authenticate the packets in transit without decoding and generate a verifiable signature of the packet that they have just encoded without knowing the senders secret key. In this scheme one key pair is require for a file to be verified.

The scheme proposed in [9] uses a standard signature scheme that based upon the hardness of discrete logarithm problem. The blocks of data are considered as vectors spanning a subspace. The signature is not calculated for every data blocks, but for vectors subspace. The signature verification allows to check if the received vector belongs to the data subspace and the file is authenticated. This scheme also requires fresh keys for every file.

The signature schemes proposed in [9] follow the approach used in [4] with improvements in terms of public key size and per packet overhead. The signature schemes proposed are designed to authenticate a linear subspace designed by the vectors containing data blocks. Signatures on a linear subspace are more than enough to authenticate all the vectors used in this same subspace. With these schemes, a single public key can be used to verify multiple files

By comparing the different scheme's proposed in [2, 3, 4, 9] provides the security to data transmission in the network and minimizes the pollution in the network. Finally, the most recent related works have been presented in [5], where a message authentication code has been proposed to provide integrity for network coding, this is a secure scheme in particular network coding against pollution attacks has been given.

III. PROPOSED SYSTEM

In this paper, we propose an unconditionally secure solution that provides security to data packets from the pollution attacks. Our solution allows intermediate nodes and destinations to verify the data origin and integrity of the messages received without decoding, and thus to detect and discard the malicious messages that fail the verification. It is important to note that destinations must receive a sufficient number of uncorrupted messages to decode and recover the entire file sent by the source. However, our solution provides the destinations with the ability to filter out corrupted messages and to have them filtered out by intermediate nodes as well. This our scheme overcomes the problems occurred in [2, 3, 4, 9] and improves the performance and throughput of data transmission in the network.

In our scheme we propose the use of following authentication techniques

A. *Key Generation:*

The trusted authority i.e. means server generates a secure key for a file before the file is to be transferred over the network. Only one key is generated for a file by using the different key generation functions such as random number generator (RAND), different polynomials, pseudo-random number generator (PRNG) are used. As the number of digits in the key increase, the security is increases.

B. *Key Distribution*

The generated key is broadcasted over the network channels to all the destinations and to all the intermediate devices used in the network system. The key is allocated to them at the times of sign up into a service protected by this scheme.

C. *Authentication Tag*

Suppose when source want to communicate with destinations by sending *n* number of massages then the source compute an authentication tag by using different key generation functions and then this key is integrated with the message. This authentication tag is added after the message.

Pollution Attack:

Pollution attack means the hacker or attacker will hack or get control over any intermediate device (router) in network, which means the router will be in control of the hacker (unauthenticated person). He can get control all over the data which is flowing through that router**.** He may change the original data packets, add some extra packets in the network or can modify the data. Or simply we can say that pollution attack means addition of malicious packets other than the sender has send.

Network Coding

Network coding is a technique which can be used to improve a network's throughput, efficiency and scalability, as well as resilience to attacks and eavesdropping, as compared to traditional methods of OSI model or TCP/IP model. Instead of simply relaying the packets of information they receive, the nodes of a network take several packets and combine them together for transmission. This can be used to attain the maximum possible information flow in a network.

Network coding replaces the traditional store and forward mechanism of intermediate resources and assign some task of authentication to intermediate resources and to nodes to identify the polluted packets and remove the pollution from the network.

In the multicast network coding problem, a source S needs to deliver n packets to a set of k terminals over an underlying network G. The nodes of the coding network can be broadly categorized into two groups. The first group includes encoding nodes, i.e., nodes that generate new packets by combining data received from two or more incoming links. The second group includes forwarding nodes that can only duplicate and forward the incoming packets. Encoding nodes are, in general, more expensive due to the need to equip them with encoding capabilities. In addition, encoding nodes incur delay and increase the overall complexity of the network [7].

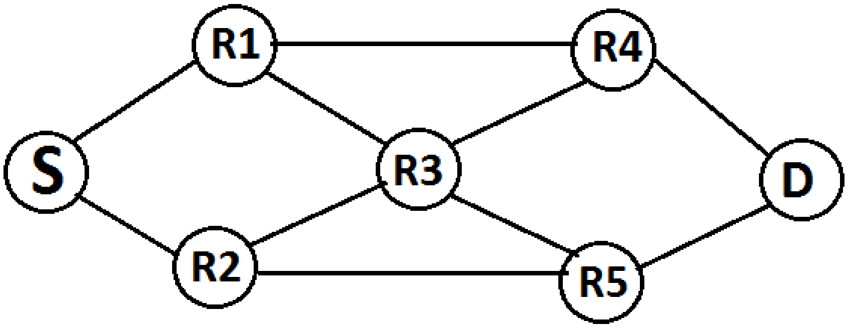

Fig. 1. Example of a network topology

To implement our proposed scheme in practice we have used one source, one destination and five intermediate devices say routers as shown in fig.1. S is the source who is sending file to destination D and R1, R2, R3, R4 are the intermediate routers or say encoding nodes. When source S want's to send a file then authentication key is generated by using random number generator function and the key distributed over the network i.e. key is assigned to all the intermediate devices, destinations and to the message file which is to be send. Then the file is transferred over the network by checking the integrity or authentication tag of every packet with the distributed key to devices, if the key matched then only the packets are transferred forward otherwise the packets are discarded by considering they are pollution in the network.

To check this scheme we have used a hacker module. In hacker module we are getting control over an intermediate device to inject the packets in the network. But when the device is accessed then it lost its assigned key and network identifies that the device is accessed by unauthenticated person and then it changes the path of data transmission by skipping that particular hacked router. In this way we have authenticated the network devices as well as the data packets which are going to be transferred over the network.

In this way we are checking the integrity of packets at every intermediate device without decoding the whole data packet of file which is transferred from source. This will reduce the work of source and destination i.e. generation of cryptographic key for every data packet at source and decoding the packets by using public & private key at destination, this take much time and increase the work load of source and destination.

The proposed scheme is robust against pollution attacks from outsiders, as well as coalitions of malicious insider nodes, which have the ability to perform the integrity check, but instead get corrupted and use their knowledge to themselves attack the network.

This scheme provides some advantages that are:

1) Security:

By providing the authentication tag with every packets, the data is made secure from unauthenticated access and from any kind of tampering.

2) Save the transmission time:

As the malicious packets are removed when they reach at the first intermediate device and find the clear path from source to destination.

But in our scheme we are checking the authentication tag of every incoming packet at intermediate device and at first encoding device the pollution is removed from the network and original data is received at destination without any modification or any alteration. It is quite complex and time consuming to check the authentication tag of each packet at every intermediate node.

Throughput and Goodput

The throughput is defined as the rate of non-corrupted messages received at destination. The goodput is defined as the rate of the useful information received, i.e., excluding the overhead presented by the proposed scheme. The proposed scheme enhances a packet of size sent from the source by one symbol and an authentication tag of size. The impact of the authentication tag size is so significant that it is not necessary to include the one symbol for decoding purposes in the goodput characterization [1]. The symbol included with the source packet by source is used to identify the source or who is the origin of the message.

IV. MODULES

I have implemented this scheme by using Microsoft visual Studio 2008(.NET) and developed the different modules. Following are the modules used in my wok:

A. Client
B. Server
C. Routers
D. Hacker

A. Client:

1. Client sends the request to the server(Enter the username and password to login)
2. Connect to the server.
3. Select a file to transfer.
4. Send the data to server via intermediate devices (routers)
5. Close the connection.

Client module is work as a sender, and it send the file to the server. When client wants to send the file, he has to log in in the system by entering username and password. This request is send to server, server checks the parameters and authenticate client for sending the file. When client select the file for transmission then one key is generated for entire file and this key is integrated with the file and also this key is broadcasted over the network to every intermediate devices and to server i.e. receiver.

B. Server:

1. Client will ask the request to server for connection
2. At that time server will give the response to the client by checking username and password.
3. In server we have to select a location for receiving a file.
4. Finally Server will be receiving data from client.

Server module is work as a receiver; it receives the file from the client. When client sends request for login, by checking parameters server authenticates and permits for data transmission. Also server module performs the supervisory role in the authentication system and provides security to user file. Server verifies the file by comparing the authentication tag added with the file and the key distributed by the sender.

C. Router:

1. It is an intermediate device between the Server and Client.
2. When any router is hacked then the packets which are transforming from sender to receiver are transferred from the remaining routers by skipping that particular hacked router.
3. Otherwise router forwards the incoming packet to the next node by checking their authentication.

D. Hacker:

Using this module we get control over the intermediate device (router) that means the router will be in control of the hacker. He will get all control l over the data which is flowing through that router.

V. CONCLUSION

The approach that we proposed in this paper can be applied in any coding-based network systems. In particular, our approach does not require the cryptographic functions to perform the cryptanalysis and need not require additional information to the encoded packets. Only the sender node needs to generate an authentication tag for a file and this key is broadcasted in the network and used for computations in data transmission to identify the malicious packets. Thus in this way the pollution is removed from the network and data is transferred securely. For this reason, we believe that our approach is particularly suitable for secure data transmission in the coding based network to avoid the pollution attacks.

In this paper, we have proposed an unconditionally secure authentication scheme that provides network coding scheme with message integrity protection and source authentication. It offers protection against pollution attacks by providing authority to verify the authentication tags of the packets received, despite being unable to decode the data packets, and thus to detect and discard the malicious packets that fail the verification.

VI. FUTURE WORK

To verify every packet at intermediate device is quite time consuming, this can be reduced by implemented new schemes for verification. Future work will involve the optimization of the constraints involved in the authentication scheme for a more efficient solution. Another aspect to consider in the future is to reduce the workload of the sender, as in the proposed scheme sender has to perform some additional task of key generation and distribution.

REFERENCES

[1] Frédérique Oggier and Hanane Fathi An Authentication Code Against Pollution Attacks in Network Coding, IEEE/ACM Transaction on Networking 2011

[2] C. Gkantsidis and P. Rodriguez, Cooperative security for network coding file distribution, in Proc. IEEE INFOCOM, 2006, pp. 1–13.

[3] 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.

[4] 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.

[5] S. Agrawal and D. Boneh, Homomorphic MACs: MAC-based integrity for network coding, in Proc. Appl. Cryptography Netw. Security, 2009, pp. 292–305.

[6] T. Ho, B. Leong, R. Ko¨ tter, M. Medard, M. Effros, and D. Karger, Byzantine Modification Detection in Multicast Networks Using Randomized Network Coding, Proc. 2004 IEEE Int'l Symp. Information Theory (ISIT), Jun. 2004.

[7] Langberg, Michael and Sprintson, Alexander and Bruck, Jehoshua The encoding complexity of network coding 4-9 September, 2005. IEEE , Piscataway

[8] Y. Desmedt, 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] D. Boneh, D. Freeman, J. Katz, and B. Waters, Signing a Linear Subspace: Signature Schemes for Network Coding. Springer, Mar. 2009.