Load Balanced Onion Relay for Prevention of Traffic Analysis in Ad Hoc Networks

Sungchang Lee[1], Ha Young Yun[1], and Mi Lu[2]

[1] Hankuk Aviation University, Goyang, Korea
{sclee,hyyun}@mail.hangkong.ac.kr
[2] Texas A&M University, College Station, U.S.A.
mlu@ee.tamu.edu

Abstract. In this paper, an ad hoc network anonymous data forwarding method and an associated routing protocol to prevent traffic analysis is presented. This method assumes trusted closed group nodes and every node can play the role of onion relay for the anonymous data forwarding. The route discovery operation of the protocol adopts the load balancing concept. The load balancing not only improves the throughput but also helps the prevention of the traffic analysis since the load cost for camouflage traffic can be reduce and the routes change dynamically. The performance of the proposed protocol is evaluated by simulation, and compared in several major aspects with the fixed mix method for anonymous data forwarding that works over existing ad hoc routing protocol.

1 Introduction

Security problem in mobile ad hoc network is essential and important in many applications. However, the peculiar attributes and limitations of the ad hoc network even make it more difficult. There are numerous types of attacks on both routing and data forwarding in the network, some of them are specific to ad hoc network. The attacks on MANET (mobile ad hoc network) routing include black holes, denial of service, routing table overflow, impersonation, energy consummation, information disclosure [1]. Also, possible attacks against anonymity network are message coding attack, message length attack, replay attack, collusion attack, flooding attack, message volume attack, timing attack, profiling attack [2, 3]. There have been much work against these attacks, but it seems to be impossible to have a single protocol that can perfectly protect the ad hoc network from all kinds of attacks. In order to cover wide range of attacks, it may be inevitable to have a security framework in which separate security capabilities that fight for different attacks cooperate together. Thus, most of the literatures deal with only limited scope of the security problems.

This paper focuses on the prevention of traffic analysis attack. The scope of the paper covers the anonymous data forwarding and the cooperating routing protocol, but the security of the routing itself is excluded. For the security routing, the methods for anonymous route discovery and maintenance using symmetric or asymmetric keys proposed in other literatures [4, 5, 6] may be applied on the routing protocol proposed in this paper.

H.-K. Kahng and S. Goto (Eds.): ICOIN 2004, LNCS 3090, pp. 24–33, 2004.

Section 2 describes the basic assumptions and the rationales of the proposed method. The proposed load balancing routing and the anonymous data forwarding scheme are presented in section 3 and 4, respectively. The performance simulation results are shown and discussed in section 5, and section 6 concludes this paper.

2 Model of the Proposed Method

The proposed method assumes that the target ad hoc network consists of a finite number of closed member group, thus there is no severe scalability requirement. Also, a trusted environment is assumed, that is, all member nodes can be trusted, and the trust is continuously probed and maintained using some other methods (such as intrusion detection, key management) that is out of the scope in this paper. Since, the main focus is on the prevention of traffic analysis, it is assumed that camouflage traffic is generated by other module or, maybe, by the higher layer function.

As the mix methods [7, 8], fixed length packets with padding will be used for data packets to hide the correlation between the incoming and outgoing packets. However, routing control packet may be used in traffic analysis by the adversary in ad hoc network, especially in the on-demand routing protocols. Therefore, it will be desirable to use two different fixed lengths in ad hoc network, one for data forwarding and the other for the routing control packets since the routing control packets are usually short and the data packets may have wide range of lengths. In this case, two different length camouflage packets will be needed.

The proposed LBOR (load-balanced onion relay) method assumes that every node in the ad hoc network can be relay node for the anonymous data forwarding. The routing scheme adopts the load balancing concept. The rationales behind this are

- An ad hoc network consists of peer nodes, thus the assumption of the existence of mix (or relay) nodes may not be relevant in situations. Also, the collecting and shuffling of packets as in the wire network mixes [7, 8] may not be appropriate for ad hoc network applications due to delay, processing overhead and buffer requirement. Rather, simpler scheme with camouflage traffic may be needed.
- Unlike the wired network, there is no high capacity back bone network in ad hoc network, where mixes are located. Instead, all ad hoc network links have the same, usually, limited bandwidth, even around the mix nodes. As a result, links around the mix nodes becomes bottleneck, causing the degradation of network throughput, delay and packet loss that may be unacceptable for the real-time applications.
- Data forwarding through few mix nodes may cause low reachability (or delivery ratio) due to the bottleneck as mentioned above, or topological problems like hop distance, which is very important for military, emergency applications.

- Load balancing not only reduces the possible bottleneck due to the limited bandwidth, but also lowers the required amount of camouflage traffic to achieve the neural traffic matrix [9, 10] that is pursued to prevent traffic analysis.
- Relay nodes for anonymity data forwarding can be selected randomly and dynamically. This helps the reduction of hops by avoiding detours, and makes it untraceable.

A number of network mix methods [11, 12, 13] provides data forwarding anonymity assuming separate routing protocols that operate below them. Load balancing concept of the proposed LBOR requires the cooperation of routing and data forwarding protocol, thus it covers both routing and data forwarding.

The route discovery and maintenance of LBOR is based on DSR protocol, but with modifications as described in next section. The modification mainly includes the adoption of load balancing routing. The anonymous data forwarding part of LBOR utilizes the well-known onion routing method, but any node in the network can be relay node for the onion routing. Thus, the route from the source node to the destination node is selected based on the load balancing routing, and the nodes that will works as onion routing relays are chosen by the source among the nodes that are en route.

3 Load Balancing Routing

In this section, the routing operation of LBOR is described. As mentioned in the previous section, the main idea of LBOR is load balancing concept. The effect of load balancing on the prevention of traffic analysis is discussed, and the load balancing routing operation is described.

3.1 Load Balancing and Prevention of Traffic Analysis

Mix methods applied in ad hoc networks have been proposed in [13]. In their methods, there are a finite number of mix nodes in the ad hoc network. Every source node has its own designated mix node (fixed mix method) or selects a mix node dynamically (dynamic mix method). In these methods, the mix nodes are well-known even to the adversary, which may be irrelevant in such as military applications. In addition, the link bandwidth of ad hoc networks is limited, and the links around the mix nodes becomes bottleneck. In this paper, it is assumed that any node can play the role of onion relay node. This model makes it possible to eliminate the vulnerable mix nodes and balance the traffic across the network.

The ad hoc network applications are more likely to be time-critical real-time applications. Also, the amount of network traffic is much smaller than the wired network. Thus, the function of collecting and shuffling of packets as in the wired network mix is not appropriate in ad hoc network. Instead, camouflage traffic will be inevitable to prevent traffic analysis. However, ad hoc network has limited bandwidth, thus the load balancing is important.

The proposed method focuses on the prevention of the traffic analysis. The method assumes that the higher layer generates dummy (or camouflage) packets to prevent the eavesdropper from gaining useful information from the traffic pattern. For this end, the camouflage traffic is generated by so that the load on all links may be equal, achieving so called neural traffic matrix [9]. In the paper, the minimum load cost (MLC) to achieve the neural traffic matrix is defined as [9]

$$MLC = n\,(n-1)\,\mu - S \tag{1}$$

where,

$$S = \sum_{i=1}^{n} \sum_{j=1}^{n} M\,[i,j] \tag{2}$$

and

$$\mu = \frac{\max\{\sum_{i=1}^{n} M\,[i,j]\,, \sum_{i=1}^{n} M\,[j,i]\,|j = 1,2,...,n\}}{n-1} \tag{3}$$

In the equation, n is the number of nodes in the network, and $M[i,j]$ is the traffic matrix.

According to this proposition, the maximum of link traffic into or out of the nodes in the network should be as low as possible to minimize MLC. The routing protocol of the proposed method tries to find routes so that the traffic on the links may be balanced to minimize load cost of using dummy packets.

3.2 Routing Operation

The proposed routing protocol is based on DSR (Dynamic Source Routing) protocol but with following modifications.

- Every node continuously updates LL (link load) of each link that is alive. LL is defined as

  LL = number of all packets on the link / measurement window (packets/sec)

- If no packet arrives for LEDI (link entry delete Interval), the item is deleted from the LL list. Measurement window (MW) is a sliding time window, and LL is measured for each direction of a link separately.
- Upon receiving RREQ, each node on the route appends the LL of the corresponding link to RREQ before it broadcasts RREQ. RREQ contains the list of the nodes and LLs of the links it travels.
- Upon receiving RREP, each node on the route updates the route cash with the following criteria.
  1. If the node does not have the same route to the destination, then add the new route entry.
  2. If the cash has route(s) to the destination, add new route and sort.
  3. The priorities for the sorting of the route entries are, in order:

(a) bottleneck load (BL) = max{LL_i} of the route,
(b) total route load (TRL) = the sum of LL_i's,
(c) hop count,

4. Each node keeps only top n_entries entries for each destination.

– If any destination is not referred for routing for CEDI (cash entry delete interval), the entries are deleted from the cash.
– Cash entry is updated every CEUI (cash entry update interval) for each destination alive in the cash.
– Every time an entry is referenced, the BL, TRL, are updated as follows, and entries are sorted again.

$$BL^{+} = BL + \lfloor \frac{n\_hop}{2} \rfloor, \quad TRL^{+} = TRL + \lfloor \frac{n\_hop}{2} \rfloor$$

Other operations are just like DSR. This routing scheme focuses on the load balance of the network links to minimize the load cost for the camouflage traffic. Specifically, the route is chosen so that the bottlenecks of the network can be prevented in advance. This scheme not only improves the throughput of the network, but also reduces the required camouflage traffic.

4 Anonymous Data Forwarding

In this section, the proposed method to anonymize the network traffic is described. For fixed networks, many solutions for untraceable communication have been proposed to keep confidential who communicates with whom. Most of them are based on Chaum's[8] method. In such solutions, special network node(s) (called mix) is(are) used to provide unlinkability between the source and the destination. However, mix method has restricted application since it need to collect sufficient number of (a batch of) packets to shuffle the order randomly before it send out a batch of packets. It may cause intolerable delay or camouflage traffic. Also, the mix needs high processing power, and if the link capacity around the mix(s) is limited, the traffic bottleneck degrades the performance of the network significantly. These aspects make the mix method infeasible for Ad Hoc network.

The dummy traffic to make network traffic even to prevent the adversary to deduce useful information from the traffic pattern may congest the limited bandwidth of the ad hoc network. In order to circumvent some of the drawback of mix method, NMD was proposed for mobile IP network, but ad hoc network has additional constraints of the limited bandwidth, the morphosis of the network topology itself, and the limited processing power of the nodes. In this section, how to provide the unlinkability of the traffic that is adopted in the proposed method is described.

A number of protocols for anonymity have been proposed based on the Chaum's untraceable electronic email solution [8]. The basic data forwarding of LBOR is also based on onion routing [12, 14]. The public keys of all nodes are known to the network members. When a node is to send a packet, the source selects the route according to the routing information. With the selected route, the source determines the number of ad hoc onion relay nodes (ORNs) as following.

Step 1: Select the route to the destination according to the routing cash. (n_hop : the number of hops to destination)

Step 2: Decide the number of ORNs (n_ORN) along the route between the source and destination as follows.

$$n\_ORN = \max(1, \lceil n\_hop/\alpha \rceil) \tag{4}$$

where, α is sparseness of ORNs along the route. $\alpha = 1$ means that all node en route to the destination are onion relay nodes.

Step 3: Select randomly n_ORN nodes along the route.

$$S_R = \{R_i |\ i = random(1,\ n\_hop)\}, \quad where \quad |S_r| = n\_ORN \tag{5}$$

Once the ORNs along the route to the destination are determined, the packet goes through a sequence of $ORNs\{ORN_1,\ ORN_2, ...,\ ORN_{n\_ORN}\}$. The onion sent by the source is

$$K_1(ORN_2, R_2, K_2(ORN_3, R_3, K_3(\cdots K_n(D, R_n, K_D(M, R_0))\cdots)))$$

where, K_i 's are public keys, and M is the message sent from the source to the destination. If the processing overhead of public key cryptosystem is not acceptable, the symmetric key cryptosystem can be used instead.

5 Performance Evaluations

To evaluate the performance of the proposed routing protocol in several aspects, the simulation of the proposed protocol and fixed mix method is implemented using *ns*-2 [15]. The ad hoc network consists of 40 wireless nodes moving in 675m x 675m space with mobility model of random waypoint [16]. The moving speed has a uniform distribution between 0m/s and 20m/s. The nodes are initially paced randomly in the space, and the radio bandwidth is 2Mb/s. The range of the transmission power is 250m. The simulation is done for several different pause times as indicated in the figures. The simulation time is 900s excluding 100s initial warm up time. 15 pairs of source and destination are randomly chosen and the connections are set up. The sources are constant bit rate (CBR) sources, and send 3 data packets of 512 bytes every second. The source nodes begin the transmission starting at random time between 0 to 8 second. All simulation results are obtained by averaging 5 different simulations with different seeds. The parameters for routing operation are MW=LEDI=2 seconds, n_entries=3, CEDI=7.5 seconds, CEUI=45 seconds.

To compare the performance, fixed mix (FM) method is also simulated. In the fixed mix method, every node has its designated mix node among a finite number of ad hoc network mix nodes. We assume that the fixed mix method operates over DSR (Dynamic Source Routing) protocol, and there are 6 mix nodes among 40 nodes including the mix nodes. Other environments are the same as the above.

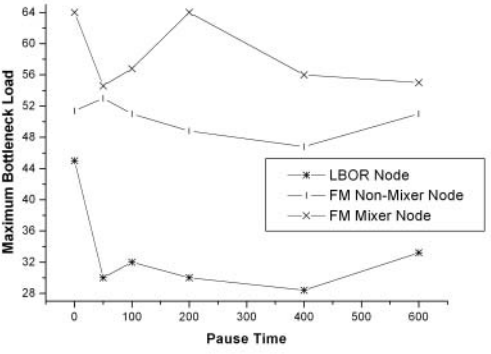

Fig. 1. The bottleneck load is the load of the link of which the load is the maximum in the network in a given measurement window. The maximum bottleneck load is the highest one throughout the simulation

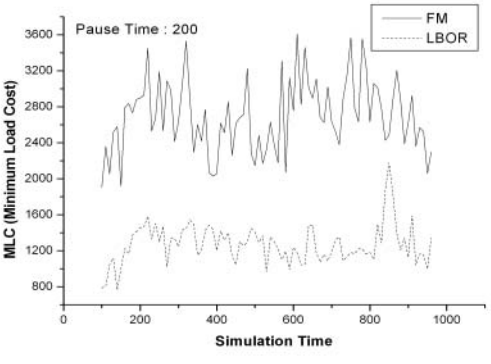

Fig. 2. The comparison of the minimum load cost of fixed mix method and LBOR is shown

In Fig. 1, the maximum bottleneck loads (MBLs) of two methods are compared. The bottleneck load (BL) is defined as the load of the link of which the load is the maximum in the network in a measurement interval. MBL is the maximum of BLs throughout the simulation. As expected the links of mix node and links around mix nodes are crowded by heavy load, and this phenomenon becomes severe as the traffic increases.

In Fig. 2, MLC (minimum load cost defined in section 3.1) to achieve neutral traffic matrix is shown. Due to the load balancing routing, it is shown that required MLC for LBOR is remarkably lower than that of fixed mix method. Similar MLC comparison results were obtained for different pause times by simulation.

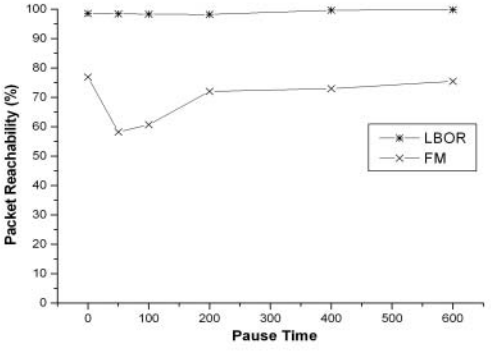

Fig. 3. The successful packet delivery ratio

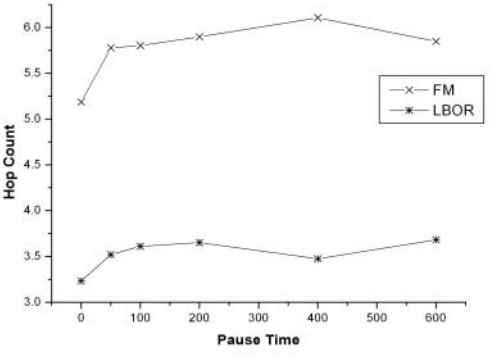

Fig. 4. Average hop count from the source to the destination

Military and emergency applications are the examples of the important applications of ad hoc network. In such circumstances, the successful packet delivery ratio is very important. In Fig. 3, the successful packet delivery ratios of the two methods are compared. The successful packet delivery ratio is defined as the ratio of the number of successfully delivered packets to the number of the total generated packets by the sources.

In the case of fixed mix method, the detour to go through a mix node causes the increase of the hop count between the source and the destination. On the other hand, LBOR does not choose the optimal route in terms of hop count, but it tries to choose the best route by avoiding bottleneck link. Even so, Fig. 4 shows that the average hop count of LBOR is much smaller than that of fixed mix method.

In Fig. 5, the ratio of the number of the routing control packets sent to the

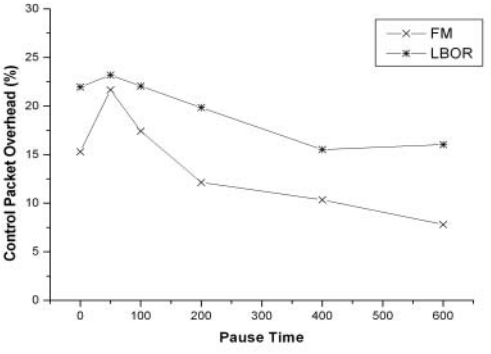

Fig. 5. Control packet overhead

number of total packets sent is shown. LBOR shows better successful packet delivery ratio, but the routing control packet overhead is slightly higher than the fixed mix method over DSR. This overhead implies the efficiency of the combined routing and data forwarding protocol.

6 Conclusion

The prevention of traffic analysis is an important part of network security. In this paper, we presented an anonymous data forwarding method accompanied by an associated routing protocol. The method assumes the nodes to be a trusted group and all nodes can take the role of onion relay node. The routing protocol is based on well-known DSR, but the load balancing concept is adopted and some operations are modified to help data anonymity and to improve other performances. The simulation results show the improved performance of the proposed method compared to the fixed mix method. The load balancing routing efficiently avoids bottleneck links in the network, which not only improves the throughput and delay but also reduces the amount of required camouflage traffic to prevent traffic analysis. Also, the packet delivery ratio is shown to be improved remarkably, which is important in ad hoc network applications.

References

[1] H. Deng, Wei Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, pp. 70-75, October 2002. 24

[2] M. Rennhard, S. Rafaeli, L. Marthy, B. Plattner, D. Hutchinson, "An architecture for an anonymity network," Proc. of 10th IEEE Intl. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2001), pp, 165-170 , Boston, USA, June 20-22, 2001. 24

[3] J. Raymond, "Traffic analysis: protocols, attacks, design issues and open problems," In H.Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 10-29, Springer-Verlag, 2000. 24

[4] Y. Hu, A. Perrig, D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in The 8th ACM International Conference on Mobile Computing and Networking, September 2002. 24

[5] J. Kong, X. Hong, M. Gerla, "An anonymous on demand routing protolcol with untraceable routes for mobile ad hoc networks," Technical Report TR-030020, April, 2003, UCLA Computer Science Department, Los Angeles, California, 90025. 24

[6] A. Fasbender, D. Kesdogan, O. Kubitz, "Variable and Scalable Security: Protection of Location Information in Mobile IP," in 46th IEEE Vehicular Technology Society Conference, Atlanta, Mar. 1996. 24

[7] A. Fasbender, D. Kesdogan and O. Kubitz, "Analysis of Security and Privacy in Mobile IP," in 4th International Conference Telecommunication Systems, Modeling and Analysis, Nashvill, Mar. 21-24, 1996. 25

[8] D. L. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms," Communications of the ACM 24, 2 (February 1981). 25, 28

[9] R. Newman-Wolfe, B. Venkatraman, "High level prevention of traffic analysis," Proceedings of the Seventh Annual Computer Security Applications Conference, pp. 102-109, San Antonio, December 2-6, 1991. 26, 27

[10] Y. Guan, C. Li, D. Xuan, R. Bettati, W. Zhao, "Preventing traffic analysis for real-time communication networks," in Proceedings of Milcom '99 (November 1999). 26

[11] O. Berthold, et. al., "Project anonymity and unobservability in the Internet," Computer Freedom and Privacy Conference 2000 (CFP 2000), Workshop on Freedom and Privacy by Design, 2000. 26

[12] M. G. Reed, P. Syverson, D. Goldschlag, "Anonymous connections and onion routing," in Proceedings of the IEEE Symposium on Security and Privacy (Oakland, California, May 1997), pp. 44–54. 26, 28

[13] S. Jiang, N. Vaidya and W. Zhao, "A dynamic mix method for wireless ad hoc networks," in Proceedings of IEEE Military Communication Conference (Milcom), Oct 2001. 26

[14] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK, May, 1996. 28

[15] K. Fall and K. Varadhan, Eds., The *ns* Manual, 2003; available from http://www-mash.cs.berkely.edu/ns/ . 29

[16] J. Broch, D. A. Maltz, D. B. Johnson, Y-C Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in ACM/IEEE International Conference on Mobile Computing and Networking(MobiCom '98), 1998. 29