EAODV: A*-BASED ENHANCEMENT AD-HOC ON DEMAND VECTOR PROTOCOL TO PREVENT BLACK HOLE ATTACKS

Khalil I. Ghathwan, Abdul Razak Yaakub and Rahmat Budiarto

School of Computing, University Utara Malaysia
06010 Sintok, Kedah, Malaysia

Email: k.i.ghathwan@gmail.com

Abstract

Black hole attack is an attack where a node that responds to RREQ from the source node by replying a fake freshness information and false hop count. The black hole nodes do not respond to distributed co-operation in routing protocol to absorb all the packets, as a result, the network performance will drop. Most previous works are focused on anomaly detection through dynamic trusted of the neighbouring nodes. We find out that the internal comparisons take a long time. This loss can be shortened by changing the routing mechanism. We propose an enhancement of AODV protocol, named EAODV, that is able to prevent black hole attacks. The EAODV can find a shortest path of routing discovery using A* heuristic search algorithm. Values of hop count and estimate time to reach the destination node are used as input in the heuristic equation and one-way hash function is used to make a secure value and then to casting it to all neighbouring nodes. Experiments were conducted in NS2 to simulate EAODV in different running time with and without black hole nodes. The EAODV performance results are indicated better in terms Packet loss and Average End-to-End delay.

Keywords: *Mobile ad hoc network (MANET), Black hole, Packet dropping, Malicious node, Routing*.

Abstrak

Black hole attack adalah serangan di mana sebuah node, merespon RREQ dari node sumber dengan informasi dan nilai hop palsu. *Black hole node* tidak merespon kerjasama terdistrbusi dalam protokol *routing* untuk menyerap semua paket. Hasilnya, kinerja jaringan akan turun. Penelitian – penelitian sebelumnya berfokus kepada deteksi anomali melalui mekanisme kepercayaan dinamis dari node tetangga. Kami menemukan bahwa perbandingan internal cukup memakan waktu. Kerugian ini dapat dipersingkat dengan mengubah mekanisme *routing*. Kami mengusulkan peningkatan protokol AODV, bernama EAODV, yang mampu mencegah *black hole attack*. EAODV dapat menemukan jalur terpendek pada *routing* menggunakan algoritma pencarian A*. Nilai-nilai hop dan perkiraan waktu untuk mencapai node tujuan digunakan sebagai input dalam persamaan heuristik dan fungsi hash satu arah digunakan untuk membuat nilai yang aman dan kemudian di-*casting* ke semua node tetangga. Percobaan dilakukan pada NS2 untuk mensimulasikan EAODV dengan *running time* berbeda dengan dan tanpa *black hole node*. Pada penelitian ini dapat dilihat bahwa kinerja EAODV lebih baik dalam hal *Packet loss* dan *Average End-to-end delay.*

Kata kunci: *Mobile ad hoc network (MANET), Black hole, Paket hilang, Node berbahaya, Routing*.

1. Introduction

MANET is a special wireless network. It has an ability to work in unusual environments without infrastructure. Black hole attack exploits the routing protocols to drop the network. Ad-hoc on demand vector (AODV) is a famous MANET protocol [1]. It depends on a freshness routing entries to find a destination node. The routing discovery with Route Request (RREQ) and Route

Reply (RREP) rely on the hop count and destination sequence number. They could be fabricated or changed by black hole nodes. In most previous work, the researchers focused on anomaly detection through dynamic trusted of the neighbouring nodes or authentication. As a result, the existing MANET protocols do not have any fully secure solution to black hole attacks by considering the shortest path. The routing algorithm in AODV relies on a fresh route to the destination node. In AODV, The main goal of black hole attacks makes the destination node unreachable. A black hole node does not respond to distributed co-operation but they respond to RREQ from the source node with false information as though it is fresh. However, it will absorb all the packets in itself, as a result, the network will drop. Furthermore, they re-respond to source node with false reply as though it is fresh enough path to the destination by the RREP. Several previous works are focused on anomaly detection through dynamic trusted of the neighbouring nodes. The process of internal comparisons in their methods take a long time and this loss can be shortened by changing the routing mechanism. In addition, most of previous solutions that proposed to modify the original AODV did not have a practical guarantee to prevent black hole attacks. Adding a mechanism to find a shortest path in routing discovery depending on the artificial intelligent heuristic search algorithm (A*) is a good solution to prevent black hole attacks efficiently and avoid waste time [2],[3]. Values of hop count and the estimate time that are taken advantage by black hole node will be used as input to heuristic equation of the new routing algorithm. One-way hash function is a strong way that can be a useful way to secure hop count value and close this gap in AODV.

The next sections of this paper are arranged as follow, Section 2 discusses some related works, Section 3 presents the proposed solution and Section 4 discusses the experiment setup, results and analysis. Section 5 concludes the paper.

2. Related Works

2.1. The Security Issues of On-Demand Routing Protocols

Hu, Perrig and Johnson [4] proposed a secure on-demand ad hoc routing protocol based on DSR [5]. The authors proposed shared secret key between two nodes, and uses a message authentication code (MAC). The study focused on using MAC in order to authenticate point to point message between these nodes. The proposed system ARIADNE is compared with the original DSR routing protocol. The system performance was reached lower packet overhead around (41.7%) compare than un-optimized DSR, and about the same on all other metrics. However, their scope is limited to the highly optimized version of DSR that runs in a trusted environment because they do not secure the optimization of DSR in the ARIADNE.

Lu, et al. [6] proposed a secure and efficient MANET routing protocol, the SAODV protocol based on AODV [1] and BAODV protocol based on AODV with black hole attack. The authors proposed a direct verification of the destination node by using the exchange of random number. The study focuses on the use of BAODV that means AODV suffers from black hole attack and (SAODV) that means AODV with secure algorithm. The system performance reached around (8%) above the average routing efficiency of SAODV than AODV and same on all other metrics. However, their scope is limited to the highly optimized version of AODV that runs in a trusted environment because the safety and efficiency must be better at the same time.

2.2. Security Issues of Black Hole Attacks

Authors in [7] proposed a solution for collective black hole attack in MANETs called PCBHA. They modified basic AODV routing protocol with Computer simulation using GLOMOSIM (Global Mobile Simulator) to achieve the required security with minimal delay and overhead. The study focuses on making use of "fidelity tables" and assigning fidelity levels to the participating nodes. The proposed algorithm makes use of Minimum threshold value used for the simulation and took 2 units as a test case. To find a valid route the proposed solution tries up to a maximum of RREQ_RETRIES TIMES at the maximum TTL value, Otherwise, declare no valid route is found. They did an experiment through GloMoSim simulation. The results for packet delivery ratio increased around 90% using PCBHA and 30% using AODV. From this result, their approach shows enhancement in the percentage of packets received through AODV less than 60% over their system in the presence of cooperative black hole attack. Although the average end-to-end delay is not high, but the important point in their study was they have solution for collective black hole attack and made fidelity tables. However, their scope is limited to ways to reduce the delay in the network due to the exchange of fidelity packet in PCBHA to achieve security.

Kurosowa, et al. [8] propose a new black hole detection method based on dynamic update training data and simulation on AODV. The study

focuses on the changing of DSN during the routing discovery in deferent stats. The average detection rate is increased by more than 8% and the average false positive rate is decreased by more than 6%. This method shows significant effectiveness in detecting the black hole attack.

Weerasinghe and Fu [9] Modify AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). Simulation results present a good performance in terms of better throughput rate and minimum packet loss percentage over Deng's solutions [10] and AODV. Furthermore, they implement simulation of the proposed solutions for the cooperative black hole attacks, and add some changes to the Deng's algorithm [10] to improve the accuracy in preventing black hole attacks. So, if there is no attack in the network, this scheme may be work very slowly and has a huge overhead for checking all nodes in a route.

Many algorithms and techniques have been investigated to highlight the advantages and disadvantage of them. It is clear from all the mentioned works that there are two types of black hole attacks in MANETs. First is single black hole attacks, and co-operative black hole attacks. The security issue of the two types is important but the most important is the second type. If an algorithm can solve the problem of co-operative black hole attack, then the problem of single will be simple to solve by using the same algorithm.

3. The EAODV

We propose a RREQ-RREP intrusion detection system for mobile ad hoc network. In the intrusion detection system, each node has a routing table which includes all features about neighbours nodes. The routing table is shown in Table I. Every node can be computed the estimate time of routing discovery using the routing table after that it can be used as a heuristic value (h).

*3.1. Heuristic Search Algorithm A**

The heuristic search A* is used to find a shortest path. It is utilized in many application and it is proved the successes into problems solving. The equation (1) is the original A* heuristic search algorithm [2], [3].

$$f(n) = g(n) + h(n) \tag{1}$$

Where: n is the node, *g(n)* is the cost, *h(n)* is the estimated cost from *n* to the goal and *f(n)* is the estimated total cost of path from *n* to the goal.

TABLE I
ROUTING TABLE OF EAODV PROTOCOL IN RREQ, RREP AND ROUTING TABLE

EAODV Table	RREQ-EAODV Table	RREP-AODV Table
Destination IP & DSN	Broadcast ID	
DSN-Flags	Destination IP Address	Destination IP Address
Flags	Destination Sequence Number	Destination Sequence Number
Network Interface	Source IP Address	Source IP Address
Hop Count	Source Sequence Number	Life Time
Next Hop	Hop Count	Hop Count
Life Time	Estimated Time	Estimated Time
Best Path to Destination	Hash Function Value	Hash Function key value

3.2. The Proposed Algorithm

We suppose g(n) equals to D is the hop count in the routing discovery, h(n) equal to h'(n) is the estimated time to destination node during the routing and f(n) is equal to f'(n) is the estimated total cost of path through n to the goal.

Equation (2) shows the objective function of the proposed algorithm and Fig. 1.is included the Pseudo code of EAODV algorithm.

$$f'(n) = h'(n) + D \tag{2}$$

In the following section, we present the idea of our Route Request for Discovery and Route Reply in EAODV.

3.3. Route Discovery Example

The example of implementation the A* algorithm with EAODV is illustrated in Fig. 2. In this figure node 1 is a source node which it wants to send a packet to node 6. According to (2), the D(n) is a hop count of n, and h'(n) is the estimate time of n. f' is the best value that calculating by (2), to update the routing table. However, we can calculate the estimate time as in Table II from (3), whenever the topology changes.

$$ET(n) = \frac{SN(n)}{\sqrt{D(n)} * D(n)} \tag{3}$$

$ET(n)$ is estimated time from node *n* to destination node, $SN(n)$ is the sequence number of node *n*, and $D(n)$ is the number of hop count of node *n*.

```
1: Start
2: Broadcast RREQ from Source node to all neighbouring
   nodes.
3:      setup hash function for all neighbouring nodes.
4:          %Hash function phase
5:              {  source node broadcast RREQ with Key
                   Disable all RREP
                }
6:          %Route discovery phase
              { if Source starts broadcasting RREQ
                   then Do route discovery using (A* to
                                find the shortest path to
                                Destination)
              }
7:          %Description phase
              {calculate Key and save new key
                   then Do Destination unicast to
            source node
               }
8:          %Update routing tables
              {if any Black hole node sends RREP
                   without  new key then
                                {Delete path from routing
                   table}
              }
9:End
% A* algorithm, a suggestion algorithm to find a shortest
path from source node to destination node %
Function A* Heuristic Search() return BestPath
{
Inputs: HopCount, EstimatedTime, Current, Temp
Local variables: FN, GN, HN
          Temp=GN(Source)
          For i=1 to Current do
                   GN(i)=HopCount(i) + HN(i)
                   If GN(i)<Temp Then Temp=GN(i)
                   Else  NEXT i
          BestPath=Temp
}
```

Fig. 1.Pseudo code of EAODV algorithm

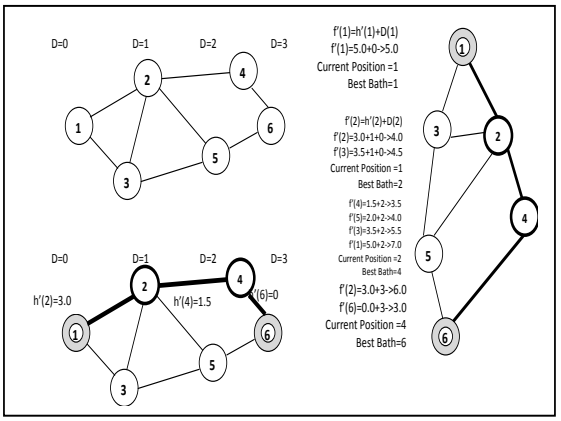

Fig. 2.Topology example of six nodes (node 1 is a source node, node 6 is a destination node and nodes 2-4 are intermediate nodes).

4. Experiments Setup, Results and Analysis

We use NS2 simulator version 2.33 to experimenting three scenarios. The framework of three scenarios is shown in Fig. 3. Scenario 1 is to test the original AODV, scenario 2 is to test the black hole AODV and scenario 3 is to test the execution of the new formula of the proposed A* for finding the shortest path and securing the AODV protocol. The Simulation Parameters for scenario 1,2 and 3 are shown in Table III.

TABLE II
EXAMPLE OF ESTIMATED TIME OF ROUTE DISCOVERY TO THE DESTINATION (NODE 6)

Source Nodes	EstimatedTime(sec.)
1	5.0
2	3.0
3	3.5
4	1.5
5	2.0
6	0.0

TABLE III
SIMULATION PARAMETERS FOR SCENARIOS 1,2,3

Parameter	Simulation1	Simulation2	Simulation3
Simulation time	1000 sec.	1000 sec.	1000 sec.
Number of nodes	50	50	50
Routing Protocol	AODV	BlackHole-AODV	HashFunction-AODV
Traffic Model	CBR(UDP)	CBR(UDP)	CBR(UDP)
Pause time	2 sec.	2 sec.	2 sec.
Maximum mobility	60 m/sec.	60 m/sec.	60 m/sec.
No. of sources	1	1	1
Map area	800m x 800m	800m x 800m	800m x 800m
Transmission Range	250m	250m	250m
Number of malicious node	1	1	1

4.1. Performance Metrics

Three performance indicators are used to measure our simulation which are End-to-end delay, Packet loss and Packet delivery ratio.

End-to-end delay (φ): The average time taken for a data packet to reach the destination including the delay of route discovery response process until transmission of data packets are made. Only the data packets successfully addressed and delivered are counted. The equation to calculate the End-to-end delay is shown in (4).

$$\varphi = \frac{\sum(\alpha - \beta)}{\sum(\delta)} \quad (4)$$

Where: α is arrival time, β is transmission time and δ is number of connections. So, when the end to end delay value goes lower, the better performance of the protocol will be reached.

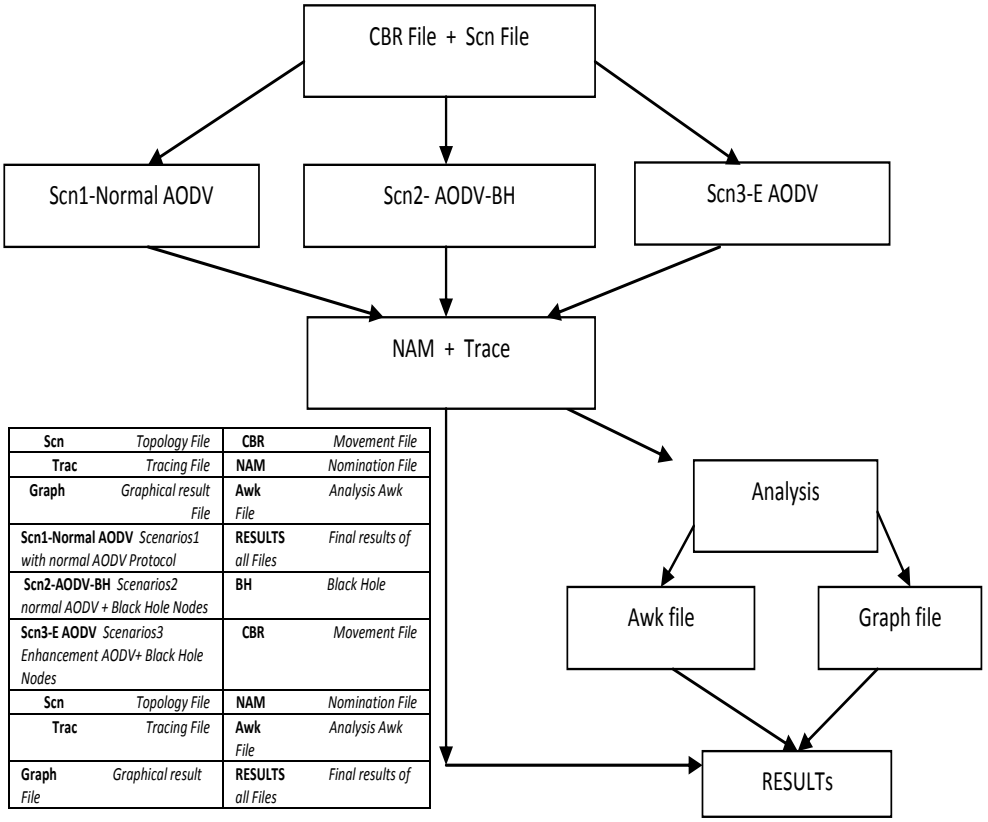

Fig. 3.The Simulation Framework of the three Scenarios

Packet loss (τ): The total number of packet loss that lost during the execution of the simulation. The Equation of Packet loss is shown in (5).

$$\tau = [\sum(\mu) - \sum(\vartheta)] * (\frac{100}{\sum(\mu)}) \quad (5)$$

Where: μ is the number of packets sent and ϑ is the number of packets received. The lower value of the package loss means better performance of the protocol.

Packet delivery ratio (*PDR*): the ratio of the number of data packets delivered to the destination. This metric shows the amount of data that arrived at the destination. The PDR is shown in (6).

$$PDR = \frac{\sum(\vartheta)}{\sum(\epsilon)} \quad (6)$$

Where: ϵ is the number of packets. The largest package delivery means that the best performance of the protocol.

4.2. Packet Loss: Results and Discussion

In Fig. 4. three scenarios; original AODV, black hole AODV and EAODV are compared. The increases in a packet loss ratio by the effects of the black hole attack will be degrades the performance of the AODV protocol and it maybe will cause a DoS attack. Compared to original AODV, the proposed EAODV indicates the EAODV minimizes the packet loss and improves the network performance. Packet loss was 21.41% in AODV but it increases with black hole 28.32% after that EAODV improve the percentage 24.96%.

Comparison between the decrease of packet loss with black hole AODV with the result of with EAODV means some improvements were conducted in avoiding the black hole attack. After the original AODV packet loss was increase 7.8 % with black hole AODV, packet loss was decrease to 3.36 % with EAODV.

4.3. Average End-to-End Delay: Results and discussion

Fig. 5. shows the comparison of the average End-to-End delay of the three scenarios. The

average End-to-End Delay increases with the existing of black hole. This delay degrades the performance of the network and causes more delay time when packets try to reach the destination node. Furthermore, when we compare the original AODV with the proposed protocol EAODV, the result indicated that EAODV minimizes the Average End-to-End Delay and improves the network performance. The percentage of delay was 29% with black hole node comparing with original AODV. This percentage was about 11.09% with EAODV.

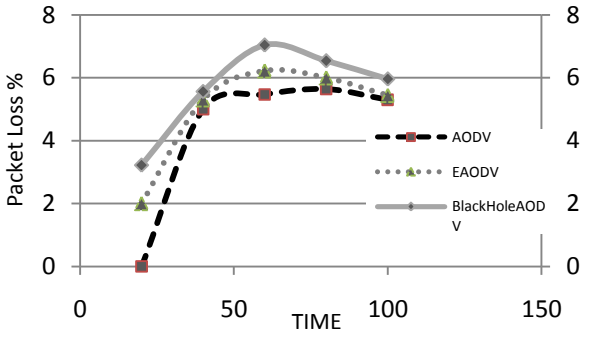

Fig. 4.Packet Loss Percentage for AODV, Black Hole AODV and EAODV

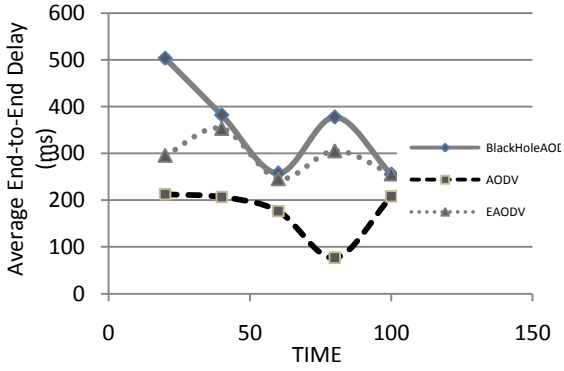

Fig. 5. The average end-to-end delay for AODV, Black Hole AODV and EAODV

4.4. Packet Delivery Ratio (PDR): Results and discussion

Graphs in Fig. 6. shows the PDR for the three scenarios; We can see from the graphs that the packet delivery ratio does not increase with the existing of the black hole in the network. The packets were reach to destination from source node was 479.77 in total for standard AODV, 469.56 for AODV with black hole nodes and 447.43 for EAODV. So we can see that the overall PDR of EAODV does not degrade significantly due to the implementation of security algorithm.

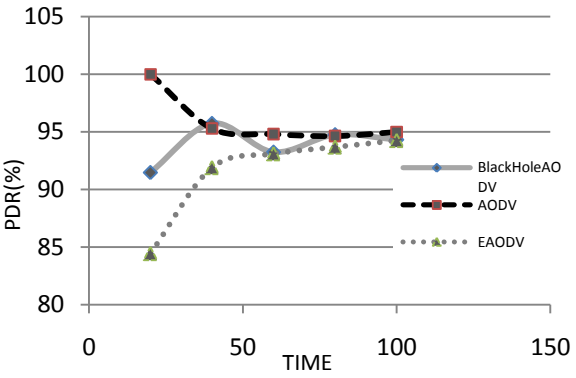

Fig. 6.The Packet Delivery Ratio for AODV, Black Hole AODV and EAODV

5. Conclusions

This paper has proposed defence mechanism against a cooperative black hole attack in a MANET that relies on AODV routing protocol named as EAODV Protocol. The proposed EAODV modifies the standard AODV and optimizes the routing process by incorporating A* search algorithm into the AODV routing process. The A* algorithm uses the value of hop count and the estimate time as input. One-way hash function is used to secure hop count value. The experimental results showed that EAODV is able to improve the performance of the network while securing from black hole attack.

As for future work we plan to consider implementation of more complex black hole attacks as well as other routing protocols such as DSR, CBRP, ZRP.

References

[1] C. Perkins and E. Royer "Ad hoc on demand distance vector Routing,"in *proceeding of the second IEEE workshop on Mobile computing Systems and Applications*, New Orleans 1999.

[2] S. Edelkamp and S. Schrodl "Heuristic Search: Theory and applications, "in *Morgan Kaufmann publishers*, Elsevier, USA, 2012.

[3] S. J. Russell and P. Norvig "Artificial Intelligence A Modern Approach," in *Prentice Hall, Englewood Cliffs*, New Jersey, 1995,pp.96–128.

[4] Y.,-C. Hu, A. B. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *Proc. 8th*

ACM Int'l. Conf. Mobile Comp. and Net. (Mobicom''02), Atlanta, Georgia, pp. 12–23, Sept. 2002.

[5] D. B. Johnson and D. A. Maltz, " Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile-Computing, edited by Tomasz Imielinski and Hank Korth, pp. 153-181, 1996.

[6] S. Lu, L. Li, K. Y. Lam and L. Jia, " SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," in *IEEE Computational Intelligence and Security, CIS '09. International Conference*, vol.2, pp. 421-425, Dec. 2009.

[7] L. Tamilselvan and V. Sankaranarayanan, " Prevention of Co-operative Black Hole Attack in MANET," in *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, AusWireless*, pp. 21- 26, 2008.

[8] S. Kurosawa, H. Nakayama, N. Kato, N. 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, 2007.

[9] H. Weerasinghe, and H. Fu, " Preventing Cooperative Black Hole attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation," *International journal of software engineering and its applications*, vol.2,No. 3, pp.39-54, 2008.

[10] H. Deng, W. Li and D. P. Agrawal, " Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 22-30, 2002.