ATLANTIS PRESS

Advances in Engineering Research, volume 166

3rd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2018)

An Improved Anonymous Communication Forwarding Strategy

Jie Ling[a], Daxiang Zheng[b,*]

Faculty of Computer, Guangdong University of Technology, Guangzhou 510000, China;
[a] 1150181103@qq.com, [b] zdxfire@foxmail.com

Abstract: Tor is one of the most widely used anonymous communication systems and has been studied by many researchers in recently years. Aiming at the disadvantages of the entry node and exit node of Tor anonymous communication circuit, this paper proposed a pseudo sender and pseudo receiver forwarding strategy in Tor circuit. This strategy can prevent the entry node and exit node from directly contacting the sender and receiver which is securer than original forwarding strategy. In the strategy, there are two random forwarding circuits connecting to Tor circuit, and the nodes that make up the forwarding circuit formed a group which can effectively conceal the information of sender and receiver. What's more, there is a pseudo sender/receiver node in each random forwarding circuit which can hide the information of both parties in the circuit. Users can controls the length of the anonymous transmission circuit by the controlled variables to meet the anonymous needs of different users in the strategy.

Keywords: Anonymous Communication, Forwarding Strategy, Tor, Crowds, Message Encapsulation.

1. Introduction

Anonymous communication means to conceal the communication relationship in the service flow by a certain method, so that eavesdropper cannot directly obtain or infer the communication relationship or the information of both sides of the communication. According to the difference of hidden information, the anonymous protection can be divided into three forms [1]: sender anonymity, recipient anonymity and the uncorrelated of sender and recipient. There are four key technologies for hidden information in anonymous communication which are rerouting mechanism, broadcast/multicast mechanism, traffic padding and encryption technique.

Rerouting mechanism is an application layer routing mechanism. It provides users with indirect communication, which contains multiple hosts to store and forward data, to form a virtual path with multiple security channel. The hacker can not obtain IP address of the sender and recipient in this virtual path, so that the identity information of the communication entity is effectively hidden. There are some anonymous communication systems based on rerouting mechanism in various anonymous communication situations. Mixes [3] hide the identity of the email sender. Tor [4] hides the communication relationship between communication entities in the real-time communication. Crowds [5] protect user's identity information from being exploited by Website. Hordes [6] adopt the multicast technique to quickly return message on the basis of Crowds. Tor is one of the most widely used anonymous communication systems, and has some drawbacks in the entry node and the exit node. We improve the forwarding strategy based on the weak security problem of these node directly contacting the sender and receiver.

2. Anonymous Communication Forwarding Strategies

Crowds system adopt the strategy of random forwarding, sender uses the threshold P_f ($0 \leqslant P_f \leqslant 1$) to control the forwarding probability of intermediate nodes. When a message arrives at a node, the node

generates a random number P ($0 \leqslant P \leqslant 1$) and compares it with P_f. If $P < P_f$, the node selects a node in the group as the next node and forwards the message to the selected node. Otherwise, the node forwards the message to the receiver. This strategy is simple and fast, and implements sender anonymity. However, the nodes in the forwarding path can obtain the identity of the recipient. In addition, the length of forwarding circuit established by the strategy may be too long, thereby increasing the transmission time.

Tor forwarding strategy is based on the triple-hop rerouting mechanism. The sender selects three nodes as a Tor anonymous transmission circuit and the messages are encrypted in the nodes order from back to front in the circuit. After the encrypted message arrives at the node in Tor circuit, the node decrypts the outermost layer of the encrypted message, obtains the next node address and forwards the decrypted message to it. Until the last node in the circuit is reached, the last node decrypts the message and obtains the recipient's address, and forwards the original message to the receiver. This strategy implements the unrelated of sender and recipient, but the connection between the exit node and the receiver isn't security, and the hacker can obtain the recipient's information and the data of the anonymous communication.

An anonymous forwarding system based on the hybrid rerouting mechanism is proposed in [7], which uses the random forwarding strategy of Hordes and the forwarding strategy of Tor to forward messages. The forwarding strategy enhances the sender anonymity by combining two types of forwarding strategies, and forwards the returned message to sender within the group through multicast which reduces the network overhead. The disadvantage is that the sender and receiver must be within the same anonymous group.

An anonymous communication system based on trusted computing is proposed in [8]. As shown in Fig.1, [8] proposes that there is a weak security problem in the entry node and exit node of Tor anonymous forwarding circuit. The entry node and the exit node directly communicate with the sender and receiver, which is vulnerable to eavesdropping and destroys the anonymity of the communication relationship. Therefore, it proposes the camouflaged sender forwarding strategy and broadcast strategy to conceal information of sender and recipient. By using the random forwarding strategy in the transmission of the camouflaged sender group, user can set the threshold and the maximum length of circuit to control the length of the forwarding circuit. The random forwarding of multiple trusted nodes constitutes a camouflaged sender group, which makes it impossible for the external node to predict which node in the group is communicating. Because the random forwarding strategy returns message according to the original circuit, the node in the circuit respectively get the identity information of the entry node and the sender from the forwarding and return message, thus exposing the sender anonymity. In the broadcast forwarding strategy, the recipient anonymity is implemented through broadcasting, however, this increases the bandwidth load of the receiver's broadcast domain, in severe case, this can cause network congestion.

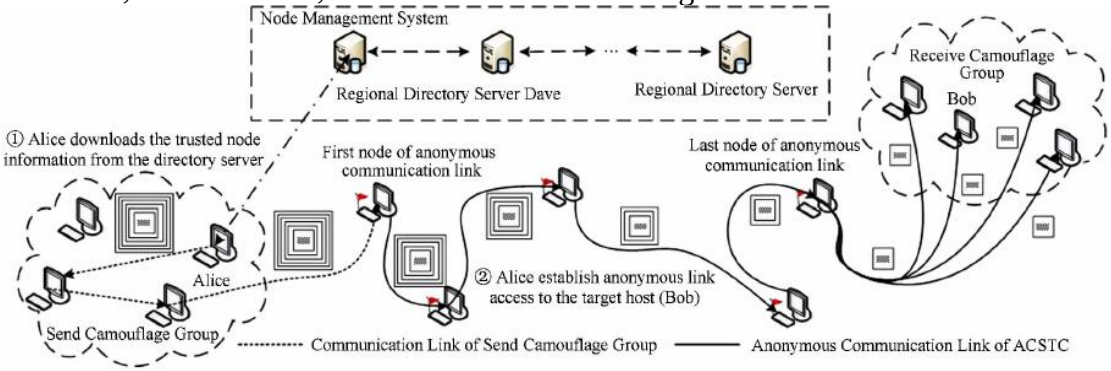

Fig. 1 The anonymous communication system based on trusted computing

3. The Improved Forwarding Strategy of this Article

For the security problem in [8], we improved the original forwarding strategy based on the pseudo receiver forwarding strategy in [9]. As shown in Fig.2, we proposes to add the pseudo sender and

pseudo receiver random forwarding circuits in the Tor forwarding circuit, in order to prevent the entry node and exit node from connecting directly to sender and receiver. In addition, we joins pseudo sender and pseudo receiver in circuit L_1 and L_2, which can avoid that the nodes in these circuits do not obtain the sender and receiver of the anonymous communication.

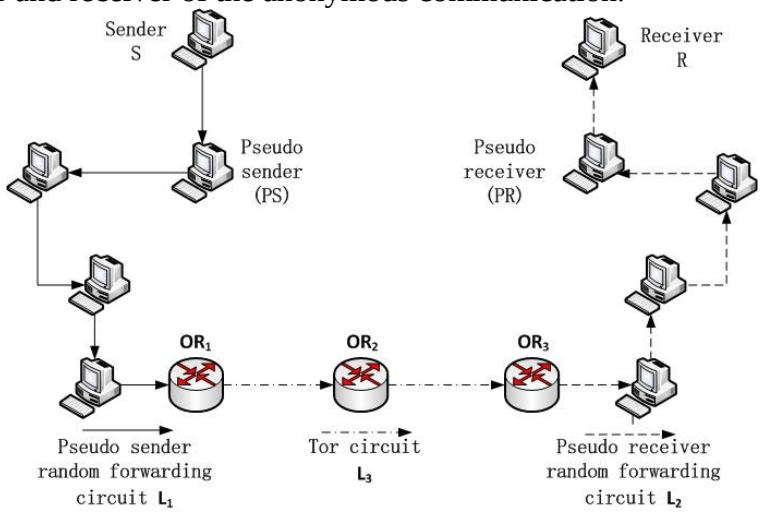

Fig. 2 Improved pseudo sender and pseudo receiver random forwarding circuits

3.1 Notations

The notations used in the paper as shown in Table 1.

Table 1 Notation

Notation	Description
P_{f1}	The threshold of the forwarding probability in circuit L_1
L_{max1}	The maximum length of circuit L_1
$E_{S\text{-}PS}\{\}$	The encrypted encapsulation by sender or pseudo sender
IP_R	IP address of receiver
Date	The information of the anonymous communications
$K_{(S,OR1)}$	The symmetric key generated by S and OR_1
P_1	The random constants of key agreement between S and OR_1
P_2	The random constants of key agreement between node PS and OR_1
r_S	The random number generated by sender
SK_S	The private key of sender

3.2 Pseudo Sender Forwarding Circuit

In circuit L_1, Sender (S) selects a node as a pseudo sender (PS) in the original sender camouflaged group. When establishing circuit L_3, the information of node OR_1 in L_3 which is determined by the onion agent, is forwarded to PS. PS exchanges the private keys with S and OR_1. After circuit L_3 has been established, S encrypts the transmitted information in the following encapsulation format.

$$E_{S\text{-}PS}\{IP_{OR1}||E_{S\text{-}OR1}\{IP_{OR2}||E_{S\text{-}OR2}\{IP_{OR3}||E_{S\text{-}OR3}\{IP_R||Data\}\}\}||P_{f1}||L_{max1}\} \quad (1)$$

When message arrives at PS, PS would decrypt its outermost layer to get the values of P_{f1} and L_{max1} required in the random forwarding strategy, and the message of Tor triple encapsulation. PS forwards the received message according to the algorithm 1.

Algorithm 1：Message encapsulation and random forwarding strategy in circuit L_1

Begin

1.Get the value of P_{f2} and L_{max2} form node S. If S does not assign them, $P_{f2}=1$ and $L_{max2}=1$; /*P_{f2} and L_{max2} are the controlled variables in circuit L_2*/

2.Data=$IP_R||Data||P_{f2}||L_{max2}$;

3.For $j=3$ To $j=1$

$Data=E_{S\text{-}ORj}\{Data\}||\ IP_{ORj}$;

End For /*the message encapsulation in circuit L_3*/

4.Get the value of P_{f1} and L_{max1} form S, if S do not assign them, $P_{f1}=1$ and $L_{max1}=1$; /*P_{f1} and L_{max1} are the controlled variables in circuit L_1*/
5.$Data=E_{S\text{-}PS}\{Data||P_{f1}||L_{max1}\}$;
6.The message arrived at PS. After PS decrypts the message, PS and other nodes forward the decrypted message.
Do
{ If($L_{max1}==1$)
Get rid of P_{f1} and L_{max1}, then forwards the message to OR_1;
Exit(*0*);
End If
P=flip(P_{f1}); /*Generating the probability of sending message in the node*/
If($P \geqslant P_{f1}$)
Get rid of P_{f1} and L_{max1}, then forwards the message to OR_1;
Exit(*0*);
Else
The node is randomly selected from the disguised member as the next node, and the message is forwarded to it;
$L_{max1}=L_{max1}-1$;
End If
} while($L_{max1} \geqslant 1$)
End

While the return message arrives at OR_1, the message is encrypted into a triple encrypted message. OR_1 encapsulates the message and forwards it to PS in circuit L_1, whose message format is as follow.

$$E_{OR1\text{-}PS}\{IP_S||E_{S\text{-}OR1}\{E_{S\text{-}OR2}\{E_{S\text{-}OR3}\{Data\}\}\}\} \quad (2)$$

The forwarding node in L_1 could only know that PS is communicating with OR_1, which can conceal the identity information of sender.

3.3 Pseudo Receiver Forwarding Circuit

In circuit L_3, the node OR_3 selects a trusted node as pseudo receiver (PR) in the receiver's broadcast domain of the original strategy. When the message arrives at OR_3, OR_3 obtains the IP address of the receiver, and exchanges the private keys with receiver (R) and PR. Then, OR_3 encrypts the transmitted information in the following encapsulation format.

$$IP_{PR}||E_{OR3\text{-}PR}\{IP_R||E_{OR3\text{-}R}\{Data\}\}||P_{f2}||L_{max2} \quad (3)$$

OR_3 forwards the message according to the algorithm 2. When the message arrived at PR, then the message is sent to R.

Algorithm 2：Message encapsulation and random forwarding strategy circuit L_2
Begin
1.$Data=IP_{PR}||E_{OR3\text{-}PR}\{IP_R||E_{OR3\text{-}R}\{Data\}\}||P_{f2}||L_{max2}$； /* the message encapsulation in circuit L_2*/
2.OR_3 and other nodes forward the message.
Do
{ If($L_{max2}==1$)
Get rid of P_{f2} and L_{max2}, then forwards the message to PR;
Exit(*0*);
End If
P=flip(P_{f2}); /* Generating the probability of sending message in the node */
If($P \geqslant P_{f2}$)
Get rid of P_{f2} and L_{max2}, then forwards the message to PR;
Exit(*0*);
Else
A node is randomly selected from the receiver's broadcast domain member as the next node, and the message is forwarded to it;

L_{max2}=L_{max2}-*1;*
End If
} while($L_{max2} \geqslant 1$)
3.PR decrypts the outermost layer of message and forwards the message to R;
End

When the receiver responds to the message, R exchanges private key with PR, then forwards the encrypted message to PR, whose message format is as follow.

$$E_{R\text{-}PR}\{IP_{OR3}||E_{OR3\text{-}R}\{Data\}\} \quad (4)$$

While the message arrives at OR_3, OR_3 forwards the message to S according to Tor forwarding strategy. The forwarding node in circuit L_2 could only know that the PR is communicating with OR_3, which can conceal the identity information of receiver.

4. Security Analysis and Conclusion

In [8], the Elliptic Curve Diffie-Hellman (ECDH) [10] was used for the key agreement. The security of circuit L_1 is analyzed with the sender, pseudo sender and entry node. The symmetric key generated by S and OR_1 is as follow.

$$K_{(S,OR1)}=P_1(r_S+SK_S)(r_{OR1}+SK_{OR1}) \quad (5)$$

The symmetric key generated by PR and OR_1 is as follow.

$$K_{(PS,OR1)}=P_2(r_{PS}+SK_{PS})(r_{OR1}+SK_{OR1}) \quad (6)$$

P_1 and P_2 are the constants in agreements, and the constants generated by different agreements are not equal. The random number and private key generated by different nodes are not equal. In that case, $K_{(S,OR1)} \neq K_{(PS,OR1)}$, and $K_{(PS,OR1)}$ cannot decrypt the message encrypted by $K_{(S,OR1)}$, so that it could avoid PS leaking the information of anonymous communication. By the same token, R, PS and OR_3 also use ECDH to generate the symmetric keys in circuit L_2, PR also cannot decrypt the encrypted message by the symmetric key generated by R and OR_3.

In circuit L_1, sender encapsulates the message according to encapsulation format 1. PS cannot obtain the receiver's information of the anonymous communication and is only responsible for forwarding the message to OR_1. For the other nodes in circuit L_1, they just know that OR_1 is the receiver of communication. When the returned message arrives in circuit L_1, OR_1 encrypts it according to encapsulation format 2. The encapsulated message is forwarded to PS by the intermediate node according to the forwarding circuit. If an eavesdropper exists in the circuit, it analyzes the forwarding message back and forth, which can be aware of the communication between PS and OR_1, so that it can conceal the identity information of sender. In addition, the nodes in circuit L_1 form the sender group, the external nodes can only know that a node in the sender group is communicating through Tor circuit, but can not know the identity information of the sender.

In circuit L_2, OR_3 encapsulates the message according to encapsulation format 3. Other nodes in the network can know that PR is the receiver of the communication, but they cannot decrypt the encrypted message. When receiver responds to the message, the recipient encapsulates the returned message according to encapsulation format 4. PR can only decrypt the outermost layer of message and forward the message to OR_3. Other nodes in circuit L_2 can be aware of the communication between PR and OR_3. In addition, the nodes in circuit L_2 form the receiver group, the external nodes can only know that a node in the receiver group is the receiver of anonymous communication, but can not lock which node is the receiver.

The improved forwarding strategy proposed in the paper implements that OR_1 and OR_3 communicate indirectly with the sender and recipient, and it is also against the middleman attack which can decrypt the message in the intermediary node of the circuit. Compared with [8], the improved forwarding strategy has the following advantage. We add two random forwarding circuit in Tor transmission, which can avoid the entry node and exit node direct connecting to both parties of anonymous communication when the message is forwarded back and forth. In the random forwarding circuits, we join the pseudo sender and pseudo receiver as the bridges connecting to Tor circuit,

which is considered as the sender and receiver of the anonymous communication by the intermediate forwarding nodes. What's more, the nodes in the random circuit form a group which can conceal the true sender and receiver. The circuit L_2 compares with the broadcasting circuit in [8], the bandwidth cost in random forwarding strategy is less than that in broadcasting transmission.

The improved forwarding strategy aims at the existing trusted nodes, and lacks of consideration for nonexistent trusted nodes. The future work will consider in the case of nonexistent trusted node implementation anonymity on both sides of the anonymous communication circuit.

5. Acknowledgments

This work is supported by the science and technology project of Guangdong Province (No.2015B010128014，2015B090906015，2015B090906016，2016B010107002) and the project of Guangzhou Science and Technology(No.201604016003).

6. References

[1] Pfitzmann, A., Köhntopp, M.: Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. In International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability, pp. 1-9 (2001).
[2] Wright M., Adler M., Levine, B.N.: An Analysis of the Degradation of Anonymous Protocols. In: DBLP (2002).
[3] Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. In: ACM , pp. 84-90 (1981).
[4] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Washington,DC: Navel Research Lab (2004).
[5] Rubin, A.D., Rubin, A.D.: Crowds: anonymity for Web transactions. In: ACM, pp. 62-92 (1998).
[6] Shields, C., Levine, B.N.: A protocol for anonymous communication over the Internet. In: DBLP, pp. 33-42 (2000).
[7] Zheng, G., Xue, Z.: A Mixed Anonymous System based on Tor. Information Security & Communications Privacy (12), 76-77, 80 (2011).
[8] Zhou, Y., Yang, Q., Yang, B., Wu, Z.: A Tor Anonymous Communication System with Security Enhancements. Journal of Computer Research and Development 51(7), 1538-1546 (2014).
[9] He, G., Chen, L., Zhang, T., Ma, Y.: Improved Anonymous Communication Protocol Base on Crowds. Journal of System Simulation 27(12), 3050-3056 (2015).
[10] Li, S.J., Zhang, C.H., Zhou, D.W.: An Authenticated Key Agreement Protocol Based on ECDH. Information Security & Communications Privacy (7), 70-72 (2011).