Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks

[†]Minda Xiang, [†]Yu Chen*, [‡]Wei-Shinn Ku, [§]Zhou Su

[†]Dept. of Electrical & Computer Engineering, SUNY - Binghamton, Binghamton, NY 13902
[‡]Dept. of Computer Science & Software Engineering, Auburn University, Auburn, AL 36849
§Dept. of Computer Science, Waseda University, Ohkubo 3-4-1, Shinjyuku, Tokyo 169-8555, Japan

Abstract — **Mobile Ad Hoc Networks (MANETs) allow mobile hosts to form a communication network without a prefixed infrastructure. Although it provides high flexibility, it also brings more challenges for MANETs to fight against malicious attacks. However, the property of mobility and redundancy also inspires new ideas to design defence strategy. In this paper, we propose a strategy to mitigate DDoS attacks in MANETs. Assume that a malicious attacker normally targets specific victims. The attacker will give up if the attack failed to achieve the desired goals after a certain length of attacking time. In our protection strategy, we take advantage of high redundancy and select a protection node. Once a DDoS attack has been detected, the suspicious traffic will be redirected to the protection node. The victim will function normally, and it is reasonable to expect that the attacker will stop the meaningless efforts. Through intensive simulation experiment using NS-2, we have verified the effectiveness of our approach and evaluated the cost and overhead of the system.**

***Keywords*—DDoS Attack Mitigation, MANETs, Redundancy, Protection Node.**

1. Introduction

Security of Mobile Ad hoc Networks (MANETs) has been a hot topic in the research community. Due to the lack of prefixed physical infrastructure, the dynamic network topologies bring unique challenges. In addition, other issues also contribute to its vulnerability, such as the open architecture, shared radio channels, and limited resources, etc. Without a clear network boundary, it is extremely difficult to develop a comprehensive ad hoc security strategy for MANETs. Currently, MANETs are vulnerable to various attacks including impersonation, message distortion, eavesdropping, Denial-of-Service (DoS), and Distributed DoS (DDoS). These attacks can be roughly divided into two categories: routing attacks and packet forwarding attacks.

The goal of routing attacks is to prevent legitimate nodes from constructing the correct routing tables. This is often accomplished by disrupting the establishment of routing tables, diverting directions of packet forwarding, or tampering the routing information being exchanged among nodes. For example, in routing cache poisoning attacks, two malicious nodes inject falsified routing message into the network in order to feign that there exists links [1].

In contrast, the packet forwarding attacks maliciously inject excessive data or control packets into the network that saturate the network link bandwidth and computing resources. The overwhelming network traffic prevents the innocent legitimate users from accessing network based services. As one type of DoS attacks, for example, in rushing attacks, the malicious nodes constantly send routing requests and, hence, run out precious network resources such as bandwidth and CPU cycles [2].

Although various security strategies have been adopted widely in wired networks, they cannot be applied in MANETs directly. It is more challenging in MANETs to satisfy the common security requirements such as information confidentiality, data integrity, and service availability. Research has been conducted in past decades that tries to integrate security solutions on top of secure routing protocols. To date, however, it is still an ongoing research on techniques to fight against malicious behaviors, such as tunneling attack and DoS.

In this paper, we propose a novel approach to alleviate the impact of DoS or DDoS attacks in MANETs based on AODV (Ad hoc On demand Distance Vector) routing protocol. Our method, which is named Protection Node-based Strategy, is based on two fundamental assumptions: first, the attacker is not aimless; and second, the MANETs adopt a hierarchical architecture, and the nodes are classified into different levels according to their importance. This scheme is suitable to be applied in environments where lower level nodes are willing to protect higher level nodes.

Normally, the higher level nodes have higher priority, and they are more important. To achieve better network service availability, we will use lower level nodes to protect higher level nodes. Protection nodes are selected to supervise malicious flows, and meanwhile, to protect the victim nodes. Our scheme is designed to mitigate DoS or DDoS attacks once they are detected. The DDoS attack detection problem is beyond the scope of this paper, and numerous researches have been conducted [3], [4], [5].

The rest of the paper is organized as follows. A brief review of related work is presented in Section 2. Section 3 illustrates the rationale and design details of our protection node-based DDoS attacks mitigating strategy. The experimental results and performance evaluation are discussed in Section 4. Section 5 discusses some of the concerns in our design, and Section 6 concludes the paper.

2. Related Work

The research in MANETs is a broad topic covering architecture, routing, and security. Although there are many research papers about the DDoS attacks defense strategies in MANETs [4], [6], [7], this section only gives a brief discussion about research that is closely related to the idea of this paper.

Based on the approaches that the nodes adapt to gather the routing information, routing protocols in MANETs can be classified into two categories: on-demand routing protocols

* Manuscript submitted on August 1, 2011 to *the 2011 IEEE Global Communications Conference (GLOBECOM 2011)*, Dec. 5 – 9, 2011, Houston, Texas, USA. Corresponding author: Yu Chen, SUNY – Binghamton, Binghamton, NY 13902. E-mail: ychen@binghamton.edu, Tel.: (607) 777-6133.

and table-driven protocols. The well-known on-demand routing protocols include AODV (ad hoc on-demand distance vector) [8], DSR (dynamic source routing) [9], and TORA (temporally-ordered routing algorithm) [10]. Protocols in this category do not keep in time routing information. When the source node wants to send data to the destination node, it will begin a route detection procedure to find a route to the destination node.

Examples of table-driven routing protocol include OLSR (optimized link state routing protocol) [11], TBRPF (topology dissemination based on reverse-path forwarding) [12], DSDV (destination-sequenced distance vector routing) [13], WRP (wireless routing protocol) [14], and STARA (system and traffic dependent adaptive routing algorithm) [15]. In this category of routing protocol, every node maintains one or more routing tables by exchanging routing tables with peers periodically. These tables include all the routing information of the network. The AODV protocol is one of the protocols that have been widely recommended in MANETs, and our strategy is based on AODV environment.

Yi *et al*. have proposed a Security-Aware Routing protocol for wireless ad hoc networks, or SAODV for short [16]. The main idea of this protocol is to divide different nodes into different security levels. During the routing procedure, only the nodes in the same level or higher level can be selected. Therefore, when the nodes need to establish a path, they first compare the level of intermediate nodes with the source node. Only if the level requirement is satisfied, then the node will be included in the route; otherwise, the RREQ (route request) packets are flooded continuously.

A DoS attack defense strategy has been proposed by Liu and Shen [17]. In this scheme, every individual node is assigned the duty to supervise its neighbors. Each node arranges its buffer uniformly to every neighbor nodes. For example, if there are N neighbor nodes, every one of them will get 1/N buffer space. If any of them takes more buffer space than 1/N, succeeding packets will be dropped from it. In addition, each node assigns priorities to its neighbors based on the transmission rates. Specifically, if a neighbor node sends M packets per second, then its priority value is set as 1/M. A node handles the incoming packets according to the priority values of the senders.

A threshold of the transmission rate is set, and a neighbor node will be deemed as a malicious one if its transmission rate is higher than the threshold. Consequently, the node will be isolated. The assigned buffer space for the recognized malicious node will be reallocated to other neighbors. The overhead in bandwidth and the wasted buffer assigned to non-active nodes are two major disadvantages of this strategy.

Previously, a strategy had been proposed that is capable of tolerating DoS attacks using a proxy network [18]. Proxy networks are proven effective in handling the incoming packets and are capable of providing resilient mediation to user to support continued network access. Although the reported specific strategy was only applicable in wired network, we are inspired by the idea to apply the principle in MANETs to achieve our goal.

3. Protection Node-based DDoS Mitigating

3.1 Rationale of Protection Node Selection

Inspired by the SAODV scheme, we adopt the hierarchical network architecture in which the nodes are divided into multiple levels according to their importance. Lower level nodes are used to protect high level nodes. Specifically, each node will be assigned a lower level node as its protection node, which is named as a destination protection node or Local Protection Node (LPN). They protect the target of DoS attacks. For the lowest level nodes, a neighbor of the same level will be selected as its protection node.

Meanwhile, at the source of the DDoS attacks traffic, a node can be used to monitor the malicious node. In our strategy, when an attack route is built, the node that is the first hop from the source node will also be assigned as a protection node. This kind of protection node is named a Remote Protection Node (RPN), which is used to monitor the attack source node. If the source node is identified as a malicious one, the packets from it will be dropped by the RPN. In addition, the new RREQ from the malicious node will be dropped by RPN, too. Hence it prevents the DoS attack agent from establishing a new route.

In our system, each higher level node selects its LPN when it joins the MANETs. Due to the dynamical network topology, the LPN of a protected node needs to be updated periodically. Once the LPN node is selected, it will be inserted into the route whose destination is the protected node. The LPN will serve as the last hop in front of the destination node, and all packets to the destination node will be forwarded through the LPN. Therefore, the LPN monitors the traffic whose destination is the node under protection.

3.2 LPN Selection Procedure

A three-step-handshake approach is adopted to find an LPN for a higher level node that needs to be protected. In the first step, the higher level node broadcasts the LPN query packet (LPNREQ) to its neighbor lower level nodes. Once the request is received, the neighbor nodes unset their fresh tags. Then subsequent LPNREQ packets from other nodes will not be accepted.

In the second step, the receivers send an acknowledgement packet (LPNACK) back to the sender. This LPNACK message serves two purposes: 1) the receiver notifies the sender that it is willing to serve as the LPN; and 2) the sequence of the LPNACK messages helps the sender make a decision. The generator of the first received LPNACK packet is selected as the LPN.

In the third step, the protected node will broadcast an LPN confirm (LPNCFM) message. Besides notifying the LPN node that it is selected, the LPNCFM message lets other un-selected nodes reset their fresh tag that allows them to be selected by other nodes. After the three steps, the protected node-LPN pair can be established.

Figure 1 illustrates how a newly selected LPN is inserted into the route as the last hop node goes toward the destination. A source node broadcasts RREQ to construct the route, and only if the LPN receives the RREQ will the INROUTE tag value of the RREQ be set. When the protected node receives a RREQ, it checks the INROUTE tag first and only accepts the RREQ with the set tag. If the tag value is not true, the LPN must not be in the route. In the situation that an intermediate node receives a RREQ, but it has a fresh enough route to the destination node, the new route will still be built

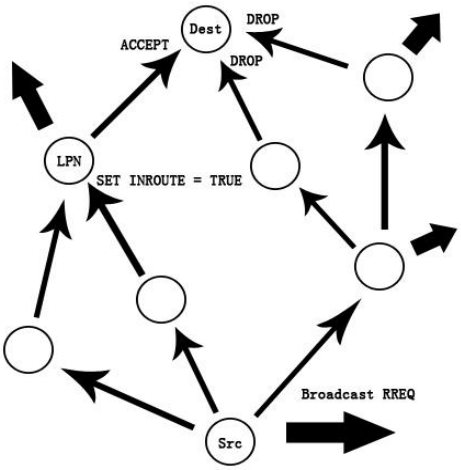

Figure 1. Process of adding LPN to route.

with the old one in it. Because in the first time the LPN will be included in the route, we can ensure that, when the above situation happens, the LPN will also be included in the route.

3.3 DDoS Attack Mitigation Strategies

Figure 2 presents a scenario in which LPN protects the victim node of a DDoS attack. The LPN node filters all the attacking packages in the traffic whose destination is the victim. In addition, the LPN recognizes the source IP addresses corresponding to the malicious traffic, and an Attack Notification Message (ANM) is sent to the victim node. The ANM includes the source IP addresses of involved malicious attack agents. Then, the victim node broadcasts an Attack Information Message (AIM) packet towards the remote protection node (RPN). With the information in AIM, the RPN nodes filter off all the malicious packets at the source side. This mechanism aims to recover the service for destination protection node and to tell every other node to drop the RREQ from the malicious node. After doing this, the malicious nodes cannot send out traffic or build a route.

Essentially, this protection node-based DDoS attack mitigation approach is a trade-off of the redundancy in the

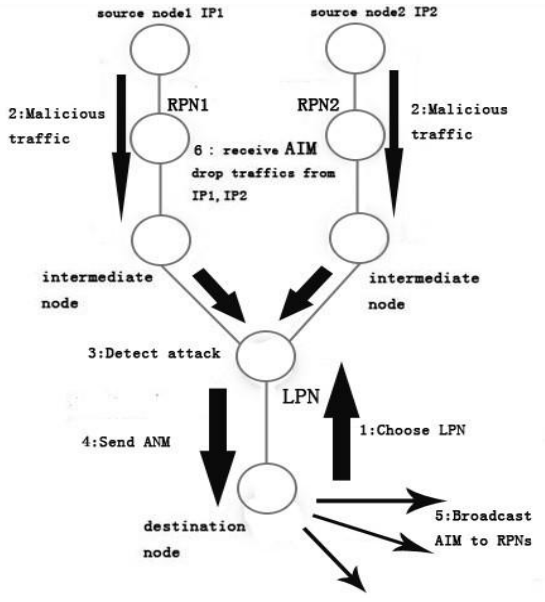

Figure 2. Process of defending DDoS attack

route for higher system availability. The false positive alert leads to impact on throughput of legitimate traffic while it blocks the malicious traffic efficiently.

4. Experimental Study

4.1 Experiment Setups

Our experiments are conducted using the NS-2 simulator. We conduct the experiments in two steps. The first step is to verify the effectiveness of our scheme, and then deeper study is carried out to evaluate the cost and overhead in more detail.

In the first step, there are 60 mobile nodes in the network, and five nodes are sending traffic concurrently to the same destination node. None of the individual traffic rate goes beyond a certain threshold, but the sum of them does. Another malicious node will send traffic to the same destination after 60 seconds to check if the soft state of the protocol can go back to the initial status. Then it will be able to respond to new attacks properly.

All of the nodes randomly move at an average speed of 10m/s. The simulation time is 300 seconds; three malicious nodes send their traffic at 202 seconds, and another malicious node sends traffic at 264 seconds.

The connections among mobile nodes are UDP connections, and we send CBR (Constant Bit Rate) traffic in each communication channel. The CBR rate of the connections is 512Kb/s, and the threshold of the agent is 1.5M/s, so two nodes sending the traffic to the same destination node will not cause an alert but three nodes will. The size of the scenario field is 1000m x 1000m. The queue drop mechanism is tail drop. The routing protocol we use is a revised AODV routing protocol that integrates our LPN, RPN methods. The LPN re-select interval is 20 seconds. Four GAWK documents are used to evaluate the performance of the new protocol.

In step two, we evaluate the performance of our new DDoS attack mitigating scheme in a different network scale. The configurations of different network scale are shown in Table 1. The traffic threshold of the node is set to infinity so that the alert will not be triggered.

Table 1. Network scale configurations

node number	field size (m x m)	number of high level node	number of connections
8	200 x 200	1	2
16	350 x 350	2	4
32	600 x 600	4	8
64	1000 x 1000	8	16
96	1200 x 1200	12	24
128	1500 x 1500	16	32

Five metrics are adopted to conduct a comparison study between our protection node-based DDoS attack mitigation approach and the original AODV protocol. The main purpose is to check how much overhead has been caused in order to mitigate the DDoS attacks. The five metrics are defined as below:

- *Average Hops per Route*: average hops for one packet to propagate from the source node to destination node.
- *Packet Propagation Delay*: average time for one packet to propagate from the source node to destination node.

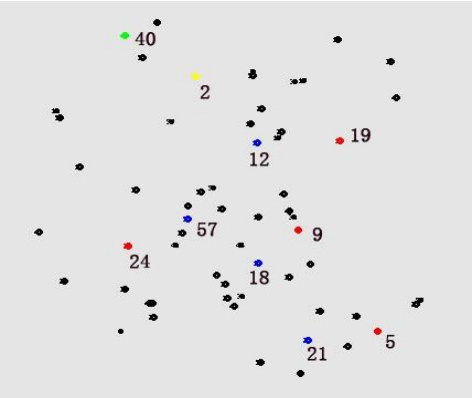

Figure 3. The network topology.

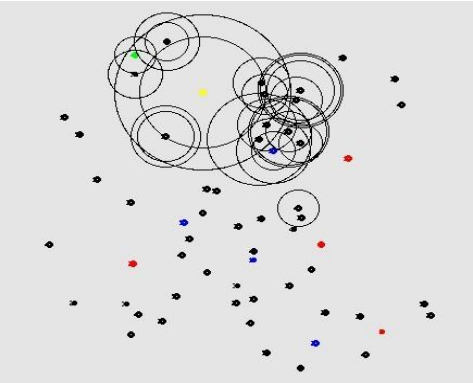

Figure 4 The protected node is broadcasting AIM packet

- *Packet Drop Rate*: drop rate of packet in the whole simulation.
- *Route Building Frequency*: the number of route building process per second.
- *Network Routing Load*: the number of other control packets that transmitted for transmit one data packet.

4.2 Result Analysis

The first experiment is used to verify the effectiveness of our strategy from the perspective of DDoS attack mitigation. And the second step is conducted to evaluate the cost, particularly the overhead compared to the AODV protocol.

4.2.1 Verification of Effectiveness

In the first experiment, 60 nodes are randomly generated, and one of the topologies is shown in Figure 3. Three malicious nodes that send attacking traffic are node 5, node 9, and node 19 that are marked in red. All of them send attack traffic at almost the same time. Node 24 which is also marked in red sends malicious traffic after 60 seconds. The destination of all the traffics is node 2, a high level node, which is marked in yellow as the DDoS attack victim.

During the simulation, the LPN of this victim node is node 40, which is marked in green. The RPNs that dropped the traffic of malicious nodes are marked in blue, which include node 21, node 18, node 12, and node 57. The LPN sends ANM packets to the victim node, which broadcasts AIM packets to the entire network as shown in Figure 4. The RPN nodes that are allocated close to the malicious nodes filter off the attacking traffic. All the other nodes will record the malicious IDs and then drop all the packets sent from the malicious nodes. Therefore, during the simulation, we have

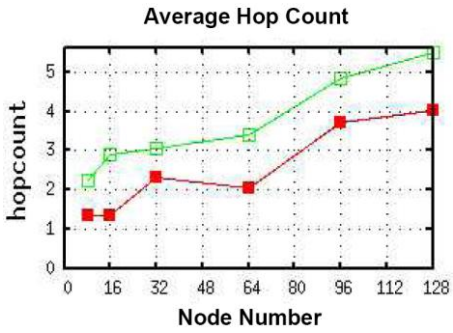

Figure 5. Average hops per route.

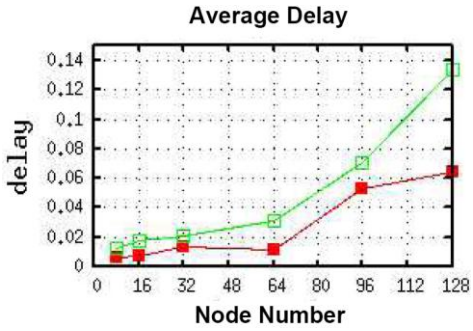

Figure 6. Packet propagation delay.

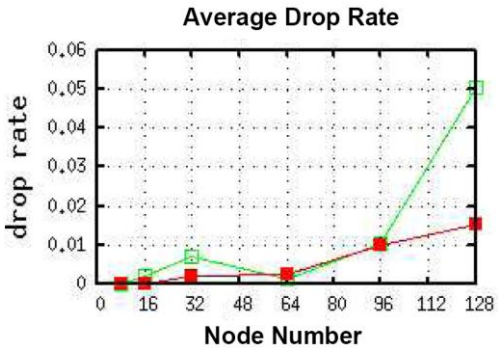

Figure 7. Packet drop rate.

observed that the malicious nodes have tried to rebuild the route many times, but the neighbor nodes never accept their requests.

The simulation results have verified that our protection nodes are capable of mitigating the DDoS attacks and allowing the victim node function normally. In addition, it has also shown that the protocol can recover and return to its initial state after handling a DDOS attack.

4.2.2 Performance Analysis

Figures 5 to 9 present the experimental results of the five performance metrics measured on our new protocol and the original AODV protocol. The lines with hollow square points present the performance of new routing protocol, while the lines with solid square point present the performance of original AODV protocol.

The experimental results have shown that our DDoS attack mitigating protocol does not bring significant overhead to the performance of network. Since it is explicitly required that the LPN has to be in the route of the high level node, the route as well as the hop count must not be optimized. As shown in Figure 5, our protocol only requires one extra hop on top of the original AODV protocol.

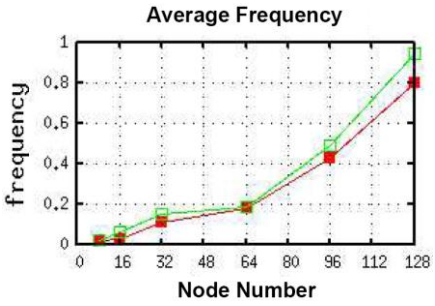

Figure 8. Route building frequency.

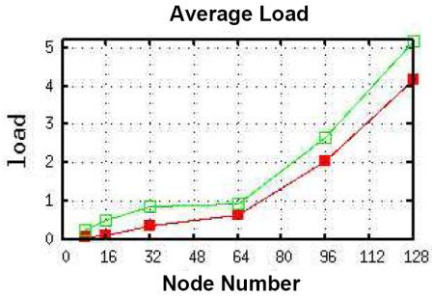

Figure 9. Network routing load.

Meanwhile, Figure 6 shows that the delay is a little higher when the node number passes 64. When a normal node wants to communicate with a high level node, it will buffer some packets first and then start the route discovery process. As one high level node only has one LPN at certain time, the broadcasted RREQ may spend more time finding it and will include it in the route. For instance, in our experiment, the RREQ traversed around almost half of the network to find the LPN. As a result, the first buffered packets will be delayed for a longer time before getting to the receiver. With the increase of the number of high level nodes and network scale, the probability of this situation increases and its effects on average delay are more obvious.

Logically, our protocol does not affect the packet drop rate. Figure 7 shows that, before the total number of node increases to 128, the packet drop rate remains as low as the AODV protocol while the network scale grows. When the node number is 128 the drop rate becomes much higher. The reason is that LPNs cannot be shared between high level nodes. With the increased number of high level nodes, it is more difficult to allocate LPNs. In worst cases, some high level nodes may not be able to find a suitable LPN. Thus, in this case, an old LPN may be used, but the route from the old LPN to the protected high level node may not be available, which will cause routing failure and packet dropping.

The other two metrics, Route Building Frequency and Network Routing Load, actually reflect the behavior of our solution in the face of the mobility. Figure 8 and Figure 9 have shown that our protocol does not affect the route building frequency much, but it poses some overhead on network routing load. In order to find LPN for high level node, LPN packet, LPNACK packet, and LPNACKACK packet should be sent every 20 seconds. In addition, both RREQ and RREP packets are forwarded multiple times to find a valid route for high level node. All of these functions introduce more routes establishing load to the network.

In summary, the experimental results show that our DDoS mitigating strategy is capable of protecting the victim node and isolating the malicious attacking agents. The cost is small, and there is not significant impact on the performance of the network. In fact, in order to examine the performance in extreme situations, we made all the traffic connections high level node related. Therefore, the performance must be better for normal situations in which there would be connections between normal nodes.

5. Discussions

This section discusses several important concerns we considered in the design of our protection node-based DDoS attack mitigating scheme.

LPN is introduced in our model, and almost all the functions are based on it. Therefore, there is a potential threat that LPN will be utilized by attackers to launch attacks. LPN could be compromised to send fake ANM. The consequence is that the fake information contained in ANM will make benign nodes be banned. Actually, any fake ANM or AIM can lead to such a severe attack in the network. To handle these attacks, first, MAC (message authentication code) or message digests can be used to achieve data integrity. Second, signature is used to verify the identity of the traffic source.

In case the LPN is compromised and it sends fake ANM to its protected node, we can verify the real traffics that related to the information contained in ANM. For example, when the RPNs receive the AIMs, they can work cooperatively to verify if the sum of the traffic from the nodes that indicated if AIMs really exceeds the threshold. A record for the reliability of the ANM should be set in the network. If too much mismatching happens, the source LPN node of the ANM will be banned. Another solution is to shorten the LPN selection time. By doing this, the malicious node will have little chance to remain as the LPN.

Mobility is one of the major challenges that make it difficult to implement security solutions in MANETs. To address this problem, all the LPNs are re-selected periodically. In our simulation, the re-selection time is 10 seconds, and the results show that it works well. The mobility also makes it difficult to predict the availability of certain connections among nodes in MANETs. We adopted the approach used in AODV protocol, in which every node maintains a neighbor list that is updated periodically. And the local repair mechanism can help to fix the failed route.

Note here that the nodes in a MANETs can be divided into multiple levels, and it really depends on the characteristics of certain specific applications. Therefore, once an LPN becomes the victim of an attack, it needs help from its own protection node. Such a situation will lead to more complexity in routing. However, due to the limited space, we will study this interesting scenario in our future work.

Actually, our scheme works well in the MANETs that are not built following a hierarchical architecture. In this case, the system administrators can apply any policy to separate the nodes into different groups. One group of nodes can choose protection nodes from other groups.

One of the assumptions of our scheme is that the attacker always aims at specific victims. In practice, sometimes the attacker simply attempts to harm the network functionality without having in mind a specific victim. However, even

when the attacker does not have a specific target, to launch DoS/DDoS attacks, a destination address is needed. This implies that a victim has to be indicated. And it still makes sense to assume that the attacker may give up when it is observed that the attack does not achieve the expected effects.

From the perspective of traffic amount, this scheme does not incur much overhead to the entire network. Only packets whose destination is the victim are forwarded through the protection node. That only leads to one more extra hop in the area around the victim. If the victim is merely one of the intermediate nodes on a path between a source and destination pair, such traffic is not required to be sent through the protection node.

Our strategy may not be able to protect all the nodes in MANETs, since higher level nodes are protected by lower level nodes. The nodes with lowest priority may not be able to find a protection node. However, as we assumed, the failure of these least important nodes will not impact the performance of the whole network. An alternative solution is, as mentioned earlier in Section 3.1, the lowest level nodes may be allowed to select a neighbor of the same level as its protection node.

The effectiveness of this mitigating method depends on the information provided by the DDoS attack detection schemes. Particularly, if the detector cannot determine the address of the attack agents, the RPNs will not be triggered to filtering the malicious traffic at the source side. Then, neither can they isolate these agents effectively.

One limitation of our strategy is that it does not deal with such situation that the attackers just broadcast packets to the entire network to make it congest.

6. Conclusions

This paper presents a novel strategy that protects critical nodes from DDoS attacks in MANETs. Considering the different roles that certain nodes play in a MANETs, it is assumed that there are some important nodes that should be protected with higher priority. Lower level nodes would be allocated as protection nodes to handle the incoming traffic to the higher level nodes.

Through intensive simulation experiments using NS-2, we proved that every functionality works well, and DDoS attack can be mitigated effectively. We have also evaluated the cost of the protocol, and the results are encouraging. The overheads are small to implement the DDoS mitigating scheme on top of the well known AODV protocol.

This paper presents the initial results of our work. More comprehensive studies are being conducted, including the impact of different setting of LPN updating period, the assignment of LPNs in multi-level networks, etc. More results will be reported in our future papers.

References

[1] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," *the 10th IEEE International Conference on Network Protocols* (ICNP 2002), Paris, France, Nov. 12 - 15, 2002.

[2] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *ACM Workshop on Wireless Security (WiSe)*, San Diego, California, September 2003.

[3] I. Aad, J.P. Hubaux, E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks," *IEEE/ACM Transactions on Networking* (TON), vol. 16 (4), pp. 791-802, 2008.

[4] A. Nadeem and M. Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs," *International Conference on Communications and Mobile Computing*, Leipzig, Germany, 2009.

[5] W. Ren, D.-Y. Yeung, H. Jin, and M. Yang, "Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks," *International Journal of Network Security*, Vol. 4, No. 2, Mar. 2007.

[6] M. Alicherry, A. D. Keromytis, and A. Stavrou, "Evaluating a Collaborative Defense Architecture for MANETs," *IEEE Workshop on Collaborative Security Technologies* (CoSec), December 2009.

[7] M. Carvalho, "Security in Mobile Ad Hoc Networks," *IEEE Security & Privacy*, March/April 2008.

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

[9] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol," *RFC 4728*, Feb. 2007.

[10] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA)," draft-ietf-manet-tora-spec-00.txt.

[11] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," *RFC3626*, Oct. 2003.

[12] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," *RFC3684*, Feb. 2004.

[13] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM *SIGCOMM Computer Communication Review*, Vol. 24, Issue 4, Oct. 1994.

[14] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Network and Distributed System Security Symposium (NDSS)*, San Diego, California, February 2003.

[15] P. Gupta and P. R. Kumar, "A system and Traffic Dependent Adaptive Routing Algorithm for Ad Hoc Networks," *the 36th IEEE Conference on Decision and Control*, San Diego, California, Dec. 10 -12, 1997.

[16] S. Yi, P. Naldurg, and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," *ACM Symposium on Mobile Ad Hoc Networking & Computing (MOBIHOC 2002)*, Lausanne, Switzerland, June 9 – 11, 2002.

[17] Y. Liu and L. Shen, "Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks," *Computer Knowledge and Technology 2007 3(16)*, 2007.

[18] J. Wang, X. Liu, and A. Chien, "Empirical Study of Tolerating Denial-of-Service Attacks with a Proxy Network," *the 14th USENIX Security Symposium*, Baltimore, MD, USA, July 31 – Aug. 5, 2005.