Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

Using Apriori algorithm to prevent black hole attack in mobile Ad hoc networks

Hadis Hafizpour[a*], Mehdi Sadegh zadeh[b] and Seyed Javad Mirabedini[c]

[a]*Department of Computer, Science and Research Branch Bushehr, Islamic Azad University, Bushehr, Iran*
[b]*Department of Computer, Central Mahshahr Branch, Islamic Azad University, Mahshahr, Iran*
[c]*Department of Computer, Central Tehran Branch, Islamic Azad University, Tehran, Iran*

CHRONICLE

Article history:
Received July 2, 2012
Received in revised format
28 October 2012
Accepted 11 November 2012
Available online
November 14 2012

Keywords:
Ad hoc Networks
Apriori algorithm
Routing Protocols
Black Hole Attack

ABSTRACT

A mobile ad hoc network (MANET) is considered as an autonomous network, which consists of mobile nodes, which communicate with each other over wireless links. When there is no fixed infrastructure, nodes have to cooperate in order to incorporate the necessary network functionality. Ad hoc on Demand Distance Vector (AODV) protocol is one of the primary principal routing protocols implemented in Ad hoc networks. The security of the AODV protocol is threaded by a specific kind of attack called ‘Black Hole’ attack. This paper presents a technique to prevent the Black hole attack by implementing negotiation with neighbors who claim to maintain a route to destination. Negotiation process is strengthen by apriori method to judge about suspicious node. Apriori algorithm is an effective association rule mining method with relatively low complexity, which is proper for MANETs. To achieve more improvement, fuzzy version of ADOV is used. The simulation results indicate that the proposed protocol provides more securable routing and also more efficiency in terms of packet delivery, overhead and detection rate than the conventional AODV and fuzzy AODV in the presence of Black hole attacks.

1. Introduction

The ad hoc networks is categorized as infrastructure less networks, where all mobile nodes communicate with each other with no fixed infrastructure among them. An ad hoc network is considered as a collection of nodes, which would not depend on a predefined infrastructure to maintain the network connected. Therefore, the functioning of Ad hoc networks depends on the trust and co-operation among nodes. Nodes can assist each other in conveying data about the topology of the network and they can share the responsibility of managing the network. Therefore, each mobile node performs the function of routing and relaying messages for other mobile nodes (Deng et al., 2002; Siva Ram Murthy, & Manoj, 2007). Many network operations include routing and network

*Corresponding author.
E-mail addresses: h_h6149@yahoo.com (H. Hafizpour)

doi: 10.5267/j.msl.2012.11.019

management (Karpijoki, 2000). Routing protocols (Larsson, & Hedman, 1998) is normally categorized based on routing topology into proactive, reactive and hybrid protocols and proactive protocols are typically table-driven and instances of this kind include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-demand protocols, on the contrary, do not periodically update the routing data and it is propagated to the nodes when needed. Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV) are some examples (Perkins et al., 2000; Hu et al., 2005; Perkins et al., 2003). Hybrid protocols take advantage of both reactive and proactive approaches, e.g. Zone Routing Protocol (ZRP). Security is always a main concern in all types of communication networks, but ad hoc networks face the biggest challenge because of inherent nature of dependence on other nodes for transmission. Therefore, there is a slew of attack, which could be performed on an Ad hoc network (Deng et al., 2002; Zhou, & Haas, 1999; Wu et al., 2007).

During the past few years, there have been tremendous efforts on the cooperation issue in MANET and some of the related issues are briefly presented here. There are solutions to detect and to eliminate a single black hole node (Deng et al., 2002) and Marti et al. (2000) explained misbehavior detection and reaction where two extensions to the DSR algorithm are presented including the watchdog and the path rater. The watchdog detects misbehaving nodes by listening promiscuously to the next node transmission and it is imperfect because of collisions, limited transmit power and partial dropping. According to simulations (Buchegger et al., 2003), it is highly efficient in source routing protocols, such as DSR. The path rater implements the knowledge from the watchdog to select a path, which is most likely to deliver packets. The path rating is measured by averaging the rating of the nodes in the path, where each node keeps a rating for all the nodes it recognizes in the network. Watchdog is implemented in various solutions for the cooperation problem. The main drawback of this idea is that it helps selfishness and misbehaving nodes transmit packets without punishing them, and encourages misbehavior.

Buchegger and Le Boudec (2003) presented the CONFIDANT protocol. Each node monitor the behavior of its next hop neighbors in a similar manner to watchdog. The data is devoted to the reputation system, which updates the rate of the nodes. Based on the rating, the trust manager makes appropriate decisions on either providing or accepting route information, or even accepting a node as part of a route, etc. When a neighbor is suspicious in misbehaving, a node delivers data to its friends by sending them an ALARM message. If a node’s rating turns out to be intolerable, the data is relayed to the path manager, which proceeds to remove all routes containing the intolerable node from the path cache and this does not address partial packet dropping.

Michiardi and Molva (2002) proposed the CORE scheme and different related issues. In this scheme, every node measures a reputation value for every neighbor, based on observations, which are collected in the same way as watchdog. The reputation mechanism distinguishes between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is measured directly from neighbors past and presents observations, giving more relevance to past observations to minimize false detection impact. According to direct reputation, the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value related to each node. By preventing the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to them is behaving node to be suspended. The working of the model and its performance were not reported.

Bansal and Baker (2003) proposed OCEAN, a scheme for robust packet-forwarding, which is based on node’s observations. In contrast to previous mechanisms, no rating is exchanged and every node depends on its own information, so the trust management is prevented. The rating is based on a counter, which counts the positive and the negative steps a node performs and based on a faulty threshold, the node is added to a faulty list. In the method for route selection, a DSR node appends an avoid list to every generated RREQ and a RREP based on this list. A second-chance mechanism is enhanced to give nodes, which were previously considered misbehaving another opportunity to operate. OCEAN simulations makes a conclusion that a scheme, which relays only on first-hand observation performs almost as well and sometimes even better than a scheme that also depends on second-hand information. OCEAN also fails to deal with the misbehaving nodes properly.

Hod (2005), in his thesis highlighted different aspects of cooperation enforcement and reliability, when AODV is the underlying protocol. Furthermore, it presented a scalable protocol, which combines a reputation system with AODV that addresses reputation fading, second-chance, robustness against liars and load balancing. The proposed solution constructs various reputation properties and misbehaving reaction better suiting to AODV. The security of the AODV protocol consists of a particular kind of attack called ‘Black Hole’ attack (Deng et al., 2002). In this attack a malicious node advertises itself as having the shortest path to the node whose packets attempts to intercept. The proposed approach to combat the Black hole attack is based on node’s activity as example number of sent RREQ, number of sent RREP, number of received data and number of sent data packets. When an intermediate node reply RREQ packet, the voting process initiated about activity of replier.

Medadian et al. (2009) proposed an approach to mitigate the Black hole attack through the judgment process by implementing honesty of a nodes, which, is used from the opinions of a neighbor nodes of a node in a network and to transfer the data packets, a node must demonstrates its honesty. If a node is the first receiver of a RREP packet, it forwards packets to source and initiates judgment process on about replier. The judgment process depends on the feedback on network’s nodes about replier. These neighbors are requested to send their opinion on a node. When a node gathers all opinions of neighbors, it decides whether the replier is a malicious node based on number rules. The biggest drawback of this solution is that the opinions of neighbors may not always be correct. In this paper, we propose a novel method to make a reasonable judgement about suspicious node. We use apriori algorithm, which is association rule mining technique (Jabas, 2011). It has very low complexity, which is proper for MANETs. We implement the proposed method on ADOV and fuzzy AODV.

The rest of this paper is organized as follows. In Section 2 provides the background on apriori algorithm and section 3 describes the characteristic of the black hole attack. In Section 4, we propose the detection scheme of the attack. Section 5 analyzes the black hole attack through simulations, and evaluates its effectiveness. Section 6 concludes the paper.

2. Apriori algorithm

Agrawal et al. (1993) and Hegland (2005) are believed the first who introduced the problem of deriving association rules from information. The market-basket problem introduced in their work by the Apriori algorithm, which is the most commonly used association rule discovery algorithm and it utilizes the frequent sets. This algorithm uses the downward closure property. Fig. 1 shows the pseudo-code of Apriori algorithm. One of the advantages of the method is that before reading the database at every level, it graciously prunes different sets, which are unlikely to be frequent sets. Apriori algorithm has become a reference method, and has been improved in different ways in terms of time complexity, the number of scans of the database, size of transaction, threshold and so forth. Since association rules are derived from MFSs, the terms MFS and association rules are implemented, interchangeably. In this paper, when a node doubts on honesty of a neighbor node, it launches a judgment process. We strengthen this process by Apriori algorithm.

Apriori Algoithm

```
Initialize: k:=1,$C_1$=all the 1-itemsets;
read the traffic bit-matrix to count the Support of $C_1$ to determine $L_1$
while $L_{k-1} \neq Ø$ do
        $C_k$= gen-candidate-itemsets with the given $L_{k-1}$
        Prune($C_K$)
end while
$L_1$:={frequent 1-itemsets};
K:=2; // k represents the pass number
for all rows Є bit-matrix do
        increment the count of all candidates in $C_k$ that are contained in r;
        $L_k$:= All candidates in $C_k$ with minimum Support;
        K:= k+1
end for
Answer L:=$U_K L_K$;
```

Fig. 1. Apriori algorithm

Black hole attack

A Black Hole attack (Deng et al., 2002; Hu, & Perrig, 2004; Hongsong et al., 2006) is a type of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then attract them without forwarding them to the destination. Co operative Black hole is the malicious nodes, which acts in a group (Ramaswamy et al., 2003; Hod, & Dolev, 2005). When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receives the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of datapackets, the Black hole node simply discards them, instead of forwarding to the destination.

3. The proposed method

Mobile nodes run AODV to forward data packets to appropriate destinations and every node to be able to forward data packets and it should be in the discovered path. A malicious node sends reply packet to each received route request and it receives data packets and simply removes them. To discover malicious nodes, member nodes should monitor their neighbors with recording number of RREQ, RREP, received and forwarded data packets. When a member node suspects on another node, it sends a request to collect loged data of other members. Requester creates a data base from gathered information and Apriori algorithm is used to extract malicious nodes. Any node could implement Apriori algorithm to inference about honesty of initiator of reply packets. Activities of a node in a network show its honesty. To participate in data transfer process, a node must demonstrate its honesty. Using early simulation, all nodes are able to transfer data. Therefore, they have enough time to demonstrate its truth. In AODV protocol each member node could do following actions:

Send, receive and generate **Data packets** *Send, receive and generate* **RREQ packets** *Send, receive and generate* **RREP packets**

To make an appropriate judgment about honesty of a node, every node has to log the mentioned statistics. Therefore, the proposed method has five stages including monitoring, suspecting, polling, judgment and alarming. In the first stage, every member node monitors neighbor node's activities. It records the needed information to fill fields of table in Fig. 2. Each node upon receives a RREP packet from a neighbor node; computes level of honesty for neighbor node. Eqs. (1-3) compute a value to judge about the origin of neighbor node's activities.

$$T_n^t = \beta_n^t \times \alpha_n^t \quad (1)$$

$$\alpha_n^t = \left|\frac{\#RREP}{\#RREQ}\right| \quad (2)$$

$$\beta_n^t = \left|\frac{\#Recv_{data}}{\#Send_{data}}\right| \quad (3)$$

If value of T_n^t is greater than a threshold, node requests a polling around two-hop neighbors of suspicious node by sending a polling request packets. Every node receiving the request packet uses a typical judge table (Fig. 3). In Fig. 3, N means normal node, S means suspicious node and M is for malicious node. This table is concluded from simulation results. Polling requester records all responses and creates a table shown in Fig. 4.

Neighbor $_i$				
Rdata	**sdata**	**rrep**	**Rreq**	**utime**
confdnc		Set		

Fig. 2. Entry of log table

Judge table	**β<<1**	**β≈1**	**β>>1**
0 ≤α≤ 0.25	N	N,S	N,S,M
0.25 ≤α≤ 0.75	N,S	N,S	S,M
0.75 ≤α≤ 1	N,S	N,S,M	M

Fig. 3. Judge table

voter	**Opinion**
1	{U}
2	{N,S,M}
3	{S,M}
4	{N}
5	{S,M}
6	{M}
..	**......**
N	**{......}**

Fig. 4. Opinion table in polling requester

The requester uses Eq. (4) to compute confidence of item sets in opinion table. Indeed, the fourth stage is done by apriori algorithm. It reduces opinions of voter to conclude suspicious node belong to which one of N, M and S.

$$CONFIDENC(S \rightarrow M) = \frac{SUPPORT\ COUNT(S \cup M)}{SUPPORT\ COUNT(S)} \tag{4}$$

Fig. 5 depicts pseudo-code of the proposed method for discovering and preventing blackhole attacks in AODV protocol.

pseudo-code

```
Event_handle_function(event)
{
 Switch(event)
   {
     Case(RREP,RREQ,DATA):
           Update log table
           If (event is RREP)
               {
                 If RREP's sender in quarantine list reject forwarding RREP
                 Else
                   {
                      Check if RREP's sender is suspicious
                       If so, then send AODV_POLLING_REQ
                       Set a timer to gather enough responses
                   }
               }
           Break;
     Case (AODV_POLLING_REQ):
            If node has information about suspiciouse node, send its opinion(N,S,M) via
                AODV_POLLING_REP
            Decrement ttl
           If (ttl>0),resend AODV_POLLING_REQ
            Break;
     Case (AODV_POLLING_REP):
            If node is requester,record all information in AODV_POLLING_REP
            Break;
     Case (AODV_POLLING_RES):
            Add node to quarantine list
            Break;
     Case (TIMER_EXPIRATION):
            Run apriori algorithm to make a decision
            If node is malicious or suspicious, inform to members by AODV_POLLING_RES
            Break;
   }
}
```

Fig. 5. Pseudo-code of the proposed method

Fig. 5 presents all different events occurring in the proposed method and the needed actions taken to handle them.

4. Simulation results

This section demonstrates how Apriori algorithm is used on malicious nodes from log information of MANET nodes. The simulation is performed by NS2 (http://www.isi.edu/nsnam/ns/). Parameters used in the simulator are summarized in Table1. Hundred nodes are distributed randomly in the simulation area of 1000 × 1000 m^2 and with a 250 m transmission range for each node. The Propagation model of the signal is “Two Ray Ground”. The channel capacity is 2 mbps. The random mobility mode of the nodes is generated by the CMUs node-movement utility “setdest” with various Node Mobility Speeds (NMS) within the range of 5-30 m/s. The nodes do not move throughout the simulation time, i.e., they stop according to a constant pause time parameter, which lasts for one second. The packet size is 512 bytes.

Table 1
Simulation parameters

Parameter	Value
Number of the nodes	100
Routing protocol	AODV,FAODV
Mobility model	Random way point
Pause time	0
Radio transmission range	250 m
Channel capacity	2 mbps
Data flow	UDP
Data packet size	512 bytes
Node placement	Random
Terrain area	1000 × 1000 m^2
Simulation time	600 S

In the following figures, two different versions of AODV are used to implement Apriori algorithm: basic and fuzzy AODV (Rezaei et al., 2008).

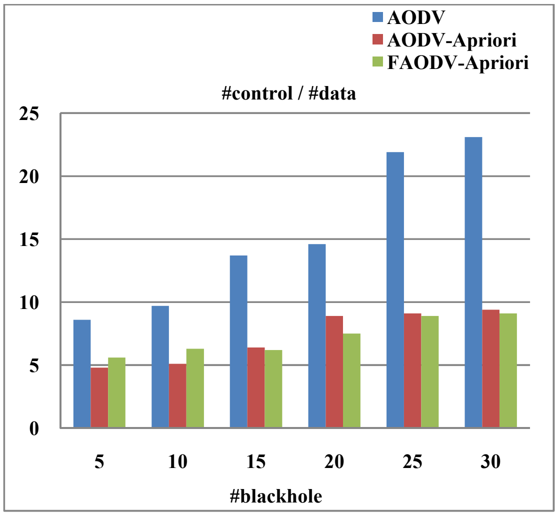

Fig. 6. Overhead with increasing attackers

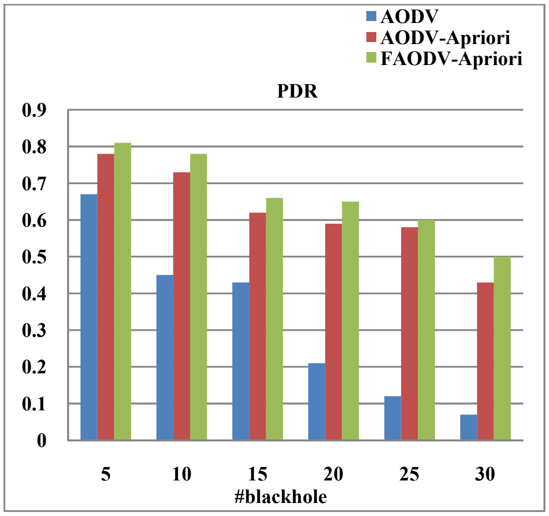

Fig. 7. Packet delivery ratio with increasing attackers

In this scenario, we increase the number of blackhole attacker and study performance in terms of data delivery ratio, overhead and detection rates. The proposed methods use Apriori technique to discover malicious nodes. It creates an efficient database of the gathered information by member nodes. We implement the proposed method on fuzzy version of AODV. The simulation results presents that FAODV-Apriori algorithm dominates other methods.

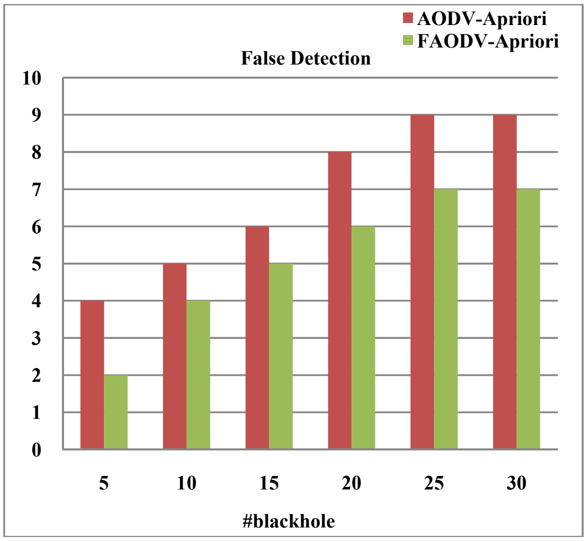

Fig. 8. False detection rate with increasing attackers

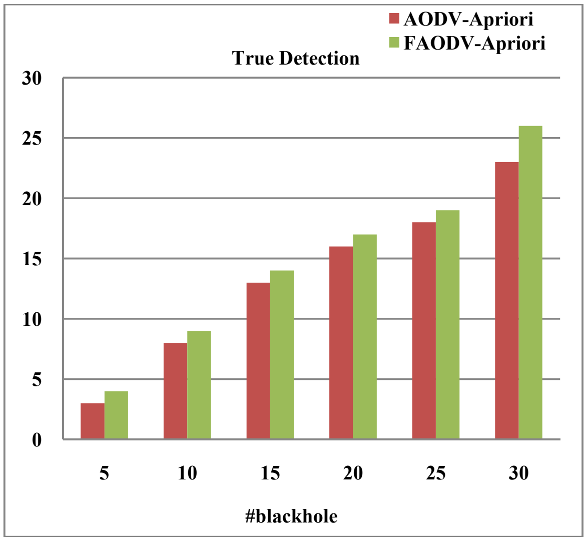

Fig. 9. True detection rate with increasing attackers

5. Conclusion and future works

In this paper, the routing security issues of MANETs have been explained and one type of attack, the black hole, which could easily be deployed against the MANET has been described. In this paper, a novel technique based on Apriori method has been proposed to discover and prevent blackhole attacks in MaNETs. Future works could be concentrated on ways to reduce the delay in the network and to get more improvement, fuzzy version of apriori algorithm can be implemented.

References

Agrawal, R., Imielinski, T. & Swami, A. (1993). Mining association rules between sets of items in large databases. *SIGMOD '93 Proceedings of the 1993 ACM SIGMOD international conference on Management of data*. 207–216.

Bansal, S. & Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks. *Networking and Internet Architecture (cs.NI).*

Buchegger, S., Tissieres, C. & Le Boudec, J.Y. (2003). A test bed for misbehavior detection in mobile ad-hoc networks -how much can watchdogs really do. *Technical Report IC/2003/72, EPFL-DI-ICA.*

Buchegger, S. & Le Boudec, J.Y. (2003). A robust reputation system for mobile ad hoc networks. *Technical Report IC/2003/50, EPFL-DI-ICA.*

Deng, H., Li, W. & Agarwal, D.P. (2002). Routing Security in Wireless Ad Hoc Networks. *University of Cincinnati, IEEE Communications magazine*. 40(10), 70 -75.

Hu, Y.C & Perrig, A. (2004). A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security and Privacy*. 2(3),28-39.

Hu, Y.C, Perrig, A. & Johnson, D.B. (2005). Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks. *In Wireless Networks Journal*. 11(1,2), 21-38.

Hod, B. & Dolev, d. (2005). Cooperative and Reliable Packet-Forwarding On Top of AODV. *A thesis on School of Engineering and Computer Science, The Hebrew University of Jerusalem, Israel.*

Hegland, M. (2005). The apriori algorithm - tutorial, Technical report. *WSPC/Lecture Notes Series: 9in x 6in In Australian National University*.

Hongsong, C., Zhenzhou, J. & Mingzeng, H. (2006). A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition. *In Asian Journal of InformationTechnology*. 5(1), 54-60.

Jabas, A. (2011). MANET Mining: Mining Association Rules. *Mobile Ad-Hoc Networks: Applications*. ISBN: 978-953-307-416-0.

Karpijoki, V. (2000). Security in Ad Hoc Networks. *Seminar on NetWork Security, HUT TML*.

Larsson, T. & Hedman, N. (1998). Routing Protocols in Wireless Ad-hoc Networks - A Simulation Study. *Masters thesis in computer science and engineering, Lulia University of Technology, Stockholm*.

Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *In mobile Computing and Networking (MOBICOM)*. 255–265.

Michiardi, P. & Molva, R. (2002). Preventing denial of service and selfishness in ad hoc networks. *In Conference Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland*.

Michiardi, P. & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *In Proceedings of The 6th IFIP Communications and Multimedia Security Conference*. 107–121.

Medadian, M., Yektaie, M.H. & Rahimi, A.M. (2009). Combat with Black hole attack in AODV routing protocol in MANET. *First Asian Himalayas International Conference on Internet.* 1-5.

Perkins, C.E., Das, S.R. & Royer, E.M. (2000). Ad-Hoc on Demand Distance Vector (AODV). *http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt.*

Perkins, C.E., Belding-Royer, E.M. & Das, S.R. (2003). Mobile Ad Hoc Networking Working Group. *http://*www.cs.ucsb.edu/*Internet Draft/draft-ietf-manet-bcast-02.txt.*

Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J. & Nygard, K. (2003). Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. *In Proc. of Int'l Conf. on Wireless Networks.*

Rezaei, M., Mirabedini, J., Latif Shabgahi, Gh., & Jalalvand, S. (2008). *Improvement of AODV protocol using fuzzy protochol*. 13th Conference in Electrical Engineering, Tehran, Iran.

Siva Ram Murthy, C. & Manoj, B.S. (2007). Ad hoc Wireless Networks: Architectures and Protocols. *Pearson Education*. ISBN: 9788131759059.

Wu, B., Chen, J., Wu, J. & Cardei, M. (2007). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. *WIRELESS/MOBILE NETWORK SECURITY*. 103-135

Zhou, L. & Haas, Z.J. (1999). Securing Ad Hoc Networks. *IEEE network, special issue on network security*. 13(6), 24 – 30.

http://www.isi.edu/nsnam/ns/