International Journal of Computer Networks and Communications Security

VOL. 4, NO. 12, DECEMBER 2016, 322–329
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Description of Black Hole Attack Behaviour in MANET

Asma Ahmed[1], A. Hanan[2] and Izzeldin Osman[3]

[1]Faculty of Computer Science and Information Technology, University of Tabuk, Tabuk, Saudi Arabia

[2]Faculty of Computer Science and Information System, Universiti Technologi Malaysia, Johor, Malaysia

[3]Faculty of Computer Science, Sudan University Science and Technology, Khartoum, Sudan

ABSTRACT

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders answer each route request with fake route reply to advertise its self-have a shortest route to the destination. In This paper a full description of black hole behaviour is presented, and state-of-the-art ways to detect and eliminate black hole attacks in existing solution are discussed, as well as analyse the categories of these solutions and provide a comparison table.

Keywords: *Mobile Ad hoc Networks, Routing Protocols, Black Hole Attack.*

1 INTRODUCTION

Mobile Ad Hoc Network (MANET) is autonomous and decentralized wireless systems. MANETs often suffer from security attacks because of their specification such as open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and unclear defense mechanism. The network-layer security designs for MANETs are concerned with protecting the network functionality to deliver packets between mobile nodes through multihop AdHoc forwarding. Therefore, they seek to ensure that the routing message exchanged between nodes is consistent with the protocol specification, and the packet forwarding behaviour of each node is consistent with its routing states [1]. During the route discovery process of on-demand routing protocols, an attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called black hole attack [2], and is a "passive" and simple way to perform a Denial of Service (DoS). The attack can be done selectively (drop routing packets for a specified destination, and may have the effect of making the destination node unreachable or downgrade communications in the network. The Black hole attack is an important problem that can occur *i*n ad Hoc Networks especially in popular on demand routing protocols like AODV [3].

The aim of the paper is to description the balck hole attack behviour, and analysis the existing solution that proposed to to detect and eliminate black hole attacks.

The rest of paper is organized as follows: Section II provide an overview of routing protocols in MANET. Section III and Section IV, respectively introduce the black hole attack and describe the behaviour of balck hole attack in AODV routing protocol and also provide the comparison between and the solutions that are proposed to overcome the attack. The paper is concluded with plan for future work in Section V.

2 BACKGROUND

A Routing Protocol is a protocol that specifies how routers communicate with each other. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing [4][5][7].

A. Proactive (Table driven) Routing Protocols

Proactive protocols maintain the routing information even before it is needed. In these protocols, each node has to keep up-to-date routing tables. To maintain reliable routing tables, every node propagates the update messages to the network when the network topology changes. Therefore, the disadvantage is that the overhead rises as the network size increases, a significant communication overhead within a larger network topology. However, the advantage is that network status can be immediately reflected if the malicious attacker joins. Some of the existing proactive ad hoc routing protocols are: Destination-Sequenced Distance-Vector (DSDV) [10], Wireless Routing Protocol (WRP) [11], Fisheye State Routing (FSR) [12], and Optimized Link State Routing (OLSR) [13].

B. Reactive (on-demand) Routing Protocol

Reactive or on-demand routing protocols create routes only when they are needed [14]. Unlike the proactive routing, the reactive routing is simply started when nodes desire to transmit data packets. When the source node wants to connect to the destination node, it propagates the route request packet to its neighbors. Just as neighbors of the source node receive the broadcasted request packet, they forward the packet to their neighbors and this action is happen until the destination is found. Afterward, the destination node sends a replay packet the source node in the shortest path. The route remains in the route tables of the nodes through shortest path until the route is no longer needed. Here we briefly describe two on-demand routing protocols which are Ad Hoc On-Demand Distance Vector (AODV) [3][15] and Dynamic Source Routing (DSR) [16][17].

AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can't be reached from the source node, the route discovery process will be executed immediately. In the route discovery phase, the source node broadcasts a Route Request (RREQ) message to all its neighbors. If the node is the destination or the node has a route to the destination that meet the freshness requirement, it unicasts a Route Reply (RREP) back to the source node. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. When a link break occurs, *RouteError* (RERR) packets are propagated along the reverse path to the source node invalidating all broken entries in the routing table of the intermediate nodes.

In DSR each data packet contains the routing path from source to destination in their headers. Unlike the AODV which only records the next hop information in the routing table, the mobile nodes in DSR maintain their route cache from source to destination node. That means the routing path can be determined by source node because the routing information is recorded in the route cache at each node

C. Hybrid Routing Protocol

Hybrid routing protocols in MANET aggregates a set of nodes into zones in the network topology [18]. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. These protocols use proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols. In terms of the above discussion, nodes are grouped into zones based on their geographical locations or distances from each other. Inside a single zone, routing is done using table-driven mechanisms while an on-demand routing is applied for routing beyond the zone boundaries. The familiar hybrid routing protocols are the Zone Routing Protocol (ZRP)[18][20] and Zone-based Hierarchical Link State (ZHLS) [19].

3 BLACK HOLE ATTACK

Black holes refer to places in the network where incoming traffic is silently discarded or dropped, without informing the source that the data did not reach its destination. In Black hole attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other. These black hole nodes are invisible and can only be detected by monitoring the lost traffic.

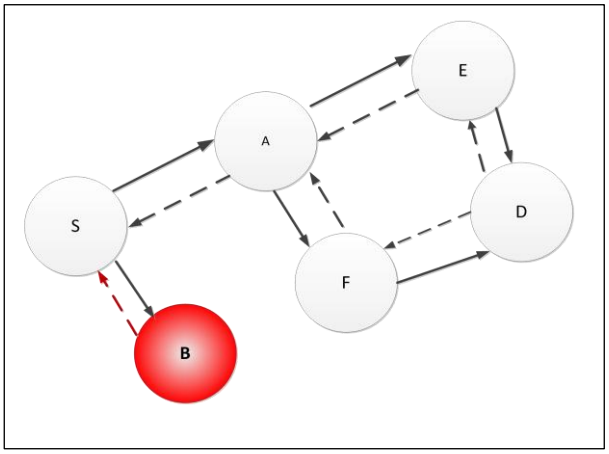

Fig. 1. Black hole attack behavior

An example of black hole attack is shown in Figure 1. The source node S constructs a route in order to communicate with destination node D. Source node S sets its RREQ and broadcasts it. Upon receiving RREQ every node forwards the RREQ since it is not the destination node. The attacker B sends spoofed RREP that it has the quickest route to the destination node. Therefore node S erroneously judges the route discovery process with completion, and starts to send data packets to node B. As mention above, the traffic from the source node S to the destination node D is deprived by malicious node B, then it probably drops or consumes the packets. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

A. Description of black hole attack

The black hole attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (black hole), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. Black hole attack in MANETs is a serious security problem to be solved. In order to launch a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the route forwarding path of data or control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network. Thus, any node can easily misbehave and provide a severe harm to the network by targeting both data and control packets. Dropping data packets leads to suspend the ongoing communication between the source and the destination node. More seriously, an attacker that captures the incoming control packets can prevent the associated nodes from establishing routes between them. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs' sequence number. Upon receiving a number of RREPs, the source node selects the one with the greatest sequence number in order to construct a route. But, in the presence of black hole attack when a source node broadcasts the RREQ message for any destination, it immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole node and discards other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole node trusting that these packets will reach the destination. Thus the black hole node will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard them. Thus the packets attracted by the black hole node never reach the destination. Thus, the black hole attack often results in very low packet delivery ratio. In AODV, the black hole attack takes place after the attacking node receives RREQ for the destination node that it is going to impersonate. To succeed in the black hole attack, the attacker must generate its RREP with sequence number greater than the sequence number of the destination [22]. Upon receiving RREQ, the attacker sets the sequence number of RREP as a very high number, so that the attacker node can always attract all the data packets from the source and then drop the packets.

The implementation of black hole attack in AODV routing protocol consists of two steps. They are:

Step 1 : Sending False RREP with Highest Sequence Number and Lowest Hop Count.

Step 2 : Consuming its own packets but dropping other packets routed through black hole node.

B. Creation of False RREP

As the first process in black hole attack, when the black hole node receives any RREQ, it immediately sends the fake RREP to the source node. The Figure 2. shows the scenario, in which, the attacker

node A is sending fake Route Reply (RREP) to the source node S.

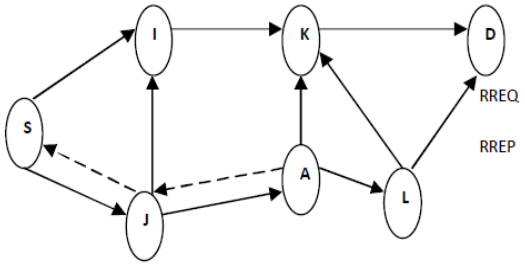

Fig. 2. RREP from a Black Hole Node

In this scenario, S is the source node, D is the destination node, A is the black hole node and I,J,K and L are intermediate nodes. Here, attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes.

C. Dropping Routed Packets

Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A and sends all its data packets to the destination through the black hole node A. Thus, by sending false route reply, the black hole node attracts all the data packets towards it. When it receives packets, if the packets are intended to it, then it consumes them otherwise, it simply drops the packets.

4 CONVENTIONAL DETECTION SCHEMES FOR BLACK HOLE ATTACK

This section classified the detection scheme in two types they are:

A. Routing Procedure Secure Schemes

1) RREP packet with next hop information

H. Deng, W. Li, and D. P. Agrawal [25] proposed a method that require the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route.

2) Route Confirmation Request (CREQ)

In [26], the author proposed the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon 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 matched, the source node judges that the route is correct.

3) Verifies the authenticity of node that initiates RREP

M. Al-Shurman, S-M. Yoo, and S. Park [22], proposed a method that source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops (in ad hoc networks, the redundant paths in most of the time have some shared hops or nodes). From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired.

B. Anomaly Detection Schemes

1) Anomalous Specification behaviour Method

Huang and Lee [27] they utilize an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; modelize normal state; and detect attacks with both specification-based detection and anomaly

detection. A Route Discovery process starting from the source node delivers the initial *Route Request* until the source node receives the *Route Reply* message and establishes a route to the destination. If all of its operations are performed in the specified order, it is considered to display a normal behaviour. In specification based detection, they simply detect attacks as deviant packet from condition defined by EFSA. In anomaly detection, they define normal state and compare it with condition of EFSA and amount of statistic of transition; that is the threshold is used and the feature is defined as the number of time that the destination sequence number is greater than the threshold. and then detect attacks as a deviation from those states.

2) Cross-Feature Method

Huang, Fan, Lee and Yu [28] propose a method in which the packet flow is observed at each node. The cross-feature method organize as the follows:

1- Define features that include both traffic related and non-traffic; that is topology related features.
2- Then study the correlations between one feature and all other features, and suggest anomaly detection means with this interrelation.

3) Profile based neighbor monitoring method

Wang, Lin and Wong [29] proposed propose a profile-based intrusion detection system that each node monitor its neighbor's traffic and builds a profile for each of its neighbors. Holding the profile, a node can use it to monitor its neighbor nodes' behavior. Once the traffic feature exceeds a certain threshold an alert should be reported.
They see that the features each node is monitoring are too many so in feature selection, they infer the related features from the Markov blanket and try to decrease the number of features without affecting the detection rate.

They adopt score-based approach to learn the Bayesian network structure from the training data. They then adopt hill-climbing has been used to search the best quality network structure. After obtaining the best network structure, they infer the Markov Blanket from the network structure.

4) Dynamic Training Approach

Kurosawa, Nakayama, Kato, Jamalipour and Nemoto [30] proposed an anomaly detection scheme uesing dynamic training technique. In this method, the training data is updated at regular time intervals to adopt with dynamically changes of network topology to defining the normal state. In normal state each node's sequence number changes depending on its traffic conditions. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. They investigate that when the attack took place, regardless of the environment the sequence number is increased largely. Also, usually the number of sent out RREQ and the number of received RREP is almost the same. From these reasons they use the following features to express the state of the network.

- Number of sent out RREQ messages
- Number of received RREP messages
- The average of difference of Dst Seq in each time slot between the sequence number of RREP message and the one held in the list

Here, the average of the difference between the Dst Seq in RREQ message and the one held in the list are calculated. When sending or forwarding a RREQ message, each node records the destination IP address and the Dst Seq in its list. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of Dst Seq is calculated, and this operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as the feature.
Table 1 shows the comparison of balckhole detection scheme.

Table 1: comparison f balckhole detection schemes

Detection Schemes	Methods	Proc and Cons
Routing Procedure Secure Schemes	- RREP packet with next hop information - Route Confirmation Request (CREQ)	In these methods, the routing protocol has to be modified. The operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth constrained.
	- Verifies the authenticity of node that initiates RREP	This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay because many RREP packets have to be received and processed by the source. In addition, if there are no shared nodes or hops between the routes, the packets will never been sent.
Anomaly Detection Schemes	-Anomalous Specification behaviour Method -Cross-Feature Method -Profile based neighbor monitoring method -Dynamic Training Approach	The change of network states can be caused by mobility; and it may also occur due to the sudden participation and disappearance of nodes in a MANET. When the nodes in the current MANET differ from those in the training data, the defined baseline profile cannot express the current network state.

5 CONCLUSIONS AND FUTURE

Due to security vulnerabilities of routing protocol, however, mobile ad hoc network may unprotected against attacks cause by the malicious node. Blackhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. Blackhole attacks cannot be prevented by cryptographic measures as in a blackhole attack they attackers coming from the authorized node. In this paper, the overall concept of AODV routing protocol in MANET has been explained. The black hole attack and characteristics against AODV is describes. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

6 REFERENCES

[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. Hu, A. Perrig, and D. Johnson., (2002) "Ariadne: A secure on-demand routing protocol for ad hoc networks". In Proceedings of ACM MOBICOM'02.

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

[4] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Publications, 2002.

[5] Royer EM, Toh C-K (1999) A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications 6(2):46–55. doi: 10.1109/98.760423

[6] Sanzgiri K, Dahill B (2002) A Secure Routing Protocol for Ad Hoc Networks. Paper presented at the 10th International Conference on Network Protocols, Paris, France, 12-15 November 2002

[7] Xiaoyan Hong, Kaixin Xu, and Mario Gerla.(2002) Scalable routing protocols for mobile ad hoc networks.

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

[9] M.Abolhasan, T.Wysocki, E.Dutkiewicz, “ A Review of Routing Protocols for Mobile Ad Hoc Networks,” Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[10] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Com- mun. Rev., Oct. 1994, pp. 234-44.

[11] C.K.Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems,” Prentice Hall Publications, 2002.

[12] Guangyu Pei; Gerla, M.; Tsu-Wei Chen; (2000) “Fisheye state routing: a routing scheme for ad hoc wireless networks,” IEEE International Conference on Communications, 2000.

[13] Th. Clausen et al., (2003) “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietfmanet- olsr-11.txt.

[14] C.M barushimana, A.Shahrabi, (2003) “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684.

[15] Farooq Anjum and Petros Mouchtaris (2007), "SECURITY FOR WIRELESS AD HOC NETWORKS", Copyright © 2007 by John Wiley & Sons, Inc. for MANETs in adversarial environments. IEEE Transactions on Vehicular Technology. 58(1), 449 - 460. ISSN 00189545.

[16] D. B. Johnson et al., (2004). “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),” IETF Draft, draft-ietf-manet-dsr-10.txt.

[17] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[18] Pearlman, Marc R., Haas, Zygmunt J. (1999) : Determining the Optimal Configuration for the Zone Routing Protocol, August 1999, IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8.

[19] Haas, Zygmunt J., Pearlman, Marc R., Samar, P. (2001): Interzone Routing Protocol (IERP), June 2001, IETF Internet Draft, draft-ietf-manet-ierp-01.txt.

[20] Haas ZJ, Pearlman MR, Samar P (2002) The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft

[21] Xu, Y. and Xie, X. (2008). Security analysis of routing protocol for MANET based on extended Rubin logic. Sanya, China.

[22] M. Al-Shurman, S-M. Yoo, and S. Park, (2004) “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf.

[23] Levent, E. and Chavan, N. J. (2007). Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs. IJCSNS International Journal of Computer Science and Network Security. 7(4), 48–61.

[24] H. Deng, W. Li, and D. P. Agrawal, (2002) “Routing security in ad hoc networks,” IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75.

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

[26] S. Lee, B. Han, and M. Shin, “Robust routing in wireless ad hoc networks,” in ICPP Workshops, pp.73, 2002.

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

[28] Huang, W. Fan, W. Lee and P. Yu, “Cross-Feature analysis for detecting ad-hoc routing anomalies”, Proc. of the 23rd IEEE Intl Conference on Distributed Computing Systems (ICDCS'03), May 2003.

[29] X. Wang, T. Lin and J. Wong, “Feature selection in intrusion detection system over mobile ad-hoc network,” Technical Report, Computer Science, Iowa State University, 2005.

[30] Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Proc. Int’l. J. Network Sec., 2007.

[31] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, “Authenticated routing for ad hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610,Mar. 2005.

[32] Asma Ahmed, A. Hanan, Izzeldin M., Yahia A, 2012. “Detection Techniques in MANET”, in Proceedings of the 2012 International Conference on Wireless Networks (ICWN'12), July 16-19 Nevada, USA.

[33] Xu, Y. and Xie, X. (2008). Security analysis of routing protocol for MANET based on extended Rubin logic. Sanya, China.

[34] Kim, J. and Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Networks. 7(6), 1097 - 1109. ISSN 15708705.