An Efficient Defence Approach For Improving Network Coding Architectures Against Pollution Attack In Wireless Network

Dr.T. Ganesan [1], Ms.S.Praveena [2]
[1]Professor Dept of Computer Science and Engineering
[2]Dept of Computer Science and Engineering
[1, 2] E.G.S.Pillay Engineering College(Autonomous), Nagapattinam ,Tamilnadu,India.

Abstract- *Network coding is a way for achieving channel capacity in networks. 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 pollution attacks against network coding systems in wireless network. we demonstrate that previous solutions are impractical in wireless networks, incurring an unacceptable high degradation of throughput. propose a recombination scheme where nodes draw packets to be recombined according to their age in the input queue, paired with a decoding scheme able to detect the reception of polluted packets early in the decoding process and short generations. the effectiveness of our approach is experimentally evaluated in a real system we developed and deployed on hundreds to thousands peers .the proposed schemes rely on techniques such as checksum block cipher. these schemes have high computational overhead, a seach verification requires a large number of modular exponentiations. in addition, they require the verification information to be transmitted separately and reliably to all nodes in advance; this is difficult to achieve efficiently in wireless networks.*

Keywords- Malicious packets, recombination, checksum block cipher,pollution attacks.

I. INTRODUCTION

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[1][2]. 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.[7] 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. To check this scheme we have used a hacker module.

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[4].
Most pollution detection and avoidance schemes rely on a two pillars approach: pollution detection and malicious nodes isolation. First, honest nodes must be able to understand if there is an ongoing pollution attack[6]. Because the nodes exchange coded packets, waiting to recover the original content to detect a pollution attack involves a delay during which the pollution may have already spread beyond recovery. Second, honest nodes must (cooperatively) identify the malicious nodes and isolate them from the network, e.g. via blacklisting. However, discovery of a pollution attack and in particular the identification of the malicious nodes are challenging problems which require the allocation of substantial computational and network resources. For this

reason, pollution avoidance mechanisms that enable the nodes to early detect an ongoing pollution attack and react with minimum computational and communication efforts are sought.

Wireless mesh networks are a promising technology for providing economical communitywide wireless access. Typically, a wireless mesh network consists of a set of stationary wireless routers that communicate via multi-hop wireless links. The broadcast nature of the wireless medium and the need for high throughput protocols make wireless mesh networks a prime environment for protocols based on network coding[9][10]. As a result, many such systems have been developed. However, as recently, the wireless environment makes the threat of pollution attacks particularly severe, since in wireless networks packets can be easily injected and bogus nodes can be easily deployed. Even when authentication mechanisms are used, such networks are vulnerable to insider attacks because wireless devices can be compromised and controlled by an adversary due to their increased susceptibility to theft and software vulnerabilities.
Designed to control the decoding complexity of NC, i.e. the number of operations a node must perform to recover a generation, by constraining the coding operations at the source and at the network nodes to a subset of the original blocks or received packets which are drawn for recombination. We show in this work that BC can be turned into an effective countermeasure to pollution attacks as well, by exploiting the packet decoding mechanism to spot the presence of polluted packets in the nodes input buffer prior to whole generation recovery; this early detection mechanism allows nodes to coordinate and take proper actions against the ongoing attack; adaptively (after pollution detection) modifying the coding scheme so to minimize the likelihood that any of the polluted packets is drawn for recombination.

The main contribution is a novel packet recombination strategy where the nodes draw the packets to recombine among those in the input buffers with a probability that grows with the age of the packet in the buffer. Our recombination scheme dramatically reduces the probability that an honest node transmits a polluted packet, which is further lowered by dividing the media stream in short generation[6]s. By comparison, in traditional NC every packets are drawn for recombination with identical probability and the media stream is subdivided in long generation to maximize the code efficiency. To put up with the somewhat lower code efficiency of our recombination policy, we propose a simple heuristic which restores the code efficiency to almost pre-attack levels and improves the overall network utilization efficiency.

II. RELATED WORK

The scheme based on[1] [2] 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 pree stablished 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 is[8][3] [9] uses a standard signature scheme that based upon the hardness of discrete alogarithm 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 keysfor every file.

III. PROPOSED SYSTEM

To verify every packet at intermediate device is quite time consuming, this can be reduced by implemented new schemes for verification. Another aspect to consider in the work is to reduce the work load of the sender, as in the proposed scheme sender has to perform some additional task of key generation and distribution.

The proposed schemes rely on techniques such as checksum block cipher. These schemes have high computational overhead, as each verification requires a large number of modular exponentiations. In addition, they require the verification information to be transmitted separately and reliably to all nodes in advance; this is difficult to achieve efficiently in wireless networks.

The original homomorphic encryption scheme is inefficient, because it encrypts plaintexts per a char or an integer, and it decrypts once for each cipher text. To improve the performance, we propose a model to encrypt plaintexts once a block and to decrypt cipher text once a block. The previous homomorphic encryption schemes are lack of data integrity. And, it is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

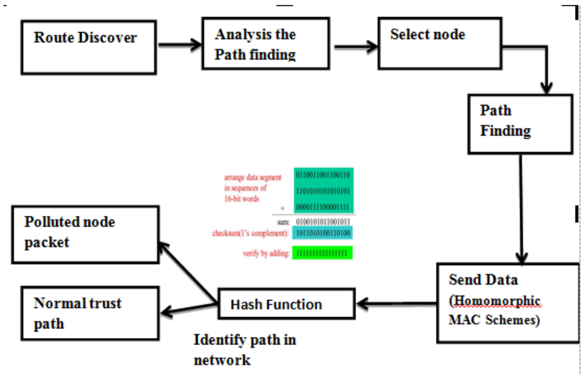
Route Discover
Analysis the Path finding
Select node
Path Finding
arrange data segment in sequences of 16-bit words
0110011001100110
1101010101010101
+ 0000111100001111
sum: 0100101011001011
checksum(1's complement): 1011010100110100
verify by adding: 1111111111111111
Polluted node packet
Normal trust path
Hash Function
Send Data (Homomorphic MAC Schemes)
Identify path in network

Fig:pollution Packet Identify Using Homomorphic Mac Schemes

Checksum Block Cipher

A mode of operation is an algorithm that uses a block cipher to provide an information service such as confidentiality or authenticity in cryptography. In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called a block, with an unvarying transformation that is specified by a symmetric key. Block ciphers operate as important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data.A block cipher by itself is only suitable for the ciphering purpose. Cipher Block Chaining has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential and that the message must be padded to a multiple of the cipher block size. One way to handle this issue is tackled through the method known as cipher text stealing.

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.

Homomorphic MAC Schemes

MAC is used for expanding spaces and are called Space MAC. This is allowed a node to verify the received packets. MAC algorithms are sometimes called as HASH keypad function. MAC's output's are sometimes called as tag. MACs differ from digital signatures. The term Message Integrity Code (MIC) is frequently substituted for the term MAC.

MAC algorithms can be constructed from other cryptographic primitives, such as However many of the fastest MAC algorithms such as UMAC and VMAC are constructed based on universal hashing.

Homomorphic Schemes

Homomorphic Functions can be used with Network Coding to verify the blocks are received at each Single system

HASH Functions

The mechanisms implementing homomorphic hashes or homomorphic signatures are computationally expensive. The mechanisms that implements message authentication codes (MACs) are also suffering from some problems like large number of colluding peers, works on fixed acyclic graph networks.

Definition 1: Hash function H is one-way if, for random key k and an n-bit string w, it is hard for the attacker presented with k,w to find x so that Hk(x) = w.

Definition 2: Hash function H is second-preimage resistant if it is hard for the attacker presented with a random key k and random string x to find y 6= x so that Hk(x) = Hk(y).

Definition 3: Hash function H is collision resistant if it is hard for the attacker presented with a random key k to find x and y 6= x so that Hk(x) = Hk(y) .

pollution attack is a common attack that is seen in all Hash functions. A hash function is used to cut the actual string into specific length. Hash function is used to provide data integrity and to make a digital signing more efficient.

IV. CONCLUSION

Our proposed schemes have high computational overhead, as each verification requires a large number of modular exponentiations. Proposed work will involve the optimization of the constraints involved in the authentication scheme for a more efficient solution. We use Block cipher to provide an information service such as confidentiality or authenticity in cryptography.

REFERENCES

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

[2] 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.

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

[4] A. Fiandrotti, V. Bioglio, M. Grangetto, E. Magli, and R. Gaeta “Band codes: Complexity adaptive network coding for p2p video streaming,” in Multimedia and Expo (ICME), 2012 IEEE International Conference on. IEEE, July 2012.

[5] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding.In Public-Key Cryptography | PKC '09, volume 5443 of LNCS, pages 68{87.Springer, 2009.

[6] Y. Li and J.C.S. Lui, “Stochastic analysis of a randomized detection algorithm for pollution attack in P2P live streaming systems,” Performance Evaluation, vol. 67, no. 11, pp. 1273 – 1288, 2010.

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

[8] D. Charles, K. Jain, and K. Lauter. Signatures for network coding.In 40th Annual Conference on Information Sciences and Systems (CISS '06), 2006.

[9] M. N. Krohn, M. J. Freedman, and D. Mazieres, “On-thefly verification of rateless erasure codes for efficient content distribution,” Security and Privacy, IEEE Symposium on, 2004.

[10] C. Gkantsidis and P. Rodriguez, “Cooperative security for network coding file distribution,” in IEEE INFOCOM, 2006.