This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Stable Topology Support for Tracing DDoS Attackers in MANET

Yinan Jing, Xueping Wang, Lili Zhang, Gendu Zhang
School of Computer Science
Fudan University
Shanghai P.R. China
Email: {jingyn, wangxp, 09210240089, gdzhang}@fudan.edu.cn

Abstract—**Traceback technique is useful to identify the source of an attack. Several types of traceback schemes have been proposed for wired networks. But most of them are not suitable for mobile ad hoc networks (MANETs) due to limited resource and dynamically-changing topology. Among all of existing schemes, probabilistic packet marking (PPM) scheme might be the most promising scheme for MANET because it is more lightweight than others. However, it is difficult for PPM scheme to converge quickly in MANET, since it relies on the assumption of static topology that does not hold in MANET due to dynamic topology. In this paper, we propose a traceable overlay network with relative stable topology support for traceback based on identity replacement mechanism. We present the protocol design and experiments. The experiment results show that our approach can get a much more stable topology for traceback and better traceback performance in MANET.**

Keywords- traceback; MANET; stable topology; overlay

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a self-organizing multi-hop wireless network formed by a group of mobile nodes where all nodes take part in forwarding packets for each other. It is useful in various scenarios where infrastructure support is not available or cannot be relied upon, such as battlefield communication, emergency service, disaster recovery, environment monitoring, personal entertainment, mobile conferencing and etc [1]. MANET differs from traditional wired networks in its limited bandwidth, limited energy resource, and its dynamic topology. These properties make MANET more vulnerable to distributed denial-of-service (DDoS) attacks [2], which are characterized by an explicit attempt to prevent the legitimate use of a service by consuming the resource of remote servers or the network bandwidth.

IP traceback is one of the effective countermeasures against DDoS attacks. It allows the victim to identify the attack sources even in the presence of IP spoofing. Then some other countermeasures such as filters can be deployed in good season and in the best places. Hence, traceback technique plays a key role in the process of defense. A number of traceback schemes have been proposed for Internet [3]. However, these existing traceback schemes are not directly applicable to mobile ad hoc networks for different reasons. Among all of existing traceback schemes, *probabilistic packet marking* (PPM) scheme might be most promising scheme for attack source traceback in wireless ad hoc networks, because it is more lightweight on the network overhead and node overhead than other schemes.

The main idea of PPM scheme is that routing nodes probabilistically sample some packets and mark them with partial path information (such as node id) before packet forwarding. After the victim receives a modest number of marked packets, then it can reconstruct the complete attack graph. As we all know, the PPM scheme for Internet need rely on a strong assumption that the routes traversed by attack flow are static. However, this assumption generally does not hold in MANET. An attack path in MANET might dynamically change because of the free mobility of nodes. Once the topology is changed, the detected attack path is no longer valid and need to traceback again, or the in-processing traceback procedure can not complete in the prospective time. That is the dynamic topology of MANET makes PPM more difficult to converge. Hence, it is necessary to provide a relative stable topology support for traceback if we want to make the PPM scheme work well in MANET.

In this paper, we propose a traceable overlay network with relative stable topology support for traceback based on an identity replacement mechanism. We present the detailed protocol design and make extensive experiments. The experiment results show that our approach can get a much more stable topology for traceback in MANET.

II. RELATED WORK

IP traceback schemes in wired networks can be classified into three categories. First are *logging-based traceback schemes*, such as CenterTrack [4] and Hash-based IP traceback [5]. Second are *ICMP-based traceback schemes* called iTrace [6]. Third are *packet-marking schemes*, which can be further divided into two sub-categories: *Deterministic Packet Marking* (DPM) [7] and *Probabilistic Packet Marking* (PPM) [8]. Due to different reasons, these schemes for wired networks are not suitable for resource constrained MANET directly. In Table I, we analyze their weakness if applied in MANET.

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

TABLE I. WEAKNESS ANALYSIS OF DIFFERENT TRACEBACK SCHEMES

Traceback techniques	Weakness if applied in MANET
Logging-based	● need enormous storage space to store logs ● heavy overhead for log query
ICMP-based	● need extra bandwidth, more network overhead ● might fail under flooding DDoS attacks
Deterministic Packet Marking (DPM)	● cannot be applied for MANET because there is no definite network edge in MANET
Probabilistic Packet Marking (PPM)	● dynamic topology might make it difficult to converge (i.e. only work well on the premise of static topology) ● too long convergence time to adapt to the topology changes

The traceback problem in wireless ad hoc network is firstly addressed by Vrizlynn L. L. Thing et al [9]. The traceback schemes for wireless ad hoc networks can also be classified into the same three categories as those for wired networks.

A typical logging-based scheme is designed to log the packets or digests of packets at the intermediate routers. Once an attack is detected, the victim will retrieve the logged information from the distributed logging nodes and compare it with the suspect packet to find the attack path. Hotspot-based Traceback [10], CAPTRA [11], the scheme proposed by Kim et al [12] and SWAT [13] are logging-based traceback schemes for wireless network. The above-mentioned schemes [10]-[12] mainly inherit from the Hash-based approach [5]. Although the traceback speed of logging-based schemes is usually faster than others, they need enormous storage space to store logs and produce heavy network overhead when querying the logs. Hence, they are not suitable to be used in MANET especially when the storage space and power of nodes are limited.

The main idea of the ICMP-based traceback scheme [6] is that the intermediate routers generate some ICMP messages containing their id information with a low probability and send them to the same destination of one certain packet flow. Then once an attack happens, the victim can trace the attack source by using the node information included in the received ICMP messages. Based on this technique, Vrizlynn et al [14, 15] has proposed an iTrace-CP method for ad hoc networks. However, when the MANET is under a DDoS attack, there might be no extra bandwidth to transmit these messages, because the bandwidth of MANET is always limited and might be exhausted by the attack traffic. Hence, such an ICMP-based traceback method cannot be applied for MANET especially when under flooding DDoS attacks.

Unlike the ICMP-based schemes transmit information for traceback via an out-of-band method, packet-marking schemes provide the intermediate node information to the attack target in band by marking this information in the packets. Thus they will not produce extra network load. In the DPM scheme [7], each packet is marked by the ingress edge router. However, as we all know, MANET has no definite network edge due to dynamically changing property. Therefore DPM is obviously not suitable to MANET. Rather than mark all packets in DPM, PPM marks packets with a certain probability. Because the PPM scheme is simple and lightweight, it is popular to be applied in both wired networks and wireless networks.

However, existing PPM schemes for wireless networks have following shortcomings. First, the dynamic topology property of MANET is not sufficiently taken into consideration in some existing schemes because they are not designed for MANET. For example, the schemes [16]-[18] are designed for wireless sensor network, whose topology is usually believed to be more stable than that of MANET. In order to reduce the negative effect caused by dynamic topology of MANET, ZSBT [19] propose to divide the network into a number of zones and mark the zone id in the passing packets. However, because the victim only can receive the zone id, the traceback result of ZSBT is not accurate enough. An algebraic scheme for dynamic networks is proposed by Das et al [23]. However, it can only trace DoS attacks with a single attack source. Second, PPM usually needs a long convergence time because it must collect enough number of marking packets before reconstructing the attack path. That is the traceback speed of PPM schemes might be not fast enough to adapt to topology changes as soon as possible. Cheng et al [20], [21] propose to adapt to dynamic changes of topology by improving the traceback speed of PPM schemes. But such an improvement is limited. Third, some PPM-based schemes need to depend on one certain network architecture or routing protocol. For example, FBT [21] can only be used in a hierarchical wireless network. And the scheme proposed by Yang et al [22] must depend on the DSR (Dynamic Source Routing) protocol.

III. STABLE TOPOLOGY SUPPORT FOR TRACEBACK

As discussed in the previous sections, we should do our best to prolong the stable time of network topology to make PPM schemes work better in MANET. In this paper, we propose an *Identity Replacement* (IR) mechanism to give a more stable topology support for traceback.

A. Big Picture of Identity Replacement Mechanism

As is known to all, it is the intrinsic nature of MANET that the network topology dynamically changes due to node movement or node failure. So it is impossible to keep the physical topology being static for a long time. Nevertheless we can create a virtual overlay network above the network layer to get a relative stable logical topology. For instance, as Fig. 1 shows, we create an overlay network above the network layer. Each node has a unique *node id* (*physical id*) on network layer that is symbolized by an Arabic notation, such as n1, n2 and so on. And it has a *node name* (*logical id*) on overlay layer that is symbolized by a capital English letter, such as A, B, C, D. The node id is supposed to be fixed, while the node name can be changed according to the network context. And there is a temporary mapping between them.

As Fig. 1(a) shows, at first there is a routing path from n1 to n4 on physical network layer: n1→n2→n3→n4. And on the virtual overlay layer, there is a corresponding logical path: A→B→C→D. Here we assume the node n2 moves away and n5 just moves into this path. After a route recovery process, the

physical path will migrate to: n1→n5→n3→n4 as Fig. 1(b) shows. In order to maintain the stability of the overlay layer topology, we propose an *Identity Replacement* mechanism. For example, as Fig. 1(b) shows, in order to remain the overlay layer topology stable, the node n5 will change its name (logical id) to "B" according to the current network context, while its physical node id will not be changed. Thus depending on this mechanism, the topology of the overlay network could be remained as stable as we can.

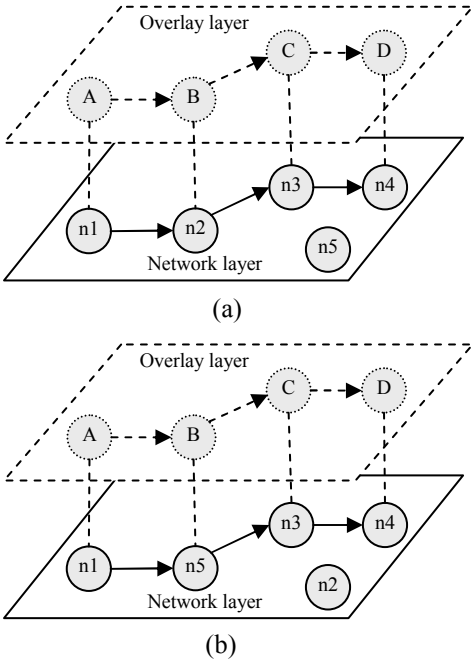


Figure 1. Migration of two layer topology

Then we can perform traceback on this overlay network with a relative more stable topology support. In the previous PPM schemes, the routing node marks its node id (physical id) into packets. If the node (e.g. n2 in Fig. 1) moves out of the attack path, those corresponding marking packets received by the victim have no meaning to traceback, because that node has no longer been forwarding attack packets and would be not the target of traceback any longer. Then the victim needs to receive more new marking packets to reconstruct the attack path. If the topology changes like this continually, the PPM scheme will be difficult to converge. It's a vicious circle. Instead, when the PPM scheme works on the above-mentioned overlay network, the intermediate node will mark its node name (logical id, e.g. "B" in Fig. 1) into packets rather than mark its node id. From the victim's view, it will reconstruct a logical attack graph, which maps to the nodes that are currently forwarding the attack traffic. Such a traceback result will be more helpful to the follow-up defense than before. Since this logical topology is relatively more stable than that physical topology, it is easier for PPM schemes to converge quickly.

B. A Cross-layer Design: IR-AODV Protocol

From the view of conceptual model, the stable topology construction method based on the *Identity Replacement* mechanism presented in the above section is independent of concrete network architectures or routing protocols, because the virtual overlay constructed for traceback will not change the original packet forwarding rule on network layer.

In this paper, in order to illustrate this mechanism, we presented a concrete implementation upon the *Ad hoc On-demand Distance Vector* (AODV) protocol [24], which is a popular reactive routing protocol designed for MANET where routes are determined only when needed. We adopt a cross-layer design principle to implement this stable topology construction method and propose a new protocol called *Identity Replacement based AODV* (IR-AODV) protocol. Next we will give the detailed design of this protocol.

1) Reconstruction of Routing Table

In order to implement our identity replacement mechanism, we need to reconstruct the original AODV routing table, which mainly includes two fields: destination of one route and next hop address of this route. Here we still take the network scenario shown in Fig. 1 as an example. Fig. 2(a) shows the reduced routing table of node n1 in AODV, where the next hop address (Next Hop) is the node id of the next hop node, namely n2. When a link error occurs, the next hop will change from n2 to n5 after recovering the route.

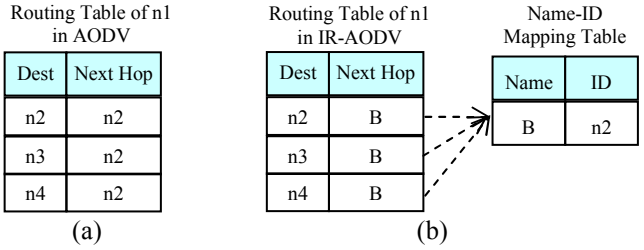


Figure 2. Reconstruction of Routing Table

In order to avoid the changes of routing table, we reconstruct the original routing table. In the new routing table in IR-AODV protocol, the next hop address (Next Hop) is revised to maintain the name of the next hop node rather than node id. Additionally, we attach a *Name-ID Mapping Table* (NMT) to the routing table to maintain the temporary mapping between virtual nodes and actual physical nodes. For example, the next hop of routes from n1 to n2, n3 and n4 is a virtual node named "B" as Fig. 2(b) depicts, and now "B" is mapped to the actual node n2. When n5 replaces n2 due to node movement as Fig. 1(b) shows, the next hop of routes does not need to be changed because the name of n5 will be replaced to be "B" by our Identity Replacement mechanism and only the NMT of n1 need to be updated from B-n2 to B-n5. That is n5 is substituted for n2 to be "B". Hence, from the view of overlay layer, the logical topology of overlay network is kept stable, although the physical topology is changed.

2) Process of Identity Replacement

To introduce the process of identity replacement, we continue to use the example shown in Fig. 1. At first there is a routing path from n1 to n4: n1→n2→n3→n4. Suppose n2 is moving out of the path and n5 is moving into the path. When

n2 moves out of the transmission range of n1, n1 will detect a link error to the virtual node B. So it needs to find a substitute for B. Then n1 will initiate a process of identity replacement rather than send a RERR message like AODV. This process includes following steps as Fig. 3 shows.

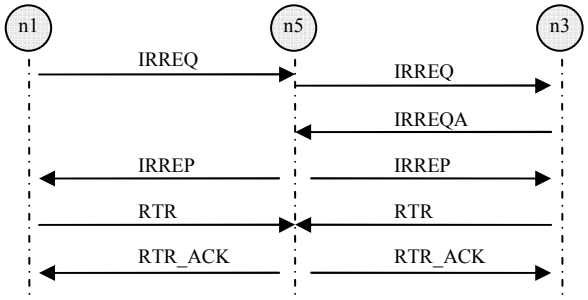


Figure 3. Process of Identity Replacement

First, as Fig. 3 shows, n1 broadcasts an *Identity Replacement Request* (IRREQ) message to its neighbors to ask who can substitute for the virtual node named "B". The IRREQ message uses the name of this virtual node, namely "B", as its message id. By the way, the node who issues the IRREQ will cache all the arriving data packets before the identity replacement process is complete. Thus there is no packet to be dropped during this process.

Second, after the new arriving node n5 receives the IRREQ message from n1, it will cache this message at first. If it receives any duplicate IRREQ messages with the same message id, it will drop them by examining its cache. For example, if the node n3 also detected a link error to the virtual node "B" at the same time and issued a same IRREQ for "B" to n5. Then n5 will ignore the duplicate request by the first-come-first-served principle. Furthermore, in order to decide whether this request is valid or not, it will ask other neighbor nodes to help itself confirm this request by propagating this request with a request-confirmation flag to its neighbors.

Third, when n3 receives an IRREQ message, it firstly decides whether it is issued by itself. If it is, it will drop this message. If not, it will examine whether the virtual node contained in this request is its neighbor and this message is attached with a request-confirmation flag. If it is, it will send an *Identity Replacement Request Acknowledgement* (IRREQA) message back to n5 to confirm this request issued by n1 is legitimate.

Fourth, once n5 receives the IRREQA message, it could make sure this request is trustworthy and then unicast an *Identity Replacement Reply* (IRREP) message to nodes that send IRREQ or IRREQA message to it. The IRREP message means that n5 is willing to substitute for the virtual node B.

Fifth, in order to help n5 rebuild its routing table as quickly as possible, after receiving the reply message from n5, n1 and n3 will send a *Routing Table Recovery* (RTR) message back to n5, which contains some up-to-date information that is useful to the new arriving node n5, including the destination address of paths passing through this virtual node, sender's node id and its name, and some routing information that might be used by this node. These messages will definitely help n5 rebuild its routing table according to the current network context as quickly as possible.

Sixth, after recovering its routing table, n5 will change its name to be "B" and send back with a *Routing Table Recovery Acknowledgement* (RTR_ACK) message in a unicast manner to confirm it has completed the identity replacement.

Finally, when n1 and n3 receives the RTR_ACK message, it needs to update its Name-ID Mapping Table from B-n2 to B-n5, while its routing table does not need any change. So far by above mentioned steps, the process of identity replacement is completed and routes are rebuilt successfully. Then nodes can continue send the cached packets to their destination.

In order to ensure protocol converge correctly, we set some timers on the nodes during the identity replacement process. For example, when n1 sends an IRREQ message, it will set a timer for this request at the same time. When the timer is time out, this run of identity replacement will be failed. Then this process will be retried for some times. If it still fails, it will work as same as the original AODV protocol. On the other hand, our protocol can ensure that one virtual node is replaced by only one physical node and one node could substitute for only one virtual node. To avoid one virtual node is replaced by two or more nodes, any node can only issue one IRREQA message for one virtual node and the nodes who receive IRREP message will check whether this IRREP message is corresponding to the valid IRREQ message. In addition, because the replacement process is restricted within one-hop local area, one node could substitute for only one virtual node. Hence, the protocol can converge without any conflicts.

If such a process of identity replacement could not be launched, e.g. two consecutive nodes in a path moved out of this path or powered off for some reasons, then the node that detected the link error will send a RERR message to report link error like in AODV protocol. In such a situation, the topology of the virtual overlay must also inevitably be changed.

IV. EXPERIMENTS

To compare the topology stability and traceback performance, we define following two performance metrics.

- *Link Break Ratio* (*LBR*). It is defined as the ratio of the total number of logical link breaks (LLB) to the total number of physical link breaks (PLB), i.e. *LBR=LLB/PLB*.
- *Traceable Ratio* (*TR*). It is defined as the ratio of the number of successful traceback to the total number of traceback attempts.

In the definition of LBR, the number of PLB reflects the stability of physical topology on network layer, and the number of LLB reflects the stability of logical topology on overlay layer. The smaller the LBR is, the more stable than the underlying network the overlay topology is. On the contrary, if

LBR is approaching to 100%, it indicates that the change of the logical topology is similar to the physical topology.

Due to dynamic changes of topology, the traceback performance in MANET cannot simply be evaluated by the convergence time metric as in [8]. Hence, we define a new metric called traceable ratio. Here, we let T_t be the time needed by a run of traceback, and T_s be the time during which the topology keeps stable after the start of traceback. If $T_s \geq T_t$, we call this run of traceback is successful, since this traceback result will not be influenced by the next change of topology. So TR can reflect the traceback performance in MANET more exactly.

We implement IR-AODV protocol based on AODV routing protocol on GloMoSim 2.03 [25] and make experiments on it. Table II describes some detailed experiment environment settings.

TABLE II. EXPERIMENT ENVIRONMENT SETTINGS

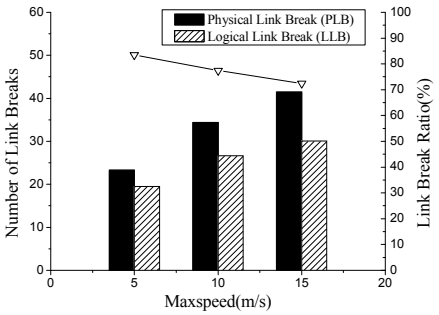
Parameter	Value
TERRAIN	1500m×900m
NODES	30
NODE-PLACEMENT	RANDOM
MOBILITY MODEL	Random Way Point (pause 30sec)
MAC-PROTOCOL	802.11
ROUTING-PROTOCOL	IR-AODV, AODV
DATA-TRAFFIC	CBR (packet size=512B)

From Table II, we can see 30 nodes are placed randomly in an area of 1500m×900m at the initial phase of each experiment. Each node communicates using 802.11 MAC layer and follows the Random Way Point (RWP) mobility model with the max speed of 5m/s to 30m/s. And data traffic is comprised of Constant Bit Rate (CBR) flows, which are at a rate of one packet per second. The value depicted in the following figures is the average value of 30 times of independent simulations.

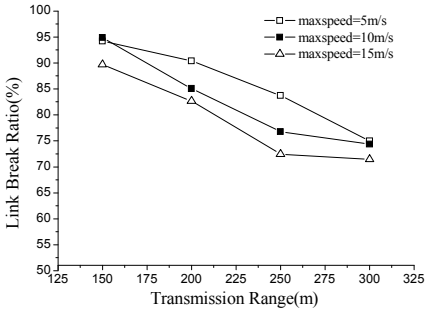
1) Performance of Link Break Ratio

Fig. 4(a) illustrates the LBR of IR-AODV with respect to different max speed. Here each node has a transmission range of about 250 meters. From Fig. 4(a), we can find that with the increase of node moving speed the number of PLB and LLB both increase. That is the faster the node moves, the more link breaks occurs. But we can also find an interesting phenomenon from Fig. 4(a) that the LBR declines with the increase of moving speed. For example, at the maximum speed of 5m/s, IR-AODV achieves over 83.43% LBR, i.e. the stability of logical overlay topology is improved about 16.57% than the underlying physical topology. At the speed of 15m/s, IR-AODV improves stability of logical overlay topology over 27.57%. This phenomenon is because when the nodes move faster, there are more chances for moving nodes to replace the virtual node where a link break occurs.

Fig. 4(b) shows the LBR when the transmission range of each node varies from 150m to 300m. On the whole, the LBR of IR-AODV protocol decreases with the increase of the transmission range. For instance, when the transmission range is 150m, the LBR under different moving speed is above 90%. That means the virtual overlay topology varies similar to the physical topology. However, when the transmission range is enlarged to be 300m, the LBR declines dramatically to approach to 70%, i.e. the virtual overlay topology is more stable than the underlying physical topology. This phenomenon is because the value of transmission range reflects the neighboring relationship between each node in fact. The larger transmission range is, the more neighborhoods there are for one node. When a link break occurs, it is easier to find a node near the broken-down virtual node to replace it. In addition, when the nodes move faster, the virtual overlay is more stable than the underlying network as Fig. 4(b) depicts. For example, even when the transmission range is as small as 150m, the LBR under 15m/s is smaller than that under 5m/s or 10m/s, because fast mobility of nodes can remedy the limitation of small transmission range to some extent in our approach.



(a) Link Break Ratio vs. Moving Speed

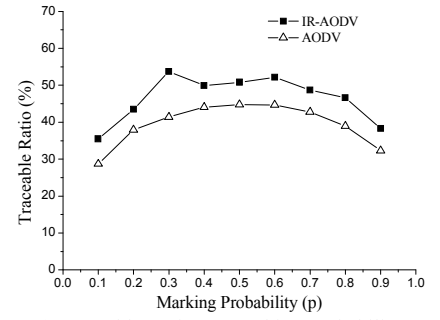


(b) Link Break Ratio vs. Transmission Range

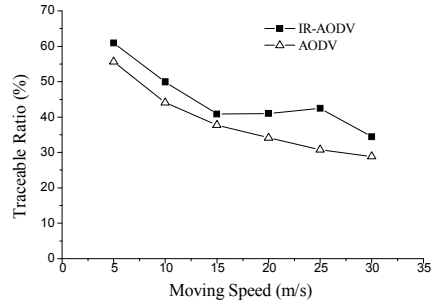
Figure 4. Link Break Ratio of IR-AODV

2) Performance of Traceable Ratio

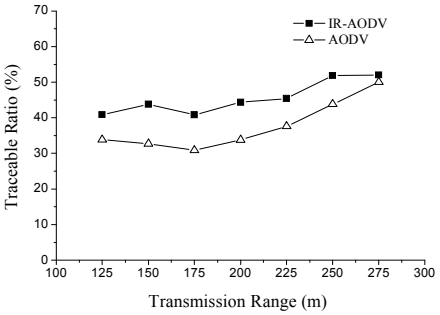
In the following experiments, we adopt the original PPM scheme proposed in [8]. Fig. 5(a) shows when the max moving speed is 10m/s, the traceable ratio of IR-AODV is all larger than that of AODV under different marking probability (p). And when p is about 0.4, the performance of both approaches is best. Fig. 5(b) shows when marking probability is 0.4, the traceback performance of IR-AODV is also better than that of AODV. But it will degrade when nodes move faster, because after all faster mobility will cause both physical and logical topology changing more dramatically. Fig. 5(c) shows when p is 0.4 and max moving speed is 10m/s, the traceable ratio of IR-AODV is also greater than that of AODV when transmission range varies from 125m to 275m.



(a) Traceable Ratio vs. Marking Probability



(b) Traceable Ratio vs. Moving Speed



(c) Traceable Ratio vs. Transmission Range

Figure 5. Traceable Ratio

V. CONCLUSION

In this paper, we analyzed the weakness of different traceback schemes if applied in MANET. Then we pointed out a more stable topology support is very important for tracing attackers by using the lightweight PPM schemes. We proposed to construct an overlay network for traceback based on the identity replacement mechanism above the existing network layer. And we presented an IR-AODV protocol which integrates the identity replacement mechanism with the AODV protocol. Finally, we conducted several experiments on the GloMoSim simulator. The experiment results show that our approach can effectively improve the stability of overlay network topology and traceback performance in MANET.

REFERENCES

[1] C. Imrich, M. Conti, and J. Liu, "Mobile Ad Hoc Networking Imperatives and Challenges," *Ad Hoc Networks*, vol. 1, Jul. 2003, pp. 13–64.

[2] Arun Kumar, Jessi K.Kouput, Saijai Chancham, YoungMi Kim. "Denial of Service Attacks in Ad Hoc Networks". *Telecommunications at the University of Colorado*, Boulder, 2003,5.

[3] A. Belenky, N. Ansari. "On IP traceback", *IEEE Communications Magazine*, 41(7), pp.142-153, (2003).

[4] R. Stone. "CenterTrack: An IP Overlay Network for Tracking DoS Floods". *In: Proceedings of the 2000 USENIX Security Symposium*, Denver, CO, July 2000.

[5] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, and Christine E. Jones, "Hash-Based IP Traceback", *in Proceedings of the 2001 conference of Applications, technologies, architectures, and protocols for computer communications*, August 2001, pp: 3-14.

[6] S. Bellovin, M. Leech, T. Taylor (2001, October). ICMP Traceback Messages. Available: http://www3.ietf.org/proceedings/01dec/I-D/draft-ietf-itrace-01.txt

[7] A. Belenky, N. Ansari. "IP Traceback with Deterministic Packet Marking". *IEEE COMMUNICATIONS LETTERS*, 2003, 7(4), 162-164.

[8] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, "Practical Network Support for IP Traceback", *ACM SIGCOMM Computer Communication Review*, Volume 30, Issue 4, October 2000, pp. 295-306.

[9] Vrizlynn L. L. Thing, Henry C. J. Lee, "IP Traceback for Wireless Ad-Hoc Networks", 60th IEEE Vehicular Technology Conference, Los Angeles, California, USA, September 2004.

[10] Yi-an Huang and Wenke Lee, "Hotspot-Based Traceback for Mobile Ad Hoc Networks", *in Proceedings of the ACM Workshop on Wireless Security*, Sept. 2005.

[11] Denh Sy and Lichun Bao, "CAPTRA: Coordinated Packet Traceback", *in Proceedings of the fifth international conference on Information Processing in sensor networks*, April 2006, pp. 124-135.

[12] Il-Yong Kim, Ki-Chang Kim. "A Resource-efficient IP Traceback Technique for Mobile Ad-hoc Networks Based on Time-tagged Bloom Filter". *International Conference on Convergence and Hybrid Information Technology*, 2008, pp: 549-554.

[13] Yongjin Kim, and Ahmed Helmy, "SWAT: Small World-based Attacker Traceback in Ad-hoc Networks", *in Proceedings of the Second Annual International Conference on Mobile and Ubiquitous System: Networking and Services*, San Diego, California, USA, July 2005.

[14] Henry C.J. Lee, Vrizlynn L.L. Thing, Yi Xu, and Miao Ma, "ICMP Traceback with Cumulative Path, and Efficient Solution for IP Traceback", *Springer Lecture Notes in Computer Science*, Vol. 2836, Sept. 2003, pp. 124-135.

[15] Vrizlynn L. L. Thing, Henry C. J. Lee, Morris Sloman, and Jianying Zhou, "Enhanced ICMP Traceback with Cumulative Path", *in Proceedings of 61st IEEE Vehicular Technology Conference*, Vol. 4, May-June 2005, pp.2415-2419.

[16] Yan Sun, Anup Kumar, and S. Srinivasam, "WON (Wireless Overlay Network) for Traceback of Distributed Denial of Service", *in Proceedings of the AusWireless Conference*, Sydney, Australia, 2006.

[17] Fan Ye, Hao Yang, Zhen Liu. Catching "Moles" in Sensor Networks. *IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2007: 69.

[18] Qiyuan Zhang, Xuehai Zhou, Feng Yang, and Xi Li, "Contact-based Traceback in Wireless Sensor Networks", *in Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing 2007 (WiCom 2007)*, Sept. 2007, pp. 2487-2490.

[19] Xin Jin, Yaoxue Zhang, Yi Pan, and Yuezhi Zhou, "ZSBT: A Novel Algorithm for Tracing DoS Attackers in MANETs", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2006, Article ID 96157, 2006, pp. 1-9.

[20] Bo-Chao Cheng, Huan Chen and Ryh-Yuh Tseng, "A Packet Marking with Fair Probability Distribution Function for Minimizing the Convergence Time in Wireless Sensor Networks", *Computer Communications*, Volume 31, Issue 18, December 2008, pp: 4352-4359.

[21] Bo-Chao Cheng, Huan Chen, Guo-Tan Liao. "FBT: an efficient traceback scheme in hierarchical wireless sensor network". *Security and Communication Networks*, 2009, 2(2), pp: 133-144.

[22] Ming-Hour Yang, Chien-Si Chiu, Shiuhpyng Shieh. "Tracing Mobile Attackers in Wireless Ad-Hoc Network". *ICIW* 2008, pp: 7-12.

[23] Abhik K. Das, Shweta Agrawal, Sriram Vishwanath: Algebraic Traceback for Dynamic Networks CoRR abs/0908.0078: (2009).

[24] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.

[25] GloMoSim Simulator, http://pcl.cs.ucla.edu/projects/glomosim/