ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

Review on Gray Hole Attack in MANET

Shaily[1] Shashi lata [2]
M-Tech Student[1], HOD.[2]& Department of ECE & Advance Institute of technology
Palwal, Haryana, India

Abstract: **Mobile Ad-hoc Networks (MANETs) are utilized most generally across the world, because it has the capability to interact each other without any static network. It has the power to take decisions on its own that is autonomous state. MANET is basically known for infrastructure less. The bridges in the network are normally called a base station. A unique security solution is very much required for networks to secure both route and data sending operations in the network layer. Security is a necessary need in MANET. Without any suitable security solution, the malicious node in the network will behave as a normal node which leads eaves dropping and selective forwarding attack basically called Gray Hole attack. In this paper we reviewed about the different kinds of mechanisms to prevent Gray Hole Attack**

Keywords— MANET, AODV, Network layer Attack, Gray Hole attack.

I. INTRODUCTION

Ad-Hoc network is called Independent Basic Service Set (IBSS) Stations. IBSS interact with each other directly and do not contain any access point. Due to the nodes mobility in ad-hoc networks, they are generally known as MANET (Mobile Ad-hoc Network). Mobile Ad-Hoc network [1] is a set of mobile nodes which are free to move arbitrarily while being capable to interact with each other without the support of an available network infrastructure. MANETs are appropriate for usage in situations where any wireless or wired infrastructure is inaccessible, damaged, overloaded or destroyed i.e. disaster relief effort, emergency or rescue missions and tactical battlefields, as well as civilian MANET circumstances, i.e. classrooms or conferences and in the research field like sensor networks. MANETs remove this dependence on a static network infrastructure where every station behaves as an intermediary switch. Security in MANETs is a complicated issue. This complication is because of mobility of node, dynamic configuration and resource restraints. In mobile ad hoc networks, nodes also act routers that find and manage routes to other network nodes. The main concern of MANET routing protocols is to set up an effective and optimum route between the communicating entities. Any attack can mess up whole communication and the entire network will be damaged. Nodes are more susceptible to security attacks in mobile ad-hoc networks as compared to conventional networks with a static infrastructure. There are several types of attacks by malicious nodes that can harm a network and build it un-flexible for communication. One such type of attack is gray hole attack. A gray hole attack is one in which a malicious node shows itself as having the shortest path to a destination node in a network. This can cause Denial of Service (DoS) [2] by discarding the obtained packets.

II. SECURITY ISSUES

The ultimate objective for MANET is to offer security solutions. To give a solution for security causes there are some of the technique which is utilized to detect, prevent and respond. They are mainly Confidentiality, Availability, Integrity and Authentication.

Availability

The network should be existed only for the authorized users and this technique is utilized to secure against the type of attacks i.e. black hole, gray hole, Information disclosure and Message modification.

Confidentiality

In MANET it is very complex to achieve the confidentiality because of intermediate nodes routing, which can easily fetch the information from the routing nodes.

Integrity
The information transmission should be secured against any alteration and message modification.
Authentication
The network should be accessed only by the authorized nodes i.e. Digital signature, Reply and Non repudiation.

III. ROUTING IN MANET

The deficiency of a backbone infrastructure [7] combined with the fact that mobile Ad Hoc networks change their configuration frequently and without prior notice builds packet routing in ad-hoc networks a challenging task. The proposed mechanisms for routing can be classified into topology-based and position-based routing.
Topology-based routing protocols utilize the information about the connections that available in the network to perform packet sending. They can be further classified into *proactive*, *reactive*, and *hybrid* approaches.
Proactive algorithms use classical routing techniques i.e. distance-vector routing (for example DSDV) or link-state routing (e.g., TBRPF and OLSR). They manage routing information about the existed paths in the network even if these paths are not currently utilized. The main limitation of these mechanisms is that the maintenance of unutilized paths may occupy an important part of the existed bandwidth if the network topology changes frequently.
In reply to this observation, reactive routing protocols were formulated (such as TORA, DSR and AODV). Reactive routing protocols manage only the routes that are currently in usage, thus decreasing the network burden when only a small subset of all existed routes is in usage at any time. Since, they still have some inherent restrictions.
First, however, routes are only maintained while in usage, it is basically needed to perform a route discovery before packets can be interchanged among communication peers. This results to a delay for the first packet to be transferred. Second, even though route maintenance for reactive algorithms is limited to the routes currently in usage, it may still create an important amount of network traffic when the network topology changes quickly. At last, packets en-route to the destination node are likely to be lost if the route to the destination node changes.
Hybrid Ad Hoc routing protocols i.e. ZRP integrate local proactive routing and global reactive routing for achieving a higher level of scalability and efficiency. Since, even a integration of both strategies still requires to manage minimum those network paths that are currently in usage, restricting the amount of topological changes that can be bear within a specified amount of time.
Position-based routing algorithms remove some of the restrictions of topology-based routing by utilizing extra information. They need that information about the physical position of the participating nodes be existed. Generally, every node determines its own position through the usage of GPS or some other kind of positioning service. A *location service* is utilized by the packet sender to determine the destination position and to involve it in the packet's destination address. The routing decision at every node is then depend on the destination's position contained in the packet and the position of the sending node's neighbors. Position-based routing hence does not need the setting up or maintenance of routes
Irrespective of the approach to routing, a routing protocol should be capable to automatically recover from any problem in a specific amount of time without human intervention. Traditional routing protocols are designed for static infrastructures and consider that routes are bidirectional, which is not always the case for ad-hoc networks. Determination of mobile terminals and correct packet routing to and from every terminal while moving are surely challenging.

IV. AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV [15] can be thought of as a integration of both DSDV and DSR. It borrows the basic on-demand strategy of Route Discovery and Route Maintenance from DSR, plus the usage of hop-by-hop routing, sequence o., and periodic beacons from DSDV. AODV is an on-demand routing protocol, which starts a route discovery procedure only when needed by a source node. When a source node S wishes to forward data packets to a destination D but cannot discover a route in its routing table, it floods a Route Request (RREQ) message to its neighbors, involving the last known sequence no. for that destination. Its neighbors then re-flood the RREQ message to their neighbors if they do not have a fresh enough route to the destination. (A fresh enough route is a valid route entry for the destination node whose related sequence no. is equal to or greater than that contained in the RREQ message.) This mechanism proceeds until the RREQ message arrive the destination node or an intermediary node that has a fresh enough route. Each node has its own sequence no. and RREQ ID1. AODV utilizes sequence no. to ensure that all routes are loop-free and have the most current routing information. RREQ ID in conjunction with source IP address uniquely determines a specific RREQ

message. The destination node or an intermediary node only accepts the first copy of a RREQ message, and discards the duplicated copies of the same RREQ message. Every node that sends the ROUTE REQUEST generates a *reverse route* for itself back to node S; after accepting a RREQ message, the target or intermediary node updates its reverse route to the source node utilizing the neighbor from which it obtains the RREQ message. The reverse route will be utilized to forward the corresponding Route Reply (RREP) message to the source – when the ROUTE REQUEST arrives a node with a route to D, that node creates a ROUTE REPLY that consist the no. of hops essential to arrive D and the sequence no. for D most recently viewed by the node creating the REPLY. Meanwhile, it updates the sequence no. of the source node in its routing table to the maximum of the one in its routing table and the one in the RREQ message. When the source or an intermediary node obtains a RREP message, it updates its *forward route* to the target node utilizing the neighbor from which it obtains the RREP message. It also updates the sequence no. of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message. A Route Reply Acknowledgement (RREP-ACK) message is utilized to acknowledge reception of a RREP message. The state generated in every node along the path from S to D is hop-by-hop state; i.e. every node remembers only the next hop and not the complete route, as would be performed in source routing.

V. ATTACKS in MANET

However, MANET is multi-hop in nature, it sturdily based upon the cooperation among the network nodes [3]. The guarantee of cooperation among nodes is needed. In current time we have viewed a variety of attacks have been determined and detected in the network. To offer a protected communication in the network we require to face the security challenges [6]. There are two major classes where we have to assume always in the security attacks, they are Active attacks and Passive attacks. A passive attack won't disrupt the MANET normal operation, while data have been interchanged from the network. The solely behavior of passive attack is to determine the data exchanged in the network The intruder snoops the data exchanged in the network without modifying it. Here the needs of confidentially gets violated. One of the solutions to the issue is to utilize powerful encryption technique to encrypt the data being transferred, thus building it impossible for the intruder to get useful information from the data overhead.

An Active attack always attempts to change the MANET normal operation, which means the disruption have been made in the network, i.e. doing data disruption, modification, deletion and fabrication. Active attacks can be external or internal. The information which is transferring through -the nodes in MANET is modified by an intruder node. Intruder node also streams some wrong information in the network. Attacker node also perform the task of route request though it is not authorized node so the other node rejecting its request because of these route requests the bandwidth is consumed and network is jammed. Some security attacks in the networks are Interception, Interruption and Modification. In *External attacks* the attacker objectives to cause network congestion which can be done by propagating wrong routing information or to disrupt the nodes from offering services [5]. The attacker always interrupts the nodes to avail the facilities. In internal attack, the attacker requires to obtain the access to participate in the network activities. Here the intruder comes with some malicious impersonation to get access from network as a novel node.

VI. GRAY HOLE ATTACK

Gray hole attack is the variation of Black Hole attack, in which the nodes will discard the packets selectively. Selective forward attack is of two kinds they are

(a) Dropping all UDP packets while sending TCP packets

(b) Dropping 50% of the packets or dropping them with a probabilistic distribution.

These are the attacks that look to interrupt the network without being determined by the security measures. Gray Hole is a node that can switch from acting correctly to acting like a black hole that is it is really an intruder and it will behave as a normal node. So we can't determine easily the attacker however it acts as a normal node. Each node manages a routing table that records the next hop node information which is a route packet to destination [9]. If a source node is required to route a packet to the destination node it utilizes a particular route and it will be checked in the routing table whether it is existed or not. If a node starts a route discovery procedure by broadcasting

Route Request (RREQ) message to its neighbor; by obtaining the route request message the intermediary nodes will manage their routing tables for back route to the source [10]. A route response message is forwarded back to the source node when the RREQ query arrives either to the destination node or to any

other node which has a current route to destination node. The Gray Hole attack has two phases:
Phase 1: A malicious node exploits the AODV protocol to show itself as having a valid route to destination, with the intention of disrupting packets of spurious route.
Phase 2: In this phase, the nodes have been discarded the disrupted packets with a certain possibility and the detection of Gray Hole attack is a complicated procedure. Generally, in the Gray Hole attacks the intruder acts maliciously for the time until the packets are discarded and then switch to their normal nature [8]. Both normal node and attacker are same. Because of this nature it is very complex to determine in the network to figure out such type of attack. The other name for Gray Hole attack is node misbehaving attack.

VII. TECHNIQUES OF GRAY HOLE ATTACK DETECTION AND PREVENTION

A. Neighborhood-based and Routing Recovery Scheme

Sun B et al. utilize AODV as their routing protocol and simulation is performed in ns2 modeler. The detection technique utilized neighborhood-based method to determine the gray hole/black hole attack and then show a routing recovery protocol to make the right path to the destination node. Depending on the neighbor set information, a mechanism is designed to deal with the black hole attack, which contains two parts: detection and response. In detection process, two major steps are: Step 1- Gather neighbor set information. Step 2-Determine whether there available a gray hole/black hole attack. In Response process, Source node forwards a modify-Route-Entry (MRE) control packet to the Destination node to build a correct path by altering the routing entries of the intermediate nodes (IM) from source to destination node. This technique efficiently and effectively determines black hole/gray hole attack without proposing much routing control overhead to the network. Simulation data represents that the packet throughput can be enhanced by minimum 15% and the false positive possibility is often less than 1.7%. The drawback of this technique is that it becomes useless when the intruder agrees to forge the fraud response packets. This technique published in year 2003 and the simulation is performed in NS-2 simulator.

B. Using watchdog/pathrater Scheme:

S. Marti, T. J. Giuli, K. Lai, and M. Baker [21] introduced to trace malicious nodes by utilizing watchdog/pathrater. In watchdog when a node sends a packet, the node's watchdog verifies that the next node in the path also sends the packet by promiscuously hearing to the next node's transmissions. If the watchdog discovers the next node does not send the packet during a pre-specified threshold time, the watchdog will accuse the next node as a malicious node to the source node; The introduced scheme has two limitations: 1) to scan the nature of nodes two or more hops away, one node has to trust the information from other nodes, which proposes the susceptibility that good nodes may be bypassed by malicious accusation; 2) The *watchdog* cannot distinguish the misbehavior from the receiver collisions, ambiguous collisions, collusion, controlled transmission power, partial dropping and false misbehavior. In *pathrater* algorithm every node utilizes the *watchdog's* scanned results to rate its one-hop neighbors. Further the nodes exchange their ratings, so that the *pathrater* can rate the paths and select a path with maximum rating for routing. Drawback of this algorithm is that the concept of exchanging ratings really opens door for blackmail attack.

C. Counter- Threshold Based & Query- Based Scheme

D.M. Shila; T. Anjali [3] provided a solution to protect selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first phase of the algorithm is Counter- Threshold Based and utilizes the detection threshold and packet counter to determine the attacks. The second phase is Query-Based and utilizes acknowledgment from the intermediary nodes to limit the intruder. In the first phase, two kinds of packets, Control packet and Control ACK packet, are utilized to find the attacker. Moreover, they determine the appropriate value of detection threshold depending on the routing Expected Transmission Count metric ETX to enhance the performance under various network conditions.

D. Aggregate signature algorithm

Gao Xiaopeng, Chen Wei [10] introduced to utilize aggregate signature algorithm to trace packet discarding nodes. The proposal was contained three related algorithms: (1) the creating proof algorithm. (2) The checkup algorithm. (3) The diagnosis algorithm. The benefits of this suggestion are: (1) the reliability is satisfying, as proof on sent packets is utilized; (2) the application scope is broad, as bidirectional communication connections are not essential; (3) the security is satisfying, as it is complicated for malicious nodes to flee detection; (4)

the bandwidth overhead is low, as nodes do not require to examine each other.

E. Centralized intrusion detection scheme based on Support Vector Machines

Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S and Ekercio Glu [11] showed a centralized intrusion detection scheme depending on sliding windows and Support Vector Machines (SVMs). This system can determine selective forwarding attacks and black hole attacks with high accuracy without the nodes depletion of their energy. They concentrate on following a simple classification based IDS to determine a particular spectrum of malicious DoS attacks i.e. the Selective Forwarding Attack, that may be established against a WSN. This IDS utilizes routing information local to the BS of the network and raises alarms depending on the 2D feature vector (hop count, bandwidth). Categorization of the data patterns is done utilizing a one-class SVM classifier. Support vector machines (SVMs) are a type of machine learning algorithms, originally to Vapnik. While originally developed for binary classification, they have been extended to involve density estimation, regression and one-class classification. Over the last decade, SVMs have achieved popularity because of their capability to tackle complicated highly nonlinear issues in a consistent structured way, while simultaneously avoiding issues of over fitting on simpler issue

F. Cross layer intrusion detection architecture based scheme

Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han (2010) introduced a new cross layer intrusion detection architecture to determine the malicious nodes and several kinds of DoS attacks by exploiting the information existed across various layers of protocol stack for improving the detection accuracy. They utilized cooperative anomaly intrusion detection with data mining mechanism to improve the introduced architecture. This architecture also determine sink hole attack at various layers of the protocol stack and determine various kinds of UDP flooding attack in an effective manner.

G. Channel appraised method

Vigilkumar V V, V. Mary Anita Rajam [5] introduced a channel appraised mechanism to determine colluding selective forwarding attack is assumed. The detection is performed in two steps. In the first step, the channel estimation is combined with traffic monitoring to obtain detection of selective forwarding attack, which can efficiently determine selective forwarding misbehavior hidden in the normal loss events because of worst channel quality or medium access collisions. In the second step, it combine colluding node detection strategy with detection of individual selective forwarding attack.

H. TWOACK scheme

K. Balakrishnan, D. Jing and V. K. Varshney [2] introduced a TWOACK technique which can be implemented as an add-on to any source routing protocol. Rather than determining specific misbehaving node, TWOACK technique determines misbehaving connection and then views to alleviate the issue of routing misbehavior by observing the routing protocol to neglect them in future routes. It is performed by forwarding back a TWOACK packet on successful reception of each data packet, which is allocated a static route of two hops in the direction opposite to that of data packets. Basic disadvantage of this technique involves it cannot differentiate exactly which specific node is misbehaving node. Sometime well behaving nodes became part of misbehaving connection and thus cannot be further utilized the network. Hence a lot of well behaved node may be neglected by network which results in losing of well behaved routes

VIII. CONCLUSION AND FUTURE WORK

A Gray Hole attack is one of the critical security issues in MANETs. It is an attack where a dangerous node impersonates a destination node by forwarding forged RREP to a source node that starts route discovery, and at last strips data traffic from the source node. In this paper a review on several available techniques for gray hole attacks detection in MANETs with their defects is shown. The detection mechanism which make usage of proactive routing protocol have better PDR and correct detection possibility, but have higher overheads. The detection mechanisms which make usage of reactive routing protocols have low overheads, but have high packet loss issue. Thus, we recommend having a hybrid detection mechanism which integrates the benefits of both proactive and reactive routing for future research direction. Although these may not be neglected in totality, there is a requirement for trade-offs to obtain a secure optimum performances. Depending on the above performance comparisons, it can be concluded that Gray Hole attacks influence network negatively. Thus, there is requirement for perfect detection and elimination techniques. The detection of Gray Holes in ad hoc networks is still assumed to be a challenging task. Future work is targeted to an effective Gray Hole attack detection and elimination algorithm with least delay and

overheads that can be used for ad hoc networks vulnerable to Gray Hole attacks.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Black Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] K. Balakrishnan, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] D.M. Shila and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Vigilkumar Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] , Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Gao Xiaopeng and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Sophia Kaplantzis, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] S. Marti,, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.