A Survey over Black hole Attack Detection in Mobile Ad hoc Network

Shahram Behzad Shahram Jamali
Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
Computer Engineering Department, University Mohaghegh Ardabili, Ardabil, Iran

Abstract
In a wireless mobile ad hoc network (MANET),Similar to other systems, there is a risk of external agent infiltration.These networks are basically no-infrastructure, meaning no routing such as router or switch is used. So, they are highly posed to the risk of damage or exhausting all their common behavior energy. Hence, there is a growing interest towards the methods which can warn the network against the black hole attacks and external agent infiltration. black hole attacks which are among the most dangerous network attacks one of such security issue in MANET, These attacks are induced through each nodes existing in the network, where the node sends confirmation RREP to RREQ, no matter what its routing table is or whether a route exists towards the node. By doing this, the black hole node can deprive the traffic from the source node. so as to get all data packets and drops it. In this paper, we survey the existing solutions ,classify type of attacks and black hole attacks.

Index terms
MANETs (Mobile ad hoc networks), Black hole attack, RREP,EERQ

1. Introduction

MANETs is an autonomous system in which different mobile nodes are connected to each other by wireless links. Mobile ad hoc networks are highly susceptible to routing attacks because of their dynamic topology and lack of any infrastructure. Each node has communicated as a peer- to - peer connection and having a direct connection with the neighbor nodes with in their transmission range. The network is a self-configuration that having abilities to discover and maintain the route without manual management. Moreover, ad hoc networks can also perform multi-hop wireless networks. In this way, ad-hoc networks have a dynamic topology such that nodes are mobile in nature, so that they can easily join or leave the network at any time. on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks [1]. Fig.1 shows The illustrated the Mobile ad-hoc network.

Figure 1 :Mobile ad hoc network

These challenges include open network Architecture, shared Wireless environment, demanding resource constraints, and, highly dynamic network topology. they introduce specific security concerns that are absent or less severe in wired networks. mobile ad hoc networks are vulnerable to Different types of attacks These include passive eavesdropping, active Intervention, Impersonation, denial-of service. Intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of an Manet. However, these methods address only a subset of the threats. Moreover, they are costly to implement. The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which monitor security status of the network and identify blach hole behavior. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a mobile ad hoc network may be compromisedin such a way that it may not be possible to detect their black hole behavior easily. Such blak hole nods can generate new routing messages to advertise Non Existent links, provide False link Position information, and flooding other nodes by routing traffic, thus Imposition Byzantine failing in the network. [2] Security in MANET [3] is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network

Manuscript received March 5, 2015
Manuscript revised March 20, 2015

functions at the early stages of their style. Unlike networks using specific nodes to support basic functions like data Forwarding, routing, and network administration, in ad hoc networks those functions are carried out by all accessible nodes. This very difference is at the core of the security problems that are specific to ad As Opposition to dedicated nodes of a conventional network, the nodes of an ad hoc network can't be trusted for the correct execution of critical network functions.There are many security issues which have been studied in recent years. For instance, wormhole attacks, black hole attacks [4], Especially, the misbehavior routing problem [5] is one of the popularized security threats such as black hole attacks. The rest of the paper is organized as follows. Section 2. Routing protocol in mobile ad hoc network. Section 3. Over view of reactive protocol .Section 4. Type of attack in mobile ad hoc network. Section 5. type of black hole attack .Section 6. related work. Last section presents the conclusion.

2. Routin Protocol In Mobile Ad Hoce Network

A. *Proactive (table driven)*

In this routing protocol is manet, nodes periodically broadcast their routing information to the neighbours. Every node needs to sustain their routing table which not only storage the adjoining nodes and reachable nodes but also the number of hops. In other words, all the every nodes have to evaluate their neighborhoods as long as the network topology has changed. hence, the disadvantage is that the overhead rises as the network size increment, a significant relationship overhead within a great network topology. but, the advantage is that network status can be immediately reflected if the black hole Aggressive joins. The most Familiar type of the proactive type (table driven) are destination sequenced distance vector (DSDV) [6] routing protocol and optimized link state routing (OLSR) [7] protocol.

B. *Reactive (on demand)*

In comparison with table-based routing protocols, in this category of protocols, not all updated routes are stored on each node; instead, the routes will be constructed whenever they are needed. When a source node wants to send one message to a destination, it will request the route discovery mechanisms to find a route to the destination (RREQ). Route remains valid until the destination is available or if is not for the long-term needs. Once a route to the destination is found, the RREP mechanism sends, in reverse, the route to the source node. AODV , DSR, TORA, some examples of need-based protocols.[8]

C. *Hybrid*

routing protocol combines the advantages of proactive routing and reactive routing to overcome the Defect of them. Most of hybrid routing protocols are developed as a hierarchical or layered network framework. Initially,proactive routing is employed to completely roll up the unfamiliar routing data, then using the reactive routing to maintain the routing data when network topology changes. The familiar hybrid routing protocols in manet are zone routing protocol (ZRP) [9] and temporally-ordered routing algorithm (TORA) [10]

3. Overview Of Reactive Protocol

D. *Dynamic Source Routing(DSR)*

DSR routing protocol is an on demand destination routing protocol where an accumulated node of the routes, including those destination routes known by the node, are stored. Here, the data entered to the route accumulation revealing new information about the current routes, are updated. Two main phases of this protocol are discovery and maintenance of the route. Once the source node wants to transmit a packet to the destination node, it scans its route hoard to determine whether it needs a route to destination or not. If there exists an appropriate route to destination, it uses the given route in packet transmission. On the other hand, if there not such a route, it initiates the route discovery process through packet distribution. When RREQ process is sent, the node waits for RREP and once the RREPs come from the nodes, it responses to the first arrived RREP. The node sends packets with this RREP, this route to its route cache and then starts to send data packets using the route included in the packet which in turn leads to ignoring other REEPs. Such a process leads to ignoring the security or insecurity of the route,

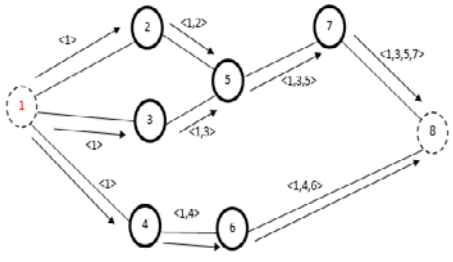

Figure 2 :depicts a discovery route in DSR protocol. (All-over distribution)

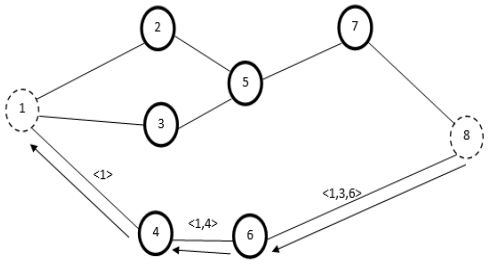

Figure 2-1: A sample of route discovery in DSR protocol

E. *Ad Hoc On-Demand Distance routing Protocol (AODV)*

AODV is a reactive protocol, where the route amongst the source and a destination node is created on an on-demand basis [29].Every mobile node maintains a routing table that hold track of the next hop node data for a route to the destination mobile node When a source mobile node wants to route a packet to a destination mobile node, it uses the determined route from the routing table to know the existing route to the destination node. If it does not finds the route in the table, it starts a route discovery process by broadcasting route request message to its neighbors, which is More spread until it reaches an intermediate node with a fresh enough route to the destination node or the destination node itself. Each intermediate node receiving the RREQ, Builds an entrance in its routing table for the node that forwarded the RREQ message, and the source mobile node. The destination mobile node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to the neighboring node from which it received the RREQ. An intermediate node Builds an entry for the neighboring node from which it received the RREP,then forward the RREP in the inverted Direction. Upon receiving the RREP,the source node updates its routing table with an entry for the destination node, and the node through which it received the RREP. The Source node will start routing the data packet to the destination node through the neighboring node that first responded with an RREP. The format of RREQ and RREP packet are shown in Table 2 and Table 2-1.

Table 2: RREQ Feild

Source address	Source sequence	Broadcast Id	Destination address	Destination sequence	Hop Count

Table 2-1: RREP Feild

Source address	Destination Address	Destination sequence	Hop Count	Lifetime

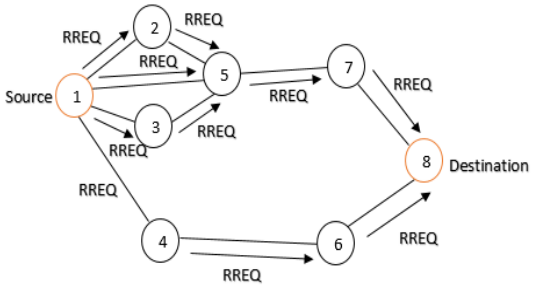

Figure 3: RREQ for Discover Route

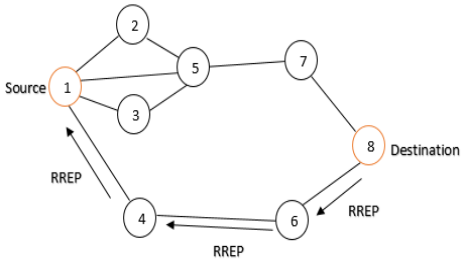

Figure 3.1: Route discovery in AODV protocol

4. Type of Attack in Mobile Ad Hoc Network

Attacks in MANET can be divided into two classes, according to the Criteria that whether the disrupt the operation of a routing protocol or not. These two classes are passive attacks and active attacks. In a inactive attack, the operation of the routing protocol is not disrupted by the attacker, and only attempts to discover valuable information by listening to the routing traffic is being done. Active attacks, however, involve actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network. Some typical kinds of active attacks can be easily performed against MANET, regarded as, flooding attack, selfing attack, gray hole attack, rushing attck, spoofing, wormhole attack, sleep deprivation and impersonation [12]. As mentioned, weak infrastructure in mobile ad-hoc networks exposed them to a large amount of attacks. One of these attacks is the black hole attack [13]. Black Hole in the (network layer attacks): all packets dropped by a Forged routing packets, the attacker can route all packets for some destination Themselves and then discard them,

5. TYPE OF BLACK HOLE ATTACK

F. *Single black hole attack*

In single black hole attack only one malicious node attack on the route.

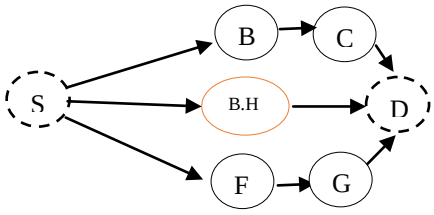

Fig 4. Single black hole attck

A. *Co-operactive black hole attack*

Co-operative Black Hole means the black hole nodes act in a group.

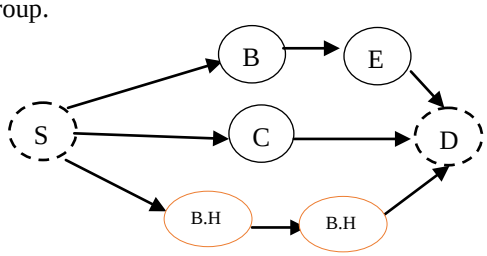

Fig 5. Co-operactive black hole attck

B. *Overview Of Black Hole Attack*

In this attack, a black hole node tries to send fake RREPs to route requests in order to advertise itself as having the shortest path to the destination. These false RREPs deceive the source to divert the traffic of the network toward the black hole node for either eavesdropping or absorbing traffic to drop the data packets [14]. Cooperative black hole attack occurs when several malicious nodes cooperate to each other in order to absorb data packets. black hole attack, a malicious node uses its routing protocol in order to With the release of false news,having the shortest path to the destination node or to the packet it wants to avoid the. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. in the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [15]. In protocol based on flooding, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole and forged route is Creation. When this route is create, now it's up to the node whether to drop all the packets or forward it to the unknown address [16].The Solution how black hole node Proportional in the data routes varies. Fig. 4 showhow black hole Problems, here node "E" want to send data packets to destination node "D" and The initial process of route discovery. So if node "F" is a black hole node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "E" before any other node. In this way node "E" will think that this is the active route and thus active route discovery is complete. Node "E" will ignore all other replies and will start seeding data packets to node "F". In this way all the data packet will be lost consumed or lost.

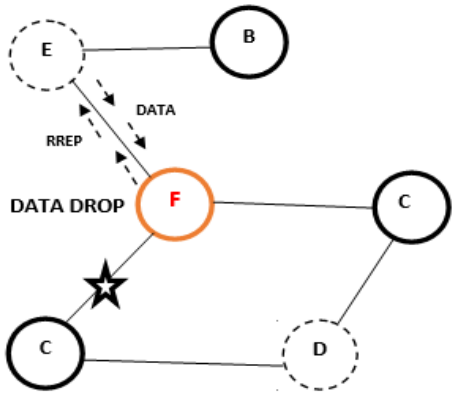

Figure 6 : Problems of black hole attacks

6. Related Work

In neighbors trust schemes,A node may request To accept the next Neighbors to verify the compliance of the package or Check do a node represents a procedure that is black hole nodes or based on good behavior. Considering that it is trustworthiness Calculated through several explanations of Activities neighbors. Below are some The solution is described.

C. *Redundant Route and Unique Sequnce Number*

Mohammad Al-shurman et al. proposed wo method .a single of them was based on searching Further than one path from source to destination. In this solution, The principle node broadcasts a ping packet route request (RREQ) to the destination. Between all of the nodes, the intermediate nodes those possessing a path to destination send the Route Reply (RREP) packet back to the source, then the source node buffers RREP packets until finding more than two packets. It Judgment that at the same time, lowest two routes present from source to destination. among these paths source nodes identifies the best and safest route based on the number of hops and nodes and prohibits the black hole Attack [17]. Due to the extra processed RREPs, in this method provides additional

computational overhead. In addition, if no shared node is identified then the source node will delay or leave the transmission of the packet data, leading to Significant degradation of the network efficiency [18]. Confronting with these problems, the second method has by proposed. This solution only provides detection of a single black hole attack and cannot detect a chain of malicious nodes which is called cooperative black hole attack. An idea of the exclusive sequence number [19] is mentioned in the second method. The sequence value is gathered; therefore, it would be ever higher than the current sequence number. In this method, two values are required to be recorded in two additional tables. The first one is the last-packet-sequencenumbers for the last packet sent to every node and the second one is for the last packet received. These two tables can be up-to-date automatically, when any packet is transmit or Receipt and according to these two table amount, the sender nodecould Recognition whether there is malicious nodes or not [20]. This method is faster than the earlier one, however a black hole node can easily evaluate the traffic passing from its vicinity and revise its tables by the sufficient packet sequence number, so it avoids the detection program

D. *(BDSR) Scheme*

In order to detect malicious intermediate nodes The solution was a fake RREP , 2011. First , before the routing Discovery process , the source node sends the bait Depending RREQ.Target address of the RREQ Package is not genuine and completely random. To avoid blocking the traffic problem Network bandwidth unoccupiying, live RREQ Closed only for a short period of time. Therefore, the black hole nodes can be identified in the first phase , Very simple, because the RREQ packet Make a fake RREP packet RREP packet Additional Field RREP sender records Packages . Hence, nodes and their black holes Position can be known by the source node . Then all The answer must be sent by malicious nodes Deleted. After that , DSR original used The routing discovery process . While the rate Delivered is less than a threshold value , DSR will again prey to detect Suspicious nodes [21]. The solution was to simulate QUALNET While the simulation results show a good rate of Packet delivery rate without excessive overhead . Is only slightly higher overhead than DSR routing Protocol. However, these solutions can not detect Cooperative black hole attack.

E. *DRI Table and Cross Checking Scheme*

Hesiri Weera singhe et al. proposed an algorithm to identify Collaborative black hole attack. Within this the AODV routing protocol is slightly modified by adding an additional table i.e. Data routing information (DRI) table and cross checking using further request (freq) and further reply (FREP). If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (route request) message to discover a secure route to the destination node same as the AODV. each node received this RREQ either Reply for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination Reply, All intermediate nodes update or insert routing entry for that destination since we always believe destination. Source node also trusts on destination node and will start to send data along the path that replies comes back. Also source node will update the (dri) table with all intermediate nodes between source and the destination. the simulation was in simulator qualnet. The algorithm is Comparison with the main AODV in terms of throughput, packet loss rate, delay and control data packet overhead. The results of the simulation that the main AODV is affected by cooperative black holes and it presents good performance in terms of throughput and minimum packet loss percentage compared to other solutions [22,23].

F. *Time-base Threshold Detection Scheme*

Tamilselvan L et al. proposed a solution based on an Enhancement of the original AODV routing protocol. The Main concept is Settings timer To collect the other request from other nodes after receiving the first Demand. It stores the packet's sequence number and the received time in a table named collect route reply table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value. [24] the results shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But delay might be Obvious raised when the black hole node is away from the source node.

G. *(MRR) MultipleRoute Replies(MRR)*

In the authors have discussed the AODV protocol that suffers from the Black hole attack in MANETs and has proposed a realistic solution for the black hole attacks, which can be implemented on the AODV protocol. This mechanism expects a source node to wait until an RREP packet arrives from more than two nodes. With getting multiple RREPs, the source node Review whether thither is a shared hop or not. If there is, the source node confirms that the route is safe and can be used. The main drawback of this solution is that it introduces time delay, because it has to wait until multiple RREPs arrive [25].

H. *Improving Routing Discovery for AODV to Prevent Blackhole*

Rutvij,et al. investigated on some of the existing approaches for black hole and gray hole attack and presented a novel solution against these attacks which is

able to find effectively short and secure routes to destination. Their own theoretical evaluation illustrated that this approach properly can increase packet delivery ratio (PDR) with negligible difference in routing overhead. The authors thought that this algorithm could be used for the other reactive protocol and also finds and eliminates malicious nodes within the route finding Stage. Nodes receiving RREP confirmed the truth of routing information;source node broadcasts a list of malicious nodes when send RREQ. Nodes update route tables when from any information of blackhole nodes from received routing packets.No additional and control packet can be mentioned as benefit of this algorithm and there is minor difference in routing overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Additionally, the black hole nodes would be isolated and packet delivery ratio (PDR) will greatly be improved [26].

I. *Risk Mitigation Of Black hole Attack*

the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attacks. In this method, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. Soon after receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it is the route, Therefrom sends the CREP to the source. After receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are coordinated, the source node judges that the route is appropriate. One drawback of this method is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, which is, when the Next Hop node is a colluding attacker sending CREPs that support the incorrect path.[27].

J. *Detection Black hole Attack on Aodv*

the authors analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is adequately. Based on this evaluation, the authors propose a statisticalbased anomaly detection approach to detect the blackhole attack, based on dissimilarities between the destination sequence numbers of the received RREPs. The important thing of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require adjustment of the Available protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.In [28].

K. *Detection Black hole attack on Aodv-based mobile ad hoc network*

Xin Li et al. proposed a trust model based on Packet forwarding Ratio (PFR). PFR measured at a node based on ratio of number of packets forwarded to the number of Data packets received. According to PFR, confidence will be assigned to the node. If node forwards packets correctly trust val ues increases otherwise Confidence values diminishes. In this Confidence model, trust values are allocated in the range between 0 to I .The trust value 0 signifies distrust node and trust value I signifies absolute trust. Confidence value among 0 to 0.5 treated as black hole node, value among 0.5 to 0.75 treated as suspected node, 0.75 to 0.9 A less reliable node, 0.9 to 1 treated as trust w0l1hy node. If node has less Confidence values, it is not allowed to send data packets for forwarding [29].

7. Conclusion

A survey of we have the characteristics of manet and about.ad hoc networks are vulnerable to the attacks.The attacks can carry the different determinants that mainly focus on Impersonation, denial of service, One of these attacks, Black hole attacks, is a main security threat that degrades the performance of the reactive and proactive routing protocol. These attacks are induced through each nodes existing in the network, where the node sends confirmation RREP to RREQ, no matter what its routing table is or whether a route exists towards the node. Its detection and defence this type attacks is the main matter of concern. many researchers have conducted diverse method to propose different types of detection and defence mechanisms for black hole problem. The black hole problem is still an active research area. This paper a survey on the various techniques that are employed in the prevention of black hole attacks in an ad hoc network with the reactive and proactive routing protocol. Each technique has advantages and disadvantages of their own.

Table 2. A Summary of proposed Methods

Technique proposed by	Techniques Solutions	Type of attack	Routing protocol	Results
Mohammad Al shurman et al.	Black hole attack in mobile ad hoc networks	Black hole	AODV	presents good performance in terms of throughput and minimum packet loss
Djahel, S., F. Naït-Abdesselam, and Z. Zhang,	Mitigating packet dropping problem in mobile ad hoc networks	Black hole	AODV,DSR	presents good performance in terms of ovr head
Lin, C.,et al	AODV routing implementation for scalable wireless Ad-hoc network simulation	Black hole	AODV	Better results than conventional methods in conventional aodv
BTsou, P.C., et al.	Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in	Black hole	DSR. Reactive and Proactive protocol	Better result in Compared to conventional DSR and other metric
K. Makki, N. Pissinou,et al	Solutions to the black hole problem in mobile ad-hoc network,"	Black hole	AODV	good performance in terms of throughput and,packet loss
J. Grønkvist, A. Hansson,et al	Evaluation of a Specification-Based Intrusion Detection System for AODV.	Black hole	AODV	Better result in packet delivery ratio,end to end delay
Rutvij, Sankita and Devesh	Improving Routing Discovery for AODV to Prevent Blackhole	Black hole	AODV	Improvement packet delivery ratio (PDR
S. Kurosawa et al.	Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method	Black hole	AODV	good performance in anomaly detection.and better result in other metric
Xin Li et al.	Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method	Black hole	AODV	Good performanceresult in packet delivery ratio,end to end delay

REFERENCE

[1] Hao yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications, February 2004.

[2] Y.C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," Proc. 2nd ACM workshop on Wireless security (WiSe '03), 2003, pp. 30-40, doi:10.1145/941311.941317.

[3] Ipsa De, Debdutta Barman Roy, "Comparative study of Attacks on AODV-based Mobile Ad Hoc Networks", International Journal on Computer Science and Engineering (IJCSE)

[4] Umang S, Reddy BVR, Hoda MN (2010) Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 4(17):2084–2094. doi: 10.1049/ietcom. 2009.0616

[5] Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Paper presented at the 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, 6-11 August 2000

[6] Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Paper presented at the ACM

SIGCOMM'94 Conference, London, United Kingdom, August 31 - September 2, 1994
[7] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001
[8] Shahram Behzad, Reza Fotohi, Shahram Jamali,"Improvement over the OLSR Routing Protocol in Mobile Ad Hoc Networks by Eliminating the Unnecessary Loops", IJITCS, vol.5, no.6, pp.16-22, 2013. DOI: 10.5815/ijitcs.2013.06.03
[9] Haas ZJ, Pearlman MR, Samar P (2002) The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft
[10] Park V, Corson S (1998) Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group
[11] Reza Fotohi, Shahram Jamali, Fateme Sarkohaki, Shahram Behzad,"An Improvement over AODV Routing Protocol by Limiting Visited Hop Count", IJITCS, vol.5, no.9, pp.87-93, 2013. DOI: 10.5815/ijitcs.2013.09.09
[12] Jathe, S.R. and D.M. Dakhane, A Review Paper on Black Hole Attack and Comparison of Different Back Hole Attack Techniques. International Journal of Cryptography and Security, 2012. 2(1): p. 22-26.
[13] Dokurer, S., Simulation of Black hole attack in wireless Ad-hoc networks. 2006: Atilim University.
[14] Malik, M., On Demand Routing Protocols in Mobile Networks. International Journal of Research in Science And Technology (ijrst), 2012. 1(Apr-Jun).
[15] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
[16] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006
[17] Al-Shurman, M., S.M. Yoo, and S. Park. Black hole attack in mobile ad hoc networks. 2004: ACM.
[18] Djahel, S., F. Naït-Abdesselam, and Z. Zhang, Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. IEEE Communications Surveys and Tutorials, 2011. 13(4): p. 658-672.
[19] Lin, C., AODV routing implementation for scalable wireless Ad-hoc network simulation (SWANS). httpy/jist. ece. cornell. 2004.
[20] Mojtaba Alizadeh, Wan Haslina Hassan, Mazleena Salleh, Mazdak Zamani, Eghbal Ghazi Zadeh. Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID. Journal of Next Generation Information Technology.
[21] Tsou, P.C., et al. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 2011:IEEE.
[22] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.
[23] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.
[24] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.
[25] Modified AODV Protocol against Black hole Attacks in MANET by K. Lakshmi1, S.Manju Priya, A.Jeevarathinam, K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore, International Journal of Engineering and Technology. Vol.2 (6), 2010.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
[26] Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. 2012 Second International Conference on Advanced Computing & Communication Technologies. 2 (2), p535-540.
[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.
[28] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.
[29] Xin Li , Zhiping Jia, Peng Zhang, Haiyang Wang, "A Trust-based MuItipath Routing Framework for Mobile Ad Hoc Networks" , 7th FSKD, 20 I O.

Shahram Behzad received his B.Sc. in computer engineering from Parsabad University, Parsabad, Iran, in 2008 and his M.Sc. in computer engineering from Azad university of Germi branch, Ardabil, Iran, in 2013. His research interests Mobile Ad-Hoc Networks, Performance Evaluation and Optimization algorithms.

Shahram Jamali received the B.Sc. degree in electrical and computer engineering from Amirkabir University of Technology, Tehran, Iran, in 1999, the M.Sc. degree in Architecture of Computer Systems from Iran University of Science & Technology - IUST, Tehran, Iran, in 2001, and the Ph.D. degree in Architecture of Computer Systems from 2008. He is currently associate professor of computer engineering at University of Mohaghegh Ardabili (UMA), His research interests include Congestion control in computer networks, UPFC Controller design, Load balancing in Grid environment.