Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure On Demand Route Routing Protocol (SODRRP) for MANET

Pradeep M Jawandhiya,
Research Scholar,
Computer Science & Engineering
PRMITR,
Badnera (M.S.), India.

Dr. M S Ali
Principal,
PRMCEM
Badnera (M.S.),
India.

Mangesh M Ghonge
Faculty,
Computer Science & Engineering,
JDIET,
Yavatmal (M.S.), India

Abstract— ***Ad-hoc networks, due to their improvised nature, are frequently established insecure environments, which makes them susceptible to attacks. These attacks are launched by participating malicious nodes against different network services. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. On Demand Route Routing Protocol (ODRRP) is a Broadcast Reply network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as ODRRP. In this paper we proposed a solution for identifying the malicious node in ODRRP protocol suffering from black hole attack.***

Keywords— ODRRP, Black Hole Attack, MANET, Destination sequence Number.

I. INTRODUCTION

An ad-hoc network has a certain characteristics, which imposes new demands on the routing protocol. The most important characteristics are the dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently, which means that we need a routing protocol that quickly adapts to topology changes. The node in an ad-hoc network can consist of laptops and personal digital assistants and are often very limited in resources such as CPU capacity, storage capacity, battery power and bandwidth, so the routing protocol should try to minimize control traffic, such as periodic update messages. Instead the routing protocol should be reactive, thus only calculate routes upon receiving a specific request. To be effective, the routing protocols have to

1) Keep the routing table up-to-date and reasonably small,
2) Choose the best route for given destination (e.g., in terms of number of hops, reliability, throughput and cost) and
3) Converge within an exchange of a small amount of messages [9].

A mobile ad-hoc network [9] is an autonomous system of mobile hosts connected with each other using multi-hop wireless links. There is no static infrastructure such as base stations, each node in the network acts as a router, forwarding data packets for other nodes, which in such a network move arbitrarily thus network topology changes frequently and unpredictably. Nodes are free to move, independent of each other, topology of such networks keep on changing dynamically which makes routing much difficult, therefore routing is one of the most concerns areas in these networks. Normal routing protocol which works well in fixed networks does not show same performance in Mobile Ad-hoc Networks. In these networks routing protocols should be more dynamic so that they quickly respond to topological changes [24]. If two hosts are not within radio range, all message communication between them must pass through one or more intermediate hosts that double as routers. The hosts are free to move around randomly, thus changing the network topology dynamically. Thus routing protocols must be adaptive and able to maintain routes in spite of the changing network connectivity. Such networks are very useful in military and other tactical applications such as emergency rescue or exploration missions, where cellular infrastructure is unavailable or unreliable. Commercial applications are also likely where there is a need for ubiquitous communication services without the presence or use of a fixed infrastructure; Examples include conferencing applications, networking intelligent devices or sensors etc. The remainder of the paper is organized as follows. Section 2 gives a brief description of the related work. Section 3 discusses problem statements. Section 4 provides the solution to blackhole attack. Section 5 presents effect of blackhole attack and proposed protocol through simulation. Section 6, gives simulation results finally, we conclude the paper in Section 7.

II. RELATED WORKS

A. Secure Routing

Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. In [4], Huet al. proposed a common key encryption system for Dynamic Source Routing (DSR) [9]. In Secure AODV (SAODV) [15] and Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [5], secure routing protocol using hash

functions have been proposed. In [13], Authenticated Routing for Ad hoc Networks (ARAN), an AODV-based secure routing protocol using public key encryption system is proposed. Hu and Perrig [6] survey the weakness and strength of various secure routing protocols. The above mentioned secure protocols can only guard against external attacks. However, for the internal attacks coming from compromised hosts could still have severe impacts on network performance and its connectivity. Therefore, detecting the internal attack launching from these compromised hosts is indispensable.

B. IDS Approaches for MANET

To protect against the blackhole attack, five methods have been proposed. In [3], the method requires the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route. In [10], the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop node toward the destination. Then, next hop node receives CREQ, and look up its cache for a route the destination. If it has one, it sends Route Confirmation Reply (CREP) to source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth-constrained. In [14], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required. Huang et al. [7] propose a method in which the packet flow is observed at each node. In this method, they define a total of 141 features with traffic related and topology related, and suggest anomaly detection means with interrelation between features. In [8], Huang et al. construct an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; modelize normal state; and detect attacks with both specification based detection and anomaly detection. In specification based detection, they simply detect attacks as deviant packet from condition defined by EFSA. Also, in anomaly detection, they define normal state and compare it with condition of EFSA and amount of statistic of transition, and then detect attacks as a deviation from those states. From the characteristics of the blackhole attack, we need to take a destination sequence number into account. In [7], feature related to the destination sequence number has not been taken into account as the feature to define the normal state. In [7], the threshold is used and the feature is defined as the number of time that the destination sequence number is greater than the threshold. However, since a destination sequence number changed depending on the network environment, up to a threshold it may be difficult to successfully discriminate between the normal state and the state where blackhole attack took place. And hence cause degradation in detection accuracy. Except the destination sequence number issue, the above mentioned approaches use static training data to define the normal state. However, we note that the MANET topology can be changed easily, and the difference in network state becomes larger by time. Furthermore, these methods cannot be applied to a network while the training has been done in another network. As a result, these methods are considered difficult in a MANET environment. To solve this problem, normal state needs to be defined using the data reflecting the trend of current situation and this leads to the idea of updating the training process within a time interval. By so doing, attack detection can be adaptively conducted even in a changing network environment.

III. PROBLEM STATEMENTS

A. Overview on ODRRP

On Demand Route Routing Protocol with broadcast reply (ODRRP) takes the advantage of both proactive and reactive routing protocol. Like proactive protocols, it maintains a routing table at each node. However, it differs from it in the way the routing table is constructed and maintained. Unlike proactive routing protocol, it does not exchange the routing table information among the nodes. The routing table at each node is built in incremental steps. Like reactive routing protocol, the source initiates route discovery only on-demand. It uses the route request (RREQ) and route reply (RREP) packet of reactive routing protocol. Routing table in our propose protocol is built during the route discovery phase and is not exchanged along the nodes.

To build routing table, it extracts necessary information from the RREQ and RREP packets. Propose protocol does not require exchange of hello message required in proactive routing protocol, needed to maintain up-to-date information. It uses the route error message of reactive routing protocol in case of link failure. A node having packet to transmit, first checks its routing table for an existence of path to destination. If an entry exists to the destination, then the packet is forwarded to the next node along the path to destination. For non existence of path, it initiates a route discovery to the destination. The structure of routing table is shown in Table 1. It consists of following three entries:

- Dest: Destination node of packet,
- Next hop: Next hop on the path to destination,
- Hop Count: Hop distance to destination from the current node,
- Bid: Broad Cast ID

Table 1: Structure of Routing Table

Dest	Next hop	Hop Count	Bid
-----	-------	----------	---------

The format of RREQ packet is shown in Figure 1. Meaning of each Field of the RREQ/RREP packet is explained below:

- Src- Source of packet.
- Dest- Destination of the packet.
- Prev node- Previous node address.
- Hop count- Noumber of hops traversed by the packet.
- Bdid- Broadcast id

Src	Dest	Prev node	Hop Count	Bdid

Figure 1: Format of RREQ/RREP Packet

The process of route discovery and routing table updates in HRP are explained below.

B. **Description of Blackhole Attack**

In ODRRP, Dst Seq is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number, and

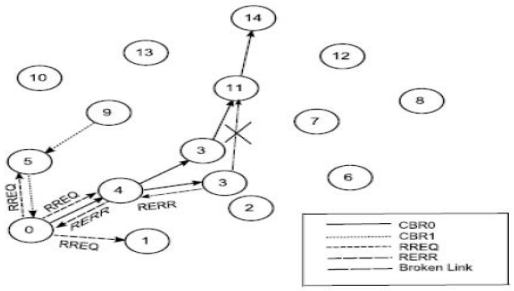

Figure 2: Route Maintenance in ODRRP

Dst Seq in the RREQ packet plus one, and then selects the larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects [1] the one with greatest Dst Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst Seq base on the received RREQ's Dst Seq. However, this RREQ's Dst Seq may not present the current Dst Seq of the destination node. Figure 3 shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in Table 1.

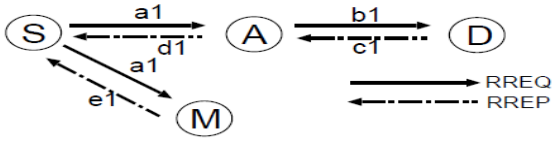

Figure 3: Blackhole attack

Table 1: Values of RREQ and RREP

	RREQ		RREP		
	a1	b1	c1	d1	e1
IP source	S	A	D	A	D(MD)
AODV.Dst	D		D		D(MD)
Dst_seq	60		61		65
AODV.Src	S		-		-

In Table 1, IP.Src indicates the node which generates or forwards a RREQ or RREP, AODV.Dst indicates the destination node and AODV.Src indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst Seq that the source node S has is 60. Hence, source node S sets its RREQ(a1) and broadcasts as shown in Table 1. Upon receiving RREQ(a1), node A forwards RREQ(b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP(e1) shown in Table 1 with IP.Src, AODV.Dst the same with D and increased Dst Seq (in this case 65 as) to source node S. At the same time, the destination node D which received RREQ(b1) sends RREP(c1) with Dst Seq incremented by one to node S. Although, the source node S receive two RREP, base on Dst Seq the RREP(e1) from the attacker M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M. Next, we consider the case shown in Figure 4. The value of RREQ and RREP using in Figure 4 are shown in Table 2. Similar to Figure 3, source node S attempts to construct a route to destination node D. However, unlike the environment in Figure 3, in this case node B, C and E are also constructing a route to D. Therefore, the destination node D's Dst Seq that the source node has is significantly different from the current Dst Seq of node D. Since the most recent Dst Seq from D

that node S has is 60, it set RREQ(a2) as shown in Table 2 and broadcasts. Upon receiving RREQ(a2),base on information contained in RREQ(a2) node M sends a spoofed RREP(e2) with Dst Seq 65 the same with previous situation to the source node. Upon receiving RREQ(b2) node D sends RREP(c2) to the source node. However, this time, since node D constructed route with other nodes, we assume that the Dst Seq is increased to 70. Then, This RREP(d2) is forwarded by node A. Upon receiving two RREP, node S selects the route to destination node D since the Dst Seq of node D is the larger one. As a result, the attack is not succeeded. For this reason, the attacker need to set Dst Seq large enough to overcome significantly changes of the Dst Seq which differed depending on the traffic condition of the destination node.

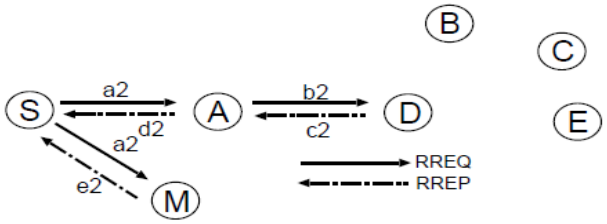

Figure 4: Blackhole attack in some connections to node D

Table 2: Values of RREQ and RREP

	RREQ		RREP		
	a2	b2	c2	d2	e2
IP source	S	A	D	A	D(MD)
AODV.Dst	D		D		D(MD)
Dst_seq	60		70		65
AODV.Src	S		-		-

IV. PROPOSED SODRRP

The Proposed method can be used to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table.

Step 1: Start the route discovery phase with the source node S.
Step 2: Store all the Route Replies Dest._Seq_No and Npde_id in Route Routing - Table
Step 3: Retrieve the first entry from Route Routing -Table
If Dest._Seq_No is much greater than Src_Seq_No then discard entry from RR-Table as
Select Dest_Seq_No from table
if (Dest_Seq_No >>>= Src_Seq_No)
{
Mali_Node=Node_Id
Discard entry from table
}
Step 4: Sort the contents of RR-Table entries according to the DSN Select the NID having highest DSN among RR-table entries
Step 5: Call ReceiveReply method of default Protocol

V. SIMULATION

To evaluate the effectiveness of the proposed scheme, we simulated the scheme in NS-2 [D.B. Johnson et al., 2001]. The simulation parameters are listed in Table 4.3. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s and the maximum simulation speed. Here, we assume that the black hole attack take place after the attacking node received RREQ for the destination node that it is going to impersonate. We also assume that the communication started from a source node to a destination node and the node numbers of the source node, destination node and attacking node are 0, 1 and 9, respectively, as shown in figure 4.5 (for 10 nodes).
For simulation, we consider *node* network as shown in figure 4.1 and Five CBR traffics are considered as given below.

Table 4.3: Simulation Parameters

Simulator	Ns-2(version 2.32)
Simulation Time	100 (s)
Number of Mobile Nodes	3,6,9,12,15
Topology	800 * 800 (m)
Routing Protocol	Black hole ,SODRRP SODRRP

Traffic	Constant Bit Rate
No of Malicious Node	1

The proposed SODRRP is compared with existing On Demand Route Routing Protocol (ODRRP). Metrics consider for comparison are: (i) Packet Loss in the Network and (ii) Packet delivery ratio.

Packet Loss in the Network: Packet loss is the difference between the packets sent and the packets received. Packet loss for malicious node is counted by how many of the packets is there which could not reach to the destination node and are absorbed by the Black Hole node.

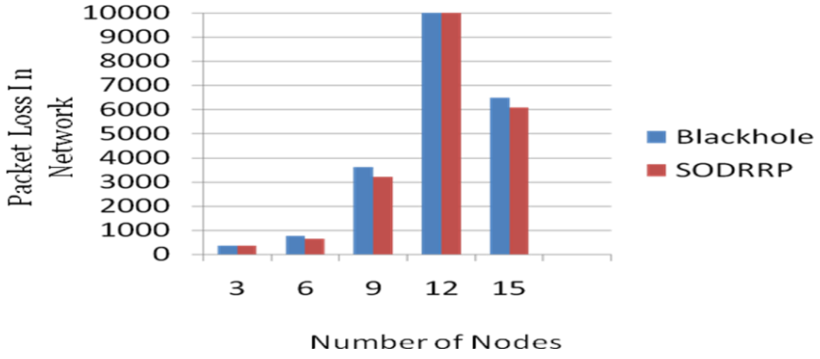

Figure 5.1 Packet loss in the Network

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

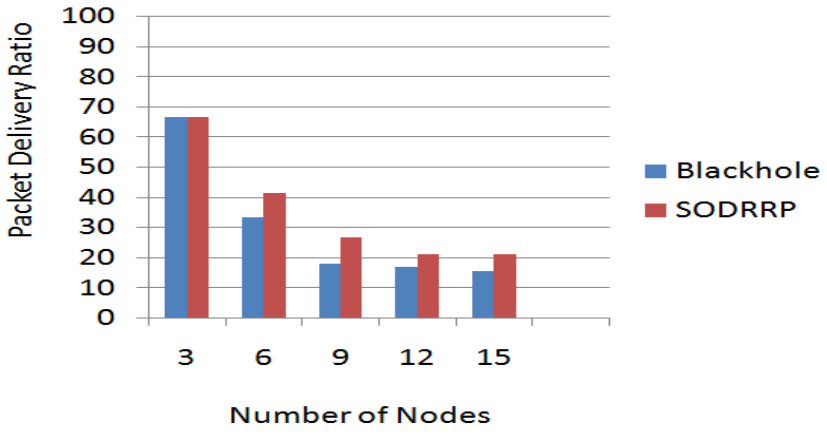

Figure 5.2 Packet delivery ratio

VI. CONCLUSION

Black hole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper, we have analysed the black hole attack and introduced the feature in order to define the normal state of the network. We have presented a new modification in ODRRP protocol i.e. SODRRP which shows significant effectiveness in detecting and preventing the black hole attack.

REFERENCES

[1] P. M. Jawandhiya, "A Novel Hybrid Routing Protocol for Mobile Adhoc Network, International Journal of Advancements in Technology, Vol 1, No 2 (October 2010)

[2] Satoshi Kurosawa1, Hidehisa Nakayama, "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, Nov. 2007.

[3] F. Bai, N. Sadagopan, and A. Helmy, \The important framework for analyzing the impact of mobility on performance of routing protocols for adhoc networks," *Ad Hoc Networks*, vol.1, pp. 383-403, 2003.

[4] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[5] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Eighth Annual International Conference on Mobile Computing and Networking (Mobi- Com 2002), pp. 12-23, Sept. 2002.

[6] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in The 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3-13, June 2002.

[7] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[8] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross feature analysis for detecting ad-hoc routing anomalies," in The 23rd International Conference on Distributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.

[9] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[10] M. S. Corson, S. Batsell, and J. Macker, Architecture consideration for mobile mesh networking," *Proceedings of the IEEE Military Communications Conference (MILCOM)*, vol. 1, pp. 225-229, 21-24 Oct.1996.

[11] S. R. Das, R. Castaneda, J. Yan, and R. Sengupta, Comparative performance evaluation of routing protocols for mobile, ad hoc networks," *Proceedings of the International Conference on Computer Communications and Networks*, pp. 153-161, Oct. 1998.

[12] X. Hong, T. Kwon, M. Gerla, D. Gu, and G. Pei, \A mobility framework for ad hoc wireless networks," *Proceedings of the ACM Second International Conference on Mobile Data Management (MDM)*, pp. 185-196, Jan. 2001.

[13] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On Demand Distance Vector (AODV) routing, RFC 3561, July 2003.

[14] D. B. Johnson, D.A. Maltz, and J. Broch, \DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", *Ad Hoc Networking*, pp. 139-172, 2001.

[15] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[16] L. Layuan, Y. Peiyan, and L. Chunlin, \Performance evaluation and simulations of routing protocols in Ad hoc networks," *Computer Communications*, vol. 30, pp. 1890-1998, 2007.

[17] M. G. Zapata, Secure Ad Hoc on-demand Distance Vector (SAODV) Routing, IETF Internet Draft, draft-guerrero-manet saodv-03, Mar. 2005.

[18] V. D. Park, and M. S. Corson, Temporally-Ordered Routing Algorithm (TORA) Version 1: FunctionalSpeci¯cation, IETF Internet Draft, Aug. 1998. (http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt)

[19] C. E. Perkins, and P. Bhagwat, \Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," *Proceedings of the ACM SIG-COMM Computer Communication Review*, vol. 24,pp. 234-244, Oct. 1994.

[20] C. Perkins, and E. Royer, \Ad-hoc on-demand distance vector routing," *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA1999)*, pp. 90-100, Feb. 1999.

[21] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, \Performance comparison of two on-demand routing protocols for Ad Hoc networks," *IEEE Personal Communications Magazine Special Issue on Adhoc Networking*, vol. 8, pp. 16-28, Feb. 2001.

[22] E. Royer, and C-K Toh, \A review of current routing protocols for Ad-Hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, pp. 46-55, Apr. 1999.

[23] The ns Manual, (formerly ns Notes and Documentation) The VINT Project a Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, Kevin Fall, Editor Kannan Varadhan, Editor, pp. 160, Generating tra±c pattern ¯les, Aug. 23, 2006.

[24] The Network Simulator - NS-2. (http://www.isi.edu/nsnam/ns/index.html)

[25] N. H. Vaidya, \Mobile Ad hoc networks routing, mac and transport issues," *Proceedings of the IEEE International Conference on Computer Communication INFOCOM*, 2004.

[26] Y. Wang, V. C. Giruka, and M. Singhal, \A truthful geographic forwarding algorithm for Ad hoc networks with sel¯sh nodes," *Proceedings of the International Journal of Network Security*, Nov. 2007.

