Optimal Path Finding using Homomorphic Encryption Schemes in Computer Networks

Levent Ertaul\textsuperscript{a} and Vaideli\textsuperscript{b}

\textsuperscript{a}Department of Mathematics and Computer Science California State University, East Bay
Hayward, CA, USA. levent.ertaul@csueastbay.edu

\textsuperscript{b}Department of Mathematics and Computer Science California State University, East Bay
Hayward, CA, USA. vaidehikedlaya@gmail.com

In this paper we find a secure routing protocol for computer networks, which finds minimum optimum path using homomorphic encryption schemes. We briefly look into the existing homomorphic encryption algorithms. We make use of ElGamal encryption, Elliptic Curve encryption and a privacy homomorphism, which exhibits the property of homomorphism in our new routing protocol. Elliptic curve exhibits the property of additive homomorphism and is computationally faster than ElGamal and RSA. However, the privacy homomorphism using mod operation is computationally much faster than both ElGamal and Elliptic Curve. Using the homomorphic property of these encryption algorithms, we propose three new protocols, which are ElGamal, Elliptic Curve and Privacy Homomorphism to find the minimum optimal path securely. These protocols provide confidentiality.

Keywords: ElGamal Encryption, Elliptic Curve Encryption, Privacy Homomorphism, Determining minimum optimal path.

1. INTRODUCTION

The routing algorithm decides which line the packet should be transmitted to. In a wireless environment the route keeps on changing, so we should dynamically select the route to transmit the packet. Using homomorphic encryption scheme we can securely find a minimum path in these networks.

Homomorphic \cite{1}, \cite{2}, \cite{3} encryption scheme can be implemented in routing protocols to enhance security. Using homomorphic encryption, operations can be performed by the intermediate nodes on the ciphertext as if performed on the plaintext without actually knowing the plaintext \cite{1} \cite{2} \cite{3}. This enhances security of the protocol as the intermediate nodes if malicious cannot determine the plaintext. Homomorphism allows operation to be performed on the encrypted data (ciphertext) as if the operation is performed on the plaintext. Homomorphism has the property of additive, multiplicative and mixed multiplicative \cite{1}.

In additive homomorphism, decrypting the sum of two ciphertext is same as addition of two plaintext, represented as $E(x+y) = E(x) + E(y)$. In multiplicative homomorphism, decrypting the product of two ciphertext is same as multiplication of the two plaintexts. Multiplicative homomorphism is mathematically represented as $E(x*y) = E(x)*E(y)$. In mixed multiplicative homomorphism, decrypting the product of one ciphertext and plaintext is same as multiplication of two plaintext, represented as $E(x*y) = E(x) * y$.

In this paper we briefly describe the encryption schemes having the property of homomorphism. We then aim to find the minimum optimal path by using ElGamal, Elliptic Curve and Privacy Homomorphism encryption schemes. The paper is organized as follows. In section 2, we briefly describe the overview of homomorphic encryption algorithms.
To find the minimum of two paths 1-2-3 and 1-3, at node 1 we add the two encrypted paths to get the resultant path,
\[ e(1 - 2 - 3) + e(1 - 3) = E(0) E(0) E(z) E(z) E(z), E(z) E(z), E(z) E(z), E(z) E(z), E(z) E(z). \]

By decrypting the 12th and 11th element together, . . . 4th and 3rd element together, we get \( D(E(x)) \neq 0 \) and by decrypting the 2nd and 1st element together we get \( D(E(z)) = 0 \).

So the minimum weight is 1.

To find the optimal path between 1-3 and 1-2-3, we decrypt 1-3 and 1-2-3 at the 3rd and 4th position together and the path, which decrypts to a value \( z \neq 0 \) is the optimal path. We find that path 1-2-3 decrypts to a value \( z \neq 0 \). Hence, path 1-2-3 is the optimal path.

We know that the path 1-2-3 has the weight 1. To combine two paths 0-1 and 1-2-3 to get 0-1-2-3, we shift the encrypted path 0-1 to the right by 1 in pairs of \( S \).

The minimum of the two paths can be found without decrypting the entire resultant path. The minimum of the two paths can be found by decrypting the two paths at the minimum weight +1 position, thus reducing the computational power by not decrypting the entire path. These proposed protocols provide confidentiality as the minimum path is found securely. Using ElGamal and Elliptic Curve encryption schemes, confidentiality is achieved, as the intermediate nodes can neither determine the encrypted weight of the other nodes nor the minimum optimal path. The minimum optimal path is chosen by the source. An intruder can neither determine the encrypted weights nor the minimum optimal path without the knowledge of ElGamal or Elliptic Curve secret keys of every node. Using privacy homomorphism, confidentiality is also achieved, as an intruder cannot determine the weight or

5. CONCLUSIONS

In this paper we have shown that a minimum optimal path can be found securely to route the packets in computer networks by using homomorphic encryption schemes. Using these homomorphic encryption schemes, minimum weight of the two paths can be found without actually decrypting the entire resultant path. The minimum of the two paths can be found by decrypting the two paths at the minimum weight +1 position, thus reducing the computational power by not decrypting the entire path. These proposed protocols provide confidentiality as the minimum path is found securely. Using ElGamal and Elliptic Curve encryption schemes, confidentiality is achieved, as the intermediate nodes can neither determine the encrypted weight of the other nodes nor the minimum optimal path. The minimum optimal path is chosen by the source. An intruder can neither determine the encrypted weights nor the minimum optimal path without the knowledge of ElGamal or Elliptic Curve secret keys of every node. Using privacy homomorphism, confidentiality is also achieved, as an intruder cannot determine the weight or
Levent Ertaul and Vaidehi

the optimal path without the knowledge of the secret key.

In the future, implementation problems of these newly proposed protocols will be addressed and performance comparison of these schemes will be given.

REFERENCES


