Reputation Based Intrusion Detection System with Threshold Cryptography for Wireless Mobile Ad Hoc Networks

*Chih-Hung Wang and Shan Chin
Department of Computer Science and Information Engineering, National Chiayi University, Taiwan, R.O.C.
**whangch@mail.ncyu.edu.tw*

Abstract*- In recent years ad hoc networks are becoming an important research due to the self-organization network, dynamically changing topology, temporary network life and equal relationship among member of nodes. However, some of the properties of ad hoc network make the security problem more serious. DoS (Denial of service) attack is the most popular attack of the security problem, which can decrease the network performance or consume the resource of the network. The most famous DoS attacks are Black Hole attack and Flooding attack. Several methods proposed to defend these attacks can be classified into two types: authentication based technique and observation based technique. In this paper, we propose a reputation based intrusion detection system (RIDS) which combines the advantages of the above two techniques to achieve high performance and less computation and control packet overheads.*

Keywords: Mobile Ad Hoc Networks, AODV, DoS, Black Hole, Network Security.

1. Introduction

A mobile ad hoc network (MANET) is a self-configuring network established automatically by collecting mobile nodes without any assistance of fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order to forward a packet from a node to another node that is out of its radio range, the cooperation of other nodes in the network is needed. Many ad hoc routing protocols have been proposed but only AODV (Ad hoc on-demand distance vector) routing protocol [3] is widely used in MANETs for its high efficiency, low control overhead and simplicity. Unfortunately, AODV is vulnerable to many attacks such as black hole attacks, flooding attacks and other kinds of denial of service attacks, which will cause huge damage on MANETs. These attacks may not only decrease the network performance but also consume lots of resource such as memory and energy. For above reasons, intrusion detection system (IDS) is proposed to avoid the attacks on MANETs. The IDS belonging to the observation based technique does not need lots of computation overheads. By using some specific monitoring nodes, the system can detect the malicious nodes and isolate them. But the observation based IDS may raise a serious security problem if some malicious nodes are selected as the monitoring nodes. A group of malicious nodes can collude with each other to launch a bad mouthing attack by falsely accusing a legitimate node and isolating it from the network. For this reason, authentication based technique is still important to avoid this kind of attack. Zhou and Haas [13] proposed some mechanisms based on authentication technique and used a threshold cryptography method to avoid the bad mouthing attack. In this paper, we propose a reputation based technique similar to Routeguard's model [5]. But our implementation only uses a small amount of monitoring nodes instead of setting all nodes as the monitoring nodes, which can achieve both distributed and cooperative advantages. Moreover, we conduct the hierarchical technique by using the threshold cryptography technique which only increases less computational overheads on a master node. The master node is used to collect the blacklist of other monitoring nodes. Of course, the blacklist of the monitoring node will be signed with its private key to avoid modifications and fabrications. With this technique, we can avoid bad mouthing attack that Routeguard [5] cannot avoid. In this case, we can make the network more secure in just taking a few extra computational costs.

This paper is organized as follows. In Section 2, some related researches of routing security in MANETs are discribed. Then, the flooding attacks and black hole attacks on AODV protocol are discussed in Section 3. In Section 4, we describe the details of our proposed reputation based intrusion detection system with threshold cryptography, and in Section 5, we present the simulations on the proposed scheme by ns-2 and analyze its performance. Finally, we close the paper with our conclusions and discussions of the future work in Section 6.

2. Related Work

In this section, we discuss some previous schemes proposed to detect several kinds of denial of service attacks. In the beginning of this section, we discuss authentication based technique such as [10] and [13]. This kind of IDS can ensure that the protocol is secure as long as the secret key has not been compromised. Although this kind of IDS is free from spoofing attack, it has a critical drawback of high computational time. Security is important to the wireless mobile ad hoc network, but performance is more important. Hence, threshold cryptography technique was proposed in [10] for high performance, and that's why we employ this technique to our scheme.

Another kind of technique called observation based IDS, detects malicious nodes or packets by neighborhood observation. Several schemes [1][2][3][4][5][6][7][11][12] have been proposed in recent years. Some of them [2][4][6] used the methods like probabilities and statistics, or training techniques as in the traditional IDSs of wired networks. The others [1][3][5][7][11][12] used some methods particularly suitable for wireless networks like reputation, cross layers or multi agent techniques. Unfortunately, all of them do not consider the bad mouthing attack that may cause huge amount of false alarms and decrease the network performance. Moreover, flooding attack and black hole attack are also important and we will describe them in the next section.

3. Flooding Attack and Black Hole Attack on AODV Protocol

In this section, we describe the flooding attack and black hole attack similar to [9]. However, these attacks in different papers may have different definitions.

3.1. Flooding Attack

The flooding attack is defined that an attacker floods lots of RREQ control packets in order to consume the resource of the network. Here we redefine the number of RREQ retries to 100 and maximum RREQ timeout to 0 second; moreover we also redefine the RREP waiting time to 0. A malicious node just forwards RREQ packets and ignores any checking mechanism, hence the node will send huge amount of RREQ packets during attack process. We modify the times of RREQ retries, max RREQ timeout, network diameter, and RREP waiting time to simulate this attack.

3.2. Black Hole Attack

In the black hole attack, an attacker may use a modified RREQ or RREP control packets with a non-existent node as the source IP address in the IP header. Then, the originating node will update its route to go through the non-existent node to the destination node. As a result, the route will be broken.

3.2.1. Black hole Attack caused by modified RREQ

Suppose node S broadcasts a RREQ message to establish a route to the node D. After receiving the RREQ message, the attacker modifies the RREQ message as follows [9]:

(1) Replace the RREQ ID of node S with the RREQ ID of node D, and increase it by a small number.
(2) Interchange the source IP address (node S) with the destination IP address (node D) in the RREQ message.
(3) Increment the destination sequence number by at least one, and then interchange the source sequence number with the destination sequence number.
(4) Fill source IP address in IP header with a non-existent IP address.

3.2.2. Black hole Attack caused by modified RREP

After receiving a RREQ message, the attacker may forge a RREP message as if it had a fresh enough route to the destination node. In order to suppress other legitimate RREP messages that the source node may receive from the other nodes, the attacker may forge a faked RREP message in the following way [9]:

(1) Set the destination IP address to the destination node's IP address.
(2) Set the source IP address to the source node's IP address.
(3) Set the source IP address in the IP header to a non-existent IP address.
(4) Set the destination IP address in the IP header to the node from the RREQ message which

the attacker receives.

(5) Increase the destination sequence number by at least one, or decrease the hop count to 0.

4. Reputation Based Intrusion Detection System

In this section, the details of the proposed reputation intrusion detection system with threshold cryptography are described. The system is divided by three parts: Local Anomaly Detection, Local Reputation System and Global Response with Threshold Cryptography.

4.1 Local Anomaly Detection

Here, we describe the local anomaly detection for the three kinds of attacks we introduced in Section 3. The detecting procedure for the RREQ flooding attack is shown in Figure 1. When a monitoring node receives a packet broadcasted from a node, it will observe all the other packets from this observed node for a period of time to check if the node broadcasts too many requests. A threshold value is used to measure if the observed node is executing a flooding attack. We used a method by counting the number of the RREQs to check if the counting value exceeds the threshold. If it does, the monitoring node will decrease the flood value (FV) of the broadcast node by 4 and drop the packet. This behavior is called suspicious dropping. Otherwise, FV of the broadcast node will be decreased by 1 and after a period of time the state will move to the local reputation system.

The black hole attack of local anomaly detection is shown as Figure 2 and Figure 3. Figure 2 is shown for detecting black hole attack caused by RREQ and Figure3 is shown for detecting black hole attack caused by RREP. In the beginning of this detection, when a monitoring node receives a RREQ control packet, it will store the RREQ destination IP and the destination sequence number. Moreover, when the monitoring node receives a RREP control packet, it will also store the destination sequence number and creates a RREQ-RREP sequence number table as Table1.

Figure 2 is a flow chart for detecting black hole attack caused by faked RREQs. When a monitoring node receives a packet, it first checks if the source IP address in the IP header is in its neighboring list. If finding a match, the monitoring node will forward the packet; otherwise it will check the difference between current destination sequence number and the previous destination sequence number related to the same destination IP. If the difference value is lager than a threshold, the monitoring node will decrease the RREQBH value of the preceding node by 1 and suspicious drop the packet; otherwise it will forward the packet. As flooding attack detection method, after a period of time, the state will move to the local reputation system.

After discussing the local detection of black hole attack caused by RREQ, now we discuss the local detection of black hole attack caused by RREP shown in Figure 3. When a monitoring node receives a RREP control packet, it first checks if it had received any RREP packet from the same destination IP of the preceding node. If it finds a match, it will check the difference between the current RREP destination sequence number and the previous destination sequence number. If the difference value is over a threshold, it will decrease the RREPBH value of the preceding node by 5 and suspicious drop the packet, otherwise increase the RREPBH value of the preceding node by 1 and forward the packet. If the monitoring node does not find a match, which means it receives the RREP control packet of the destination IP from the preceding node for the first time (ex: the third row in Table 1), it will check the RREQ-RREP sequence number table. If the difference value between the destination sequence number in the RREP packet and the destination sequence number in the last received RREQ exceeds a threshold, the monitoring node will decrease the RREPBH value of the preceding node by 5 and suspicious drop the packet. Otherwise, the monitoring node will increase the RREPBH value of the preceding node by 1 and forward the packet. Then, the same to above, after a period of time the state will move to the local reputation system.

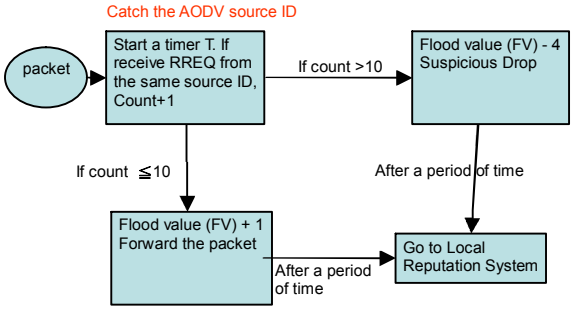

Figure 1: Local Anomaly detection for flooding attack

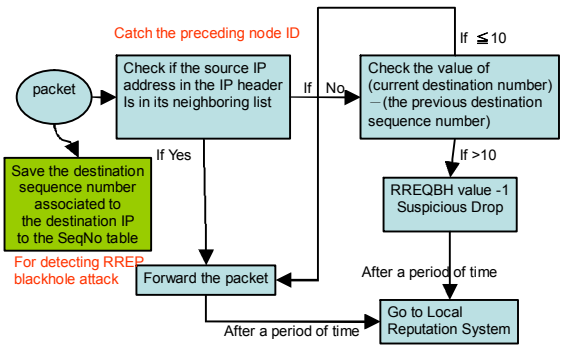

Figure 2: Local Anomaly detection for blackhole attack caused by RREQ

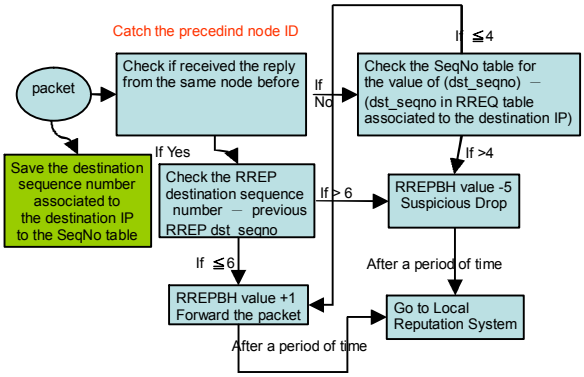

Figure 3: Local Anomaly detection for blackhole attack caused by RREP

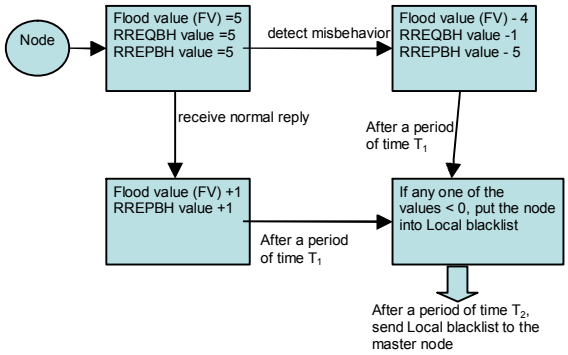

Figure 4: Local Reputation System

Table1. RREQ-RREP sequence number table

RREQ / RREP Destination IP	Previous RREQ Destination Sequence number	Previous RREP Destination Sequence number
0	2	3
1	4	5
2	4	-
: .	: .	: .

4.2 Local Reputation System

Now, we discuss about the local reputation system shown in Figure 4. In the beginning, each node has three values (flooding value, RREQBH value, and RREPBH value) and all are initialized to 5. When the local detection system detects a node with suspicious behaviors, it will decrease the reputation of the node by different values as shown in Figure 4. Of course, if the system detects the node with normal behavior, it will increase the reputation value of the node by 1. Then, after a period of time T_1, the monitoring node will observe the three kinds of values to check if any one of the values is below zero. If the monitoring node finds that, it will put the node into its local blacklist and after a period of time T_2, send its local blacklist to the master node and execute the global response.

4.3 Global Response with Threshold Cryptography

The global response with threshold cryptography is shown in Figure 5. The master node can be elected by a specific way or using a monitor election protocol proposed by Madhavi [8]. When a node was set into the local blacklist by a monitoring node, it cannot perform any operations except for forwarding normal data packets. All the monitoring nodes will send their local blacklist to the master node after a period of time T_2. The master node will integrate all the blacklists of monitoring nodes. If a certain node is placed in more than *k* monitoring nodes' local blacklists, this node will be sent to the global response to notify all the monitoring nodes putting the node to their global blacklist. Otherwise, the master node will unblock the node. The transmission security here is based on the digital signature method; that is, each node uses its private key to sign the local blacklist. The encryption and decryption computations are only applied to the blacklist transmissions belonging to data packets instead of control packets. As long as the time T_2 is not too short, these cryptography operations will not cause too much overhead. Here we discuss the global response with threshold cryptography in order to avoid the bad mouthing attack. If several malicious nodes spoof as the monitoring nodes and circumvent a legitimate node, this will cause huge amount of false alarms and the performance of the network will be decreased.

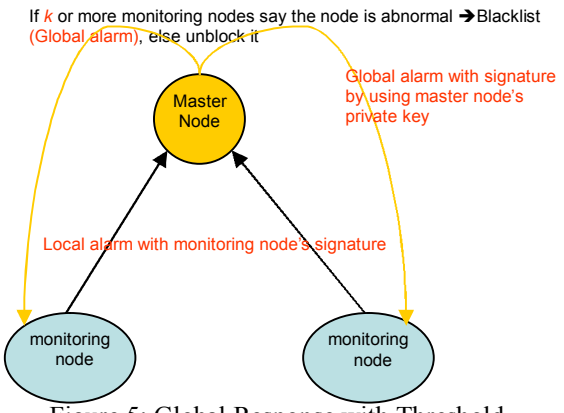

Figure 5: Global Response with Threshold Cryptography

5. Simulation and Results

In this section, we describe the performance metrics, the simulation setup, and the simulation results.

5.1 Performance Metrics

Here, we describe our performance metrics as follows:

(a) throughput:

$$\text{throughput} = \frac{\text{number of data packets sent by the source nodes}}{\text{number of data packets received by the destination nodes}}$$

(b) suspicious dropping:

$$\text{suspicious dropping} = \frac{\text{number of normal control packets suspicious dropped by monitoring nodes}}{\text{number of normal control packets received by monitoring nodes}}$$

(c) control packet overhead : number of control packets.

5.2 Simulation Setup and Results

In the experiment, we use ns-2 ver.2.29 with random waypoint model to simulate our proposed RIDS. The parameters are listed in Table 2. The attack node is allowed to perform RREQ flooding attack, and black hole attack caused by RREQ and RREP. First, we select a monitoring node near the malicious node to ensure that the malicious node can be observed. Then we randomly select monitoring nodes limited to the number of 3, 6, 9 and 12 and show the throughput, suspicious dropping and control packet overhead in Figure 6, Figure 7, and Figure 8, respectively.

In Figure6, we can see when the protocol is under attack, the throughput will decrease. With the number of monitoring nodes increasing, the throughput will also increase. Moreover, Figure 7 shows the false suspicious dropping rate. From Figure 7, we can see the false suspicious dropping rate and number of monitoring nodes are in a direct proportion. Although the false suspicious dropping increases with the number of monitoring nodes, it is only impermanent. The final blacklist will be corrected by the master node using the global response system. In Figure 8, we can see the number of control packets increases when the protocol is under attack. That is because the attack behaviors will interdict the route being created that will cause the source node need to broadcast more control packets in order to create the routes. With the number of the monitoring nodes increasing, the number of control packets will decrease due to the detection of more attack behaviors.

Finally, we show the performance comparison between the proposed RIDS and the other previous schemes in Table 3. From Table 3, we can see that the RIDS has low computational cost and no training time. Further, only partial nodes in RIDS are equipped with monitoring mechanisms. However, that can defend most of important attacks.

Table 2. Simulation parameters

Simulator	ns-2(ver. 2.29)
Simulation time	100 (s)
Number of mobile nodes	30
Number of malicious node	1
Topology	1000m × 1000m
Transmission range	250m
Routing protocol	AODV
Physical link bandwidth	2Mbps
Traffic	CBR
Packet size	512k bytes
Packet rate	4 packets/sec
Maximum connection	10
Maximum speed	10 ms
Pause time	2 sec

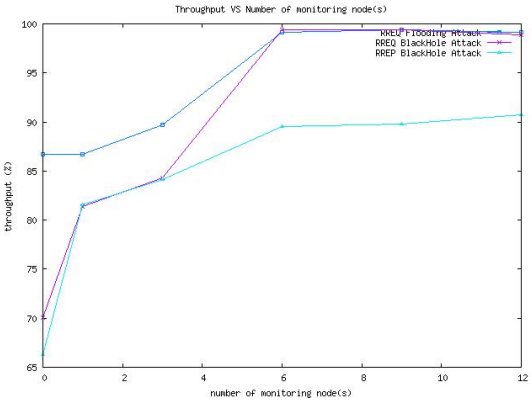

Figure 6: Throughput vs. number of monitoring node(s)

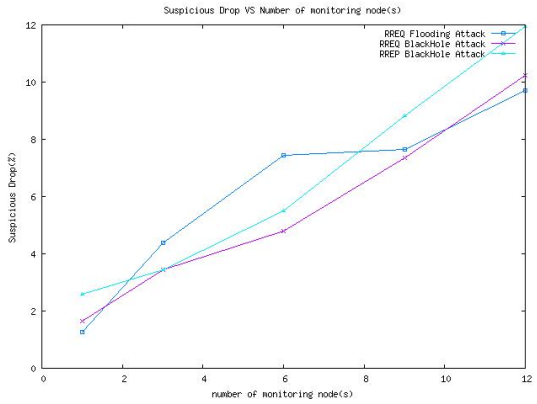

Figure 7: Suspicious dropping vs. number of monitoring node(s)

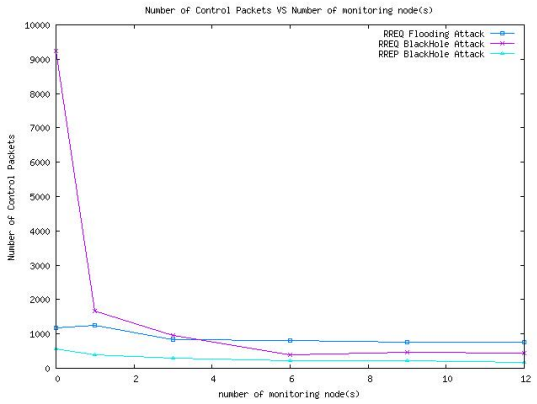

Figure 8: Number of control packets vs. number of monitoring node(s)

Table 3. Performance Comparison

	[1]	[3]	[4]	[5]	[7]	[10]	RIDS
Packet format extension	X	X	X	X	X	O	X
Computational complexity	Low	Low	Low	Low	Low	High	Low
Monitoring mechanisms	All nodes	Part nodes	Part nodes	All nodes	Part nodes	Part nodes	Part nodes
Training time	X	X	O	X	X	X	X
Ability to detect flooding attack	X	O	O	O	X	O	O
Ability to detect black hole attack	O	O	O	O	O	O	O
Ability to detect bad mouthing attack	X	X	X	X	X	O	O

6. Conclusion and Future Work

We proposed a framework of reputation based intrusion detection system with threshold cryptography to prevent the bad mouthing attacks and several types of denial of service attacks. Moreover, our scheme has low computational cost with high detection rate and throughput but only causes a little false suspicious dropping rate. The suspicious dropping rates are not the same in different traffic environments because the threshold of the suspicious dropping is adjustable. This will make our RIDS suitable for a variety of different environments by altering the threshold of suspicious dropping.

In AODV protocol, several types of active attacks also need to be considered. In the future work, we are planning to investigate other active attacks. By increasing or decreasing the threshold of suspicious dropping and the reputation value, the system will be able to detect other active attacks, but the appropriate value is not easy to find. When the different types of attacks are increasing, finding an appropriate value to get high performance and low suspicious dropping rate becomes an interesting issue.

Acknowledgement

This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 97-2219-E-006 -003.

References

[1] S. Bose and A. Kannan, “Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks,” Signal Processing, Communications and Networking, 2008. ICSCN '08. International Conference on 4-6, pp. 182 – 188, January 2008.

[2] J.B.D. Cabrera, C. Gutierrez and R.K. Mehra, “Infrastructures and algorithms for distributed anomaly-based intrusion detection in mobile ad-hoc networks,” Military Communications Conference, 2005. MILCOM 2005. IEEE 17-20, pp.1831 – 1837, October 2005.

[3] H. Chen, Z. Ji, M. Hu, Z. Fu and R. Jiang, “Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol,” Journal of Network and Computer Applications Volume: 30, Issue: 1, pp. 145-166, January, 2007.

[4] H-W. Femg and C-L. Liu, “Design of a Joint Defense System for Mobile Ad Hoc Networks,” in Proceedings of IEEE VTC 2006-Spring, Melbourne, Australia, pp.742 – 746, May, 2006.

[5] A. Hasswa, M. Zulkernine and H. Hassanein, “Routeguard：An Intrusion Detection and Response System for Mobile Ad Hoc Networks,” Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on Volume 3, 22-24, pp. 336 – 343, August 2005.

[6] Y.-A. Huang, W. Fan, W. Lee, P.S. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies,” in Proceedings of the 23th International Conference on Distributed Computing Systems, Providence, RI, pp.478 – 487, May, 2003.

[7] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method,” International Journal of Network Security, Vol.5, No.3, pp. 338 – 346, November, 2007.

[8] S. Madhavi, “An Intrusion Detection System in Mobile AdHoc Networks,” Information Security and Assurance, 2008, pp. 7 – 14, April, 2008.

[9] P. Ning , K. Sun, “How to Misuse AODV: a Case Study of Insider Attacks Against Mobile AD Hoc Routing Protocols”, Ad Hoc Networks, Volume 3, Issue 6, pp. 795-819,November, 2005.

[10] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, “Threshold-based intrusion detection in ad hoc networks and secure AODV,” Ad Hoc Networks Volume: 6, Issue: 4, pp. 578 – 599, June, 2008.

[11] G. Vigna, S. Gwalani, K. Srinivasan, E.M. Belding-Royer and R.A Kemmerer , “An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks,” Computer Security Applications Conference,2004. 20th Annual 6-10, pp. 16 – 27 December, 2004.

[12] Y. Xiao, X. Shen, and D.-Z. Du , “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” Wireless/Mobile Network Security, pp 170 – 196.

[13] L. Zhou, and Z. Haas, “Securing ad hoc network,” IEEE Network Magazine, Special issue on network security, Vol. 13, No. 6, pp. 24-30, November/December 1999.