Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs

Po-Chun TSOU*, Jian-Ming CHANG**, Yi-Hsuan LIN***, Han-Chieh CHAO*, Jiann-Liang CHEN****

* Institute of Computer Science and Information Engineering,
National Ilan University,Taiwan, R.O.C
**Department of Computer Science and Information Engineering,
National Dong Hwa University, Taiwan, R.O.C
***Department of Electronic Engineering, National Ilan University, Taiwan, R.O.C
****Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan, R.O.C

R9843011@niu.edu.tw, a0128866@ms62.hinet.net, zzzaaa12@gmail.com, hcc@niu.edu.tw, Lchen@mail.ntust.edu.tw

Abstract— **In recent year with the widespread use of mobile device, Mobile Ad hoc networks (MANETs) technology has been attracted attention day by day. Due to MANETs don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANETs suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANETs, infrastructure-less property and lack of certificate authority make the security problems of MANETs need to pay more attention. The common routing protocols in current such as DSR AODV and so on almost take account in performance. They don't have the related mechanism about detection and response. Therefore, we proposed a DSR based secure routing protocol in this paper, named BDSR (Baited-Black-hole DSR). The BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture in MANET by using the virtual and non-existent destination address to bait the malicious node to reply RREP.**

Keywords— **MANETs, DSR, Baited-Black-hole DSR, Black hole attack**

I. INTRODUCTION

MANETs [1] is a kind of point to point transmission type and is a group of mobile nodes communicate with each other by wireless. Each node among the MANETs not only works as a host but also need to play the role of router. While receiving data, nodes also need to help other nodes to forward packets, thereby forming a wireless local area network. However, the security of this particular network environment has many defects. In addition to the drawback of using radio wave to transmit in nature, there are still many problems, such as limited power, lower computing ability, and dynamic topology and so on. These problems make the security of MANET lower than cable network and produce many security issues.

The DSR [2] is an on-demand routing and it is composed of two main processes: Route Discovery and Route Maintenance. When source node want to send a packet to a destination, if there are no related routing information in source node's routing cache, the source node will start the Route Discovery process. In order to execute Route Discovery, the source node broadcasts a Route Request packet (RREQ) through all networks. As all intermediate nodes receive RREQ packet, they check the source address and Request ID within RREQ and judge if received the same packet. If the intermediate nodes receive the same RREQ, it will be discarded, or it will be updated. If the intermediate node has routing information to the destination, it will reply Route reply packet (RREP) to source node, or all nodes that receives packet will keep forwarding RREQ to their neighbors. When RREQ forwards to a node, the node add itself address information into the RREQ packet. Therefore when destination receives RREQ, it can know the entire intermediate node address among the route. The destination node can depend on the routing information among the packet to reply RREP to source node and make source node has the whole routing information of this route. Route Maintenance is the process that maintain by the source node. When the network topology has changed or the connection failed occurs, the source node is informed by Route Error packet (RERR). Then the source node uses another route to destination that exists in route cache or restart Route Discovery process to find a new route again.

Because the communication of MANETs uses the open medium, attacker can easily overhear message that are transmitted. The design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make

MANETs are vulnerable to several types of attacks. One of common attack is Black hole attack [3] that is a malicious node can attract all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination. This is depicted in Figure 1. Black hole attack is a kind of Denial-of-Service attacks [3] and derive Gray hole attack [3], a variant of black hole that selectively discards and forwards data packets when packets go through it. Cooperative black hole attacks [3] mean several malicious nodes cooperate with each other and work just like a group. This kind of attack results in many detecting methods fail and causes more immense harm to all network.

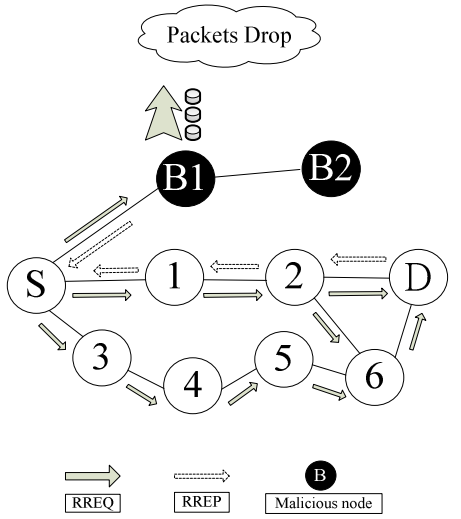

Figure 1. Black hole attack

Therefore, we propose BDSR which merges proactive and reactive defense architecture in MANET. The BDSR bait the malicious node to reply RREP by using a virtual and non-existent destination address. Finally the detected black hole node is listed in the black hole list and notices all other nodes in the network to stop any communication with them. As a result our proposal can reduce packets loss that cause by the malicious nodes and have better packet delivery ratio.

The rest of the paper is organized as follows. In section II, we introduce the background and related work. The detecting and avoid mechanism that we proposed is presented in section III. Next, in section IV we discuss and analysis the simulation result. Finally, the conclusion and future work is depicted in section V.

II. RELATE WORK

In recent years, researchers propose different solutions about black hole problem. However, most these methods just can detect single malicious node or need to cost much time and resource to detect cooperative black hole. Even these methods require specific environment to perform. In this paper we collect and introduce the mechanisms that are proposed in recent years.

William Kozma Jr et al. [4] propose a REAct system to detecting malicious node. When destination node detects a heavy packet drop, the feedback message will be sent back to source node to trigger the audit procedure. Then the source node will choose an audit node to use bloom filter to generate behavioral proof. The source node also uses bloom filter to produce behavioral proof and compare with the bloom filter that generate by the audit node. And according to the compared result to judge the segment that has the malicious node. However, the behavioral proof that generated by the bloom filter contains only the information of transmitted packets but not the information of nodes on the forwarding path. In [5], Weichao Wang et al. argues that this system may result the source node cannot identify which node on the path generates the proof. If REAct system suffers cooperative attacks, it cannot work on. Another cooperative attacker would generate the proof and transmit it to audit node. Therefore the proof would cheat the system that the malicious node is in another segment of the path. So, this system just can detect single malicious node. On the other hand, the method using binary search to find the malicious node may results the attacker can predict the audit node easily and change its behavior to cheat the source node.

Weichao Wang et al. [5] present an approach for adding hash based into REAct system. Let the behavioral proof can contain both information from data traffic and forwarding paths. Both of them take into account to help source node to detect malicious node. The above two papers depict that the detecting mechanism trigger only when the destination node detects significant drop in packet delivery ratio. In other word, the overhead of the mechanism only produces when the path exist malicious node and the malicious node begins to attack. However, these approaches still make MANETs to suffer packets loss in initial stage and result some harm to network. This kind of detecting mechanism belongs to reactive method.

Hongmei Deng et al. [6] propose a methodology which asks every intermediate node to send back next hop information among the RREP when they have the route to destination. While receiving RREP, the source node does not transmit data packets to intermediate node immediately. The source node according to the receiving information of next hop sends FutherRequest to the next hop and ask if exists route between it and the intermediate node and whether it has route to destination. The source receives FutherReply from the next hop. If the answers both are yes, the route is built. If the answer is no, the source node will send Alarm Packet to alarm other node among the network. Nevertheless, this methodology has an obvious drawback is that it only can address single black hole. It cannot face cooperative black hole attacks because the next hop colludes with the former. As a result the source gets wrong message.

Huirong Fu et al. [7] [8] stretch [6] and present an algorithm for preventing the cooperative black hole attacks. The algorithm main use the process of cross checking the intermediate nodes among the route and every nodes maintain a DRI table by monitor the neighbors. The source node compares the DRI table to judge the behavior of malicious node. Although the process of cross checking can sure all nodes be checked, the overhead and end to end delay would

higher than other approach. The DRI table use 0,1 to record the neighbors whether forwarding packets. However, if the black hole does not discards all packets that the malicious node would be difficult to detect.

Vishnu K et al. [9] propose to use the concept of Backbone network [10]. Backbone nodes (BBN) are a group of nodes which are powerful in terms of battery and range. Backbone network is formed with these nodes which are permitted to allocate Restricted IP addresses (RIP) to newly arrived nodes. The author assumes that the environment is in Backbone network. When source node wants to transmit data, it asks the nearest BBN for an unused RIP. Then the source node transmits RREQ to both destination and RIP. If the source node just receives the RREP from destination, this situation means the network is regular and safe. If the source receives RREP from RIP; however, this situation means there are black hole in this route. Therefore, the source node sends monitor message to alarm the neighbor node to go into promiscuous mode and let them start to listen the network. The source would send some dummy data packets to destination. As the same time the neighbor node can monitor the situation of the forwarding packets. If the packet loss of the monitored node beyond the normal case, the neighbor node would notices source node the situation. The source node would identify the monitored node as black hole by receiving the responded messages of the neighbors. The network environment is assumed that the normal nodes are more than the malicious nodes. So, the neighbor nodes may report fail message when the malicious nodes are more than normal node and the malicious nodes cooperate together. This result in the source node cannot know the exact locations of the malicious nodes. On the other hand, the original design of MANETs does not have Backbone network, therefore this concept and method only can suit special environment. If we only use the method of RIP, the method cannot lock the black hole and remain need to monitor and observe the suspicious node.

Marti et al. [11] presents a method in which contain Watchdog and Pathrater for detecting black hole. The Watchdog use neighbor nodes to overhear and detect malicious node. Watchdog depends on overhearing the packets whether be discarded deliberately to identify the malicious node. Pathrater give each node a default value at first, and then keep observing the transmitted behavior of each node. The value will change according to the transmitted behavior. After a period of time if the value is below the threshold, the node will list to black hole list. These methods have the same defect to find malicious node, when the neighbor reply wrong observing message. In other word, these methods cannot handle collaborative attacks. Because the neighbors collude each other may result in misjudging. Furthermore, [11] and [6] [7] [8] belong to the same type of proactive detection methods which need to constantly monitor nearby nodes. Regardless of the existence of malicious nodes, the overhead of detection will constantly create and the using resource of the detection will constantly waste.

III. BDSR MECHANISM

In this paper, we proposed a DSR based secure routing protocol, named BDSR (Baited-Black-hole DSR) which can detect and avoid the black hole attack. BDSR uses the concept of sending bait and attract black hole to reply the fake routing information. Therefore, it can achieve proactive detection and trace back the route to exact location of the existing black hole in the initial stage. That can reduce the opportunity of suffer black hole attack after the establishment of the route. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again [4] [5], which can achieve the capability of maintenance and immediately reactive response. Accordingly, our proposal merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, our mechanism doesn't like the method that just use reactive architecture would suffer black hole attack in initial stage.

Although DSR can know the all address of nodes among the route after the source node receives the RREP. However, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss. Compared with DSR, our BDSR modify DSR's packet format of RREQ and RREP to help BDSR detect malicious node. In terms of RREP, we change the Reserved field to Record address field that will record which node start to reply RREP. The Record address field stores the address of node that replies RREP. The Record address field can help to trace the intermediate node which claims that it has the shortest route to the destination node. In addition, BDSR increase RREQ' packet that are the same with original RREQ packet format except its Target address field use a address that is random, virtual and non-existent. Table I, II are the modified packet format.

TABLE I. PACKET FORMAT OF RREP

Option Type	Opt Data Len	L	**Record address**
Address[1]			
Address[2]			
…			
Address[n]			

TABLE II. PACKET FORMAT OF RREQ AND RREQ'

Option Type	Opt Data Len	Request ID
Target Address(**RREQ': Visual and not existed**)		
Address[1]		
Address[2]		
…		
Address[n]		

The detail process of detecting mechanism describe as below. When source node initializes Route Discovery, it sends out the bait RREQ'. The Target address of RREQ' is random, virtual and non-existent. In order to avoid the network is full of RREQ', BDSR use the same method as RREQ of DSR. The RREQ' could only survive a period of time. We take advantage of black hole's feature that it would fake shortest route information and reply the information to source node directly. Baiting black hole node replies RREP by the above mentioned mechanism. Because RREP has the ability of showing the address of malicious node after modifying by us, it is able to wipe out malicious node among the network in the initial period. Sending bait RREQ' and receiving the reply from malicious node that claims it has route information to the virtual and non-existent address depict as Figure 2.

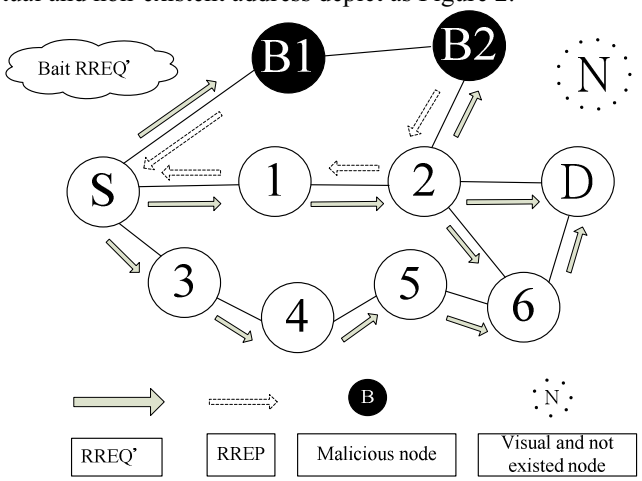

Figure 2. Send bait RREQ'

When source node detects that fake RREP reply from the virtual destination address or from the intermediate node which claim that they have the shortest route to the virtual destination address, the source node will judge that malicious nodes must exist among the replied route, and therefore trigger the adverse trace procedure. Due to our mechanism reply RREP and record the address of generating the RREP packet simultaneously. Therefore, we are able to trace which node sends back the RREP according to RREP packet's Record address field. In other words, the black hole is recognized and detected the location of black hole by source node when receiving the fake RREP. Then the detected black hole node is listed in the black hole list and noticed all other nodes to revoke the certificates of black hole by propagating Alarm packets through the network. Further any responses from black hole are discarded.

After Initial bait RREQ' process, the system Start regular DSR route discovery procedure. If destination node detects that packet delivery ratio drop to a threshold obviously after the route had been build, the detecting mechanism will be triggered again to avoid some black hole that does not detect. Consequently, our mechanism can keep protecting and reacting immediately. The threshold is a variable value that is able to adjust depended on the performance of network. In the experimental environment of our mechanism, the threshold is assigned 90%. The flowchart of we proposed mechanism is described as Figure 3. Figure 4 is our algorithm to bait black hole attack in MANETs.

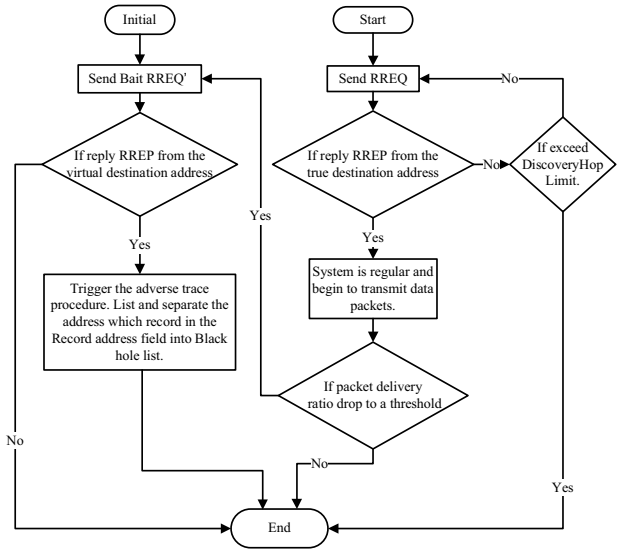

Figure 3. Flowchart of BDSR

Algorithm to bait black hole attack in MANETs
Notations :
SN: Source Node IN: Intermediate Node
DN: Destination Node

```
1. Initial( ){
2. SN broadcasts RREQ'(Visual and not existed target address);
3. SN receives RREP;
4. If (RREP is from Visual and not existed DN or IN){
5. Check for black hole using the Record address field of RREP;
6. Who send back RREP is a black hole;
7. Build black hole list;
8. Start( ){
9. Start normal DSR route discovery and maintain process;
10. Route data packets;
11. If(the packet delivery ratio is down to a Threshold)
12. Initial( );
13.          }
14. }
15.else {
16.    The nodes among the topology are safe;
17.    Start( );
18.      }
19. }
```

Figure 4. Algorithm to bait black hole attack in MANETs

Although malicious nodes cooperate and cover with each other caused such as the neighbor nodes of Watchdog [11] does not reply correctly monitoring message or the method which using the next node to check the previous node [6] doesn't work effectively under these cooperant nodes. However this paper proposes mechanism that doesn't use common method, for instance, using neighbor node to monitor [9] [11], pathrater [11] or adopting trust based relationship between nodes, our mechanism does not mislead by malicious

node. Moreover, neither does our mechanism like [9] [10] that need the special environment of semi-centralized or backbone network in MANETs nor [4] [5] that require a serious of computation. BDSR is a more comprehensive detecting mechanism which is a proactive detection in the initial stage and then turn into immediately reactive response in usual period. Adding the proactive detection portion can avoid that still stuff the chance of black hole attack in the initial stage if the detecting mechanism just purely uses reactive response detection. When the initial proactive detection stage finish, the detection become reactive response. Therefore, our BDSR would not have much extra overhead in MANETs. BDSR merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, BDSR avoids the drawbacks of using only one of the two methods.

IV. SIMULATION AND ANALYSIS

The simulation is being implemented in the QualNET simulator [12]. We adopt the same simulation parameter and experiment environment as Marti et al. proposed Watchdog, Pathrater, and SRR [11]. We use "Watchdog" to stand for the all mechanism proposed by Marti et al.

TABLE III. SIMULATION PARAMETERS

Parameter	Value
Application traffic	CBR
Radio range	250m
Packet size	64 bytes
Transmission rate	4 packets/s
Pause time	0s/60s
Speed	Random(0-20m/s)
Simulation time	200s
Number of nodes	50
Area	670m*670m

The simulation parameters are provided in Table III. There are 6 source nodes in the experiment environment. 4 nodes among the 6 source nodes are two connections each, and 2 nodes of the others are one connection each. Another 8 destination nodes receive only one flow and the 9th destination nodes receives two flow. We randomly choose malicious nodes to perform black hole attack and vary the percentage of the network comprised of malicious nodes from 0% to 40% in 5% increments. The simulation scenarios are separated into pause time 0 and 60 seconds. Then we compared DSR, Watchdog with our BDSR on the performance of packet delivery ratio and overhead in the two scenarios.

Figure 5 and Figure 6 illustrate the impact of the malicious nodes on packet delivery ratio for all protocols. First, as these figures depict, DSR heavily suffer from increasing black hole attacks since it does not have any detecting and protecting mechanism to prevent black hole attacks. Second, although Watchdog uses neighbor node to monitor and detect malicious node, neighbor node may reply wrong or fake message that they monitor when malicious node increase more and more. Therefore, the packet delivery ratio of Watchdog is affected and went down obviously. When varying the percentage of the network comprised of malicious nodes from 0% to 40%. Our protocol BDSR gives higher and smoother packet delivery ratio than the other two protocols since BDSR will send bait packet to bait malicious node to reply and then trace the location of the black hole in the initial stage.

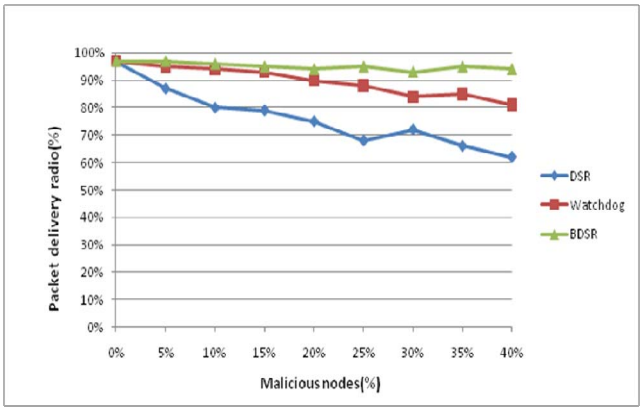

Figure 5. Comparison of Packet Delivery Ratio (0 Second Pause Time)

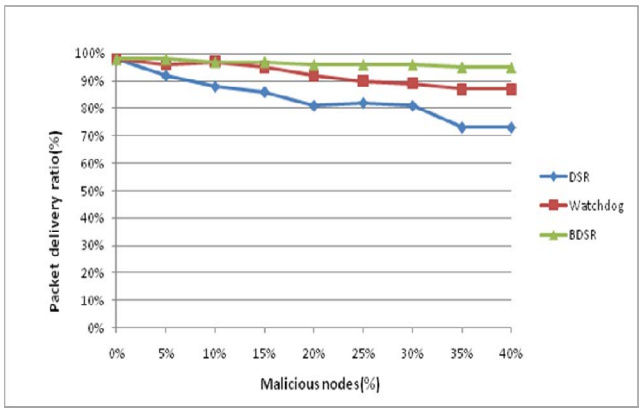

Figure 6. Comparison of Packet Delivery Ratio (60 Second Pause Time)

Figure 7 and Figure 8 demonstrate the impact of the increasing malicious nodes on overhead. First, when the malicious nodes ratio increases, DSR introduces the lowest overhead since it does not has any extra secure mechanism or defensive method. Second, Watchdog belongs to proactively detecting method which needs to constantly monitor nearby nodes. Therefore, regardless of the existence of malicious nodes, the overhead of detection and monitor will constantly create and the resource of the detection will constantly waste. Nevertheless, our protocol BDSR is able to achieve proactive detection in the initial stage and then change into reactive response in usual stage. By this way we can merge the advantage of proactive detection and the superiority of reactive response that reduce the waste of resource.

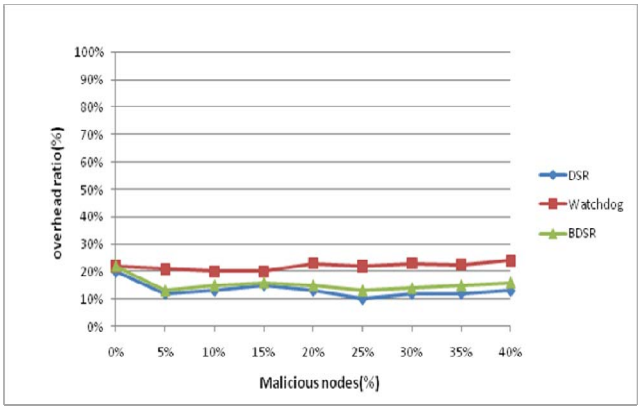

Figure 7. Comparison of Overhead (0 s Second Pause Time)

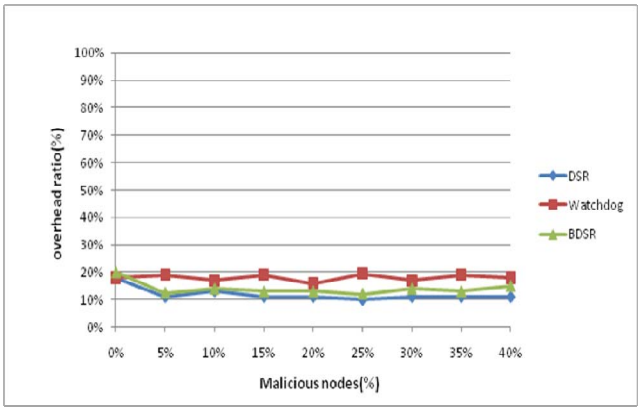

Figure 8. Comparison of Overhead (60 s Second Pause Time)

V. CONCLUSIONS

In this paper we proposed a DSR based secure routing protocol, named BDSR (Baited-Black-hole DSR). The BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture in MANETs by using the virtual and non-existent destination address to bait the malicious node to reply RREP. Our proposal merges the advantage of proactive detection that can avoid just using reactive architecture would suffer black hole attack in initial stage and the superiority of reactive response that can reduce the waste of resource. We simulate our proposed solution using the QualNet simulator and compare BDSR with Watchdog, and DSR in terms of packet delivery ratio and overhead. Simulation results show that BDSR presents good performance in terms of better packet delivery ratio and not much overhead to network overhead.

In the future work, in order to enhance and verify BDSR we will keep study and experiment our protocol to resist cooperative black hole attacks and gray hole attack.

ACKNOWLEDGMENT

This work was supported in part by the Program of Integrated Actions (PIA) ORCHID, under contract “NSC 98-2911-I-197-001”.

REFERENCES

[1] RFC 2501, http://www.faqs.org/rfcs/rfc2501.html.
[2] RFC 4728, http://www.faqs.org/rfcs/rfc4728.html.
[3] A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journal of Computer Science and Information Security," Vol. 7, No. 1, 2010.
[4] W. Kozma, and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009.
[5] W. Wang, B.Bhargava, and M. Linderman, “Defending against Collaborative Packet Drop Attacks on MANETs,” 28th International Symposium on Reliable Distributed Systems September 2009.
[6] H. Deng, W. Li, and D. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magazine, Vol. 40, No. 10, October 2002.
[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J.Dixon, and K. Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,” 2003 International Conference on Wireless Networks (ICWN’03), June 2003.
[8] H. Weerasinghe and H. Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation,” IEEE International Conference on Communication, 2007.
[9] V. K and A. J PAUL, “Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks,” 2010 International Journal of Computer Applications, Vol. 1, No.22, 2010.
[10] I. Rubin, A. Behzad, R. Zhang, H. Luo and E. Caballero, “TBONE: A Mobile-Backbone Protocol for Ad Hoc Wireless Networks,” In Proceedings of IEEE Aerospace Conference, Vol. 6, pp. 2727-2740, 2002.
[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.
[12] Scalable Network Technologies (SNT). QualNet. http://www.qualnet.com/.