AODV Robust ($AODV_R$): An Analytic Approach to Shield Ad-hoc Networks from Black Holes

Mohammad Abu Obaida[1]
Dept. of CSE
DUET
Gazipur, Bangladesh

Shahnewaz Ahmed Faisal[2]
Dept. of CSE
KUET
Khulna, Bangladesh

Md. Abu Horaira[3]
Software Engineer
DataSoft BD Ltd
Chittagong, Bangladesh

Tanay Kumar Roy[4]
Dept. of CSE
KUET
Khulna, Bangladesh

***Abstract*—Mobile ad-hoc networks are vulnerable to several types of malicious routing attacks, black hole is one of those, where a malicious node advertise to have the shortest path to all other nodes in the network by the means of sending fake routing reply. As a result the destinations are deprived of desired information. In this paper, we propose a method AODV Robust ($AODV_R$) a revision to the AODV routing protocol, in which black hole is perceived as soon as they emerged and other nodes are alerted to prevent the network of such malicious threats thereby isolating the black hole. In $AODV_R$ method, the routers formulate the range of acceptable sequence numbers and define a threshold. If a node exceeds the threshold several times then it is black listed thereby increasing the network robustness.**

Keywords- Ad-hoc Networks; Wireless Networks; MANET; RT; AODV; Ad-hoc Optimal Distance Vector; Black-hole; OPNET.

I. INTRODUCTION

Ad-hoc networks are exemplified by dynamic topology, self-configuration, self-organization, constrained power, transitory network and lack of infrastructure. Characteristics of these networks lead to using them in disaster recovery operation, smart buildings and military battlefields [3].

Mobile Ad-hoc Network (MANET) routing protocols are classified into two basic classes, proactive and reactive [2]. In proactive routing protocols, routing information of nodes is exchanged intermittently, such as DSDV [4]. However, in on-demand routing protocols nodes exchange routing information as required such as, AODV [1] and DSR [5]. The AODV routing protocol [13] is an adaptation of the DSDV protocol for dynamic link conditions.

AODV is used to find a route between source and destination as required and this routing protocol uses three significant type of messages, route request (RREQ), route reply (RREP) and route error (RERR). Ground information of these messages, such as source sequence number, destination sequence number, hop count and etc is explicated in feature in [1]. Each of the nodes has a routing table (RT), which contains information about the route to the particular destination. When source node desires to communicate with the destination and if in routing table there is no route between, source node broadcasts RREQ initially. As RREQ is received by intermediate nodes that are in the transmission range of sender, those nodes broadcast RREQ until RREQ is received by destination or an intermediate node that has fresh enough route to the destination. Then it sends RREP unicastly toward the source. As a result, a route between source and destination is established. A fresh enough route is a valid route entry that its destination sequence number is at least as great as destination sequence number in RREQ. The source sequence number is used to determine freshness about route to the source consequently destination sequence number is used to determine freshness of a route to the destination. When intermediate nodes receive RREQ, with consideration of source sequence number and hop count, make or update a reverse route entry in its routing table for that source. Furthermore, when intermediate nodes receive RREP, with consideration of destination sequence number and hop count, make or update a forward route entry in its routing table for that destination.

Though reliable environments have been assumed in the majority of researches on ad-hoc routing protocols, unreliable situations are quite often. Therefore, most ad-hoc routing protocols are susceptible to miscellaneous types of attacks such as Spoofing attack, Denial of Service (DoS) attack, Routing Loop attack, Warm hole attack [6], Black hole attack etc. Common types of threats are possessed against Physical, MAC and Network layer, that are the fundamental layers requires for proper functioning of routing protocol. The threats try to accomplish two purposes: not forwarding the packets or add/alter some parameters (e.g. sequence number or hop count) to routing messages. In Black hole attack, a malicious node uses the routing protocol to advertise itself as having the shortest or freshest path to the node whose packets it wants to intercept. In a flooding based protocol, the attacker eavesdrops to requests for routes. When the attacker receives a request for a route to the target node, it creates a reply consisting of an exceptionally short or fresh route [7], therefore, misleading the source in transferring information to the path that leads to the black hole itself.

Intrusion detection is a challenging task in MANETs. Zhang and Lee [8] propose a circulated and cooperative intrusion detection model based on statistical incongruity detection techniques. Dang et. al. [9] introduces a method that requires each of the intermediate nodes to send back the next hop information inside RREP message. This method uses further request message and further reply message to confirm the authority of the route. In Robust Routing [10] by Lee, Han, Shin, the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route

reply and authentication message, the source verifies the legitimacy of path according to its policy. An approach based on dynamic training method in which the training data is updated at regular time intervals has been proposed Kurosawa et. al. in [11]. In [12], Huang et al use both specification-based and statistical-based approaches. They construct an Extended Finite State Automation (EFSA) according to the specification of AODV and model normal state and detect attacks with incongruity detection and specification-based detection.

With the view to secure routing in MANET several intelligible researches has been carried out. Hu, and Johnson proposed SEAD [14], a secure routing protocol based on DSDV that employs Hash chains to authenticate hop counts and sequence numbers. ARAN [15] harnesses cryptographic public-key certificates in order to accomplish the security target. A modified Ad-hoc routing protocol has been proposed by Ariadne [16] that provides security in MANET and depends on efficient symmetric cryptography. Secure AODV (SAODV) [17] is a security extension of AODV protocol, based on public key cryptography. Hash chains are used in this protocol to authenticate the hop count. Adaptive SAODV (A-SAODV) [18] has proposed a mechanism based on SAODV for improving the performance of SAODV. In [19] a bit of modification has been applied to A-SAODV for increasing its performance.

II. Black Holes: A Network Layer Attack in MANET

In black hole attack, the malicious node waits for the neighbors to initiate a RREQ. Obtaining the RREQ right away it sends a false RREP with a modified higher sequence number. As a result, the source node assumes that node (malicious) is having the fresh route towards the destination.

The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. In this way, the black hole swallows all objects and data packets [20].

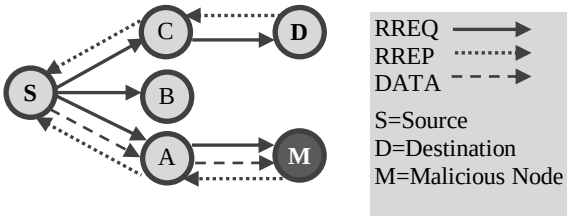

Figure 1. Black hole attack in a mobile ad-hoc network.

As demonstrated in figure 1, source node S requests to send data packets to destination D, Malicious Node M acts as a black hole replying with false reply RREP having higher modified sequence number. Accordingly, data communication initiates from S towards M instead of D.

Black hole attack in AODV protocol can be classified into two categories:

1) Black hole attack caused by RREQ

With sending fake RREQ messages an attacker can form black hole attack as follows:

a) Set the originator IP address in RREQ to the originating node's IP address.

b) Set the destination IP address in RREQ to the destination node's IP address.

c) Set the source IP address of IP header to its own IP address.

d) Set the destination IP address of IP header to broadcast address.

e) Choose high sequence number and low hop count and put them in related fields in RREQ.

So, false information about source node is inserted to the routing table of nodes that get sham RREQ. Hence, if these nodes want to send data to the source, at first step they send it to the malicious node.

2) Black hole attack caused by RREP

With sending fake RREP messages an attacker can form black hole attack. After receiving RREQ from source node, a malicious node can generate black hole attack by sending RREP as follow:

a) Set the originator IP address in RREP to the originating node's IP address.

b) Set the destination IP address in RREP to the destination node's IP address.

c) Set the source IP address of IP header to its own IP address.

d) Set the destination IP address of IP header to the IP address of node that RREQ has been received from it.

III. $AODV_R$: Approach against Black Hole Attacks

In AODV the node that receives the RREP, checks the value of sequence number in routing table and accepts if it has a higher RREP *seq_no* than the one in routing table.

```
IF (RREP seq_no > RT_seq_no) THEN
    RREP is ACCEPTED
ELSE
    RREP is DISCARDED
```

To solve this, we added an extra method to check whether the RREP seq_no is higher than the threshold value (A value that is updated dynamically in time intervals). As the value of RREP seq_no is found to be higher than the threshold value, the node is suspected to be malicious and added to the black list.

```
IF (RREP seq_no > THRESOLD) THEN
    Send ALARM to neighbors
ELSE
    RREP is ACCEPTED
```

The threshold value is dynamically updated using the data collected in the time interval. If the initial training data were used it is implausible for the routers to adapt changes in environment. The threshold value is the average of the difference of dest_seq_no in each time slot between the

sequence number in the routing table and the RREP. If a node receives a RREP for the first time, it updates value of the threshold.

If max chances of aberration (RREP seq_no>THRESOLD) is detected, it sends a new control packet ALARM to its neighbors. The ALARM packet contains the black list node as a parameter that tells the neighboring nodes to discard RREP from that malicious node. Further if any node receives the RREP, it looks over the list to check if the reply is from the blacklisted node and simply ignores the node throughout communication if identified as black hole. In this way, the malicious node is isolated from the network that results in less routing overhead under threats. Moreover the design not only detects the black hole attack, but also prevents it further by updating threshold which reflects the real environment.

A. *Route Analyzer*

Route analyzer a module in router assumed to store the past routing history, i.e. the list of destination sequence number, hop count in each time slot. We find the average of increments in destination_sequence_no for the available time slots/ history, i.e. if dest_seq_no is assumed as an array; we find the difference in every pair of successive terms and average that values. This leaves us with a value that further is used to as minimum of threshold range.

Another arithmetic mean is considered that is the average between RREP_seq_no and RT_seq_no in each time frame (i) for destination. It is added with the previous min_threshhold value to find the maximum of the range.

$$\sum(RREP\_seq\_no_i - RT\_seq\_no_i) / Total\ no.\ of\ frames$$

It would not be fair to list a node as black for single aberration in provided destination sequence number or hop count. Such an action may lead the network to bareness because the topology is dynamic in Ad-hoc Networks. Instead we count the number of anomalies detected for any node. In addition, if the total number of deception detected reaches the aberration tolerance value than it is identified as black hole and neighbors are ALARMed.

B. *AODV$_R$ Process Development*

The proposed architecture AODV$_R$ demonstrated in the Figure 2 formed of several modules that are Packet Classifier, Extractor, Blacklist Tester, RREP sequence number Tester, Threshold Tester and ALARM broadcaster. As the packet arrives in the system Packet Classifier classifies it to be RREQ, RREPsecure, RERR, ALARM and HELLO packet. AODV$_R$ assumes format of RREQ, RERR and HELLO Packets are as same as the AODV. However it modifies the content and format of RREP and includes a new type of packet ALARM.

Extractor extracts required contents of all types of packets other than HELLO. Three diamonds including threshold tester as depicted in the process flow of figure 2 check whether the packets are from a reliable source or not and discards the node or packet accordingly.

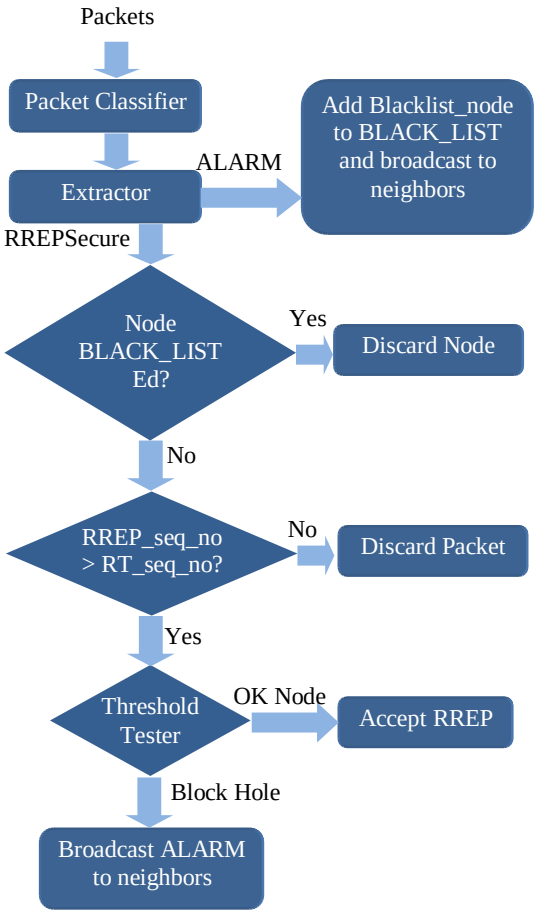

Figure 2. AODV$_R$ Process Development.

Every of the nodes are given MAX_ABBERATION_TO-LERANCE number of chances before they are attributed as BLACK_LISTed node; if an aberration is noticed than the node is check over and over before it emulates maximum chances. As a node is identified as black hole, ALARM Broadcaster broadcasts alert to neighboring nodes with the BLACK_LIST node as parameter. Any router receiving the ALARM packet forwards the message to its neighboring nodes thereby discovering the BLACK_LIST to the whole network.

C. *RREPsecure & ALARM*

```
Start
  Packet classifier←PACKET

  IF (PACKET=RREPsecure) THEN
     RREP_seq_no := Packet extractor←RREPsecure
  PACKET
     Blcklist←Check if the source_addr is in BLACK_LIST

     IF (Node is BLACK_LISTed) THEN
          Simply IGNORE the node.
     ELSE
          IF (RREP_seq_no > RT_seq_no) THEN
```

```
        IF (RREP_seq_no > THRESOLD_VALUE)
        THEN
          IF (NODE_CHANCES <
          MAX_ABBERATION_TOLERANCE)
          THEN
            NODE_CHANCES :=
            NODE_CHANCES+1;
            Recheck the authenticity of the node by
            RREQ.
          ELSE
            Broadcast ALARM to neighbors
        ELSE
            ACCEPT RREP and FORWARD
    ELSE
        DISCARD RREP

ELSE IF (PACKET=ALARM) THEN
    Blacklist_node := Packet extractor←ALARM packet
    Add Blacklist_node with BLACK_LIST
    Broadcast ALARM to neighbors
Stop.
```

IV. PERFORMANCE EVOLUTION

We implemented $AODV_R$ in OPNET [21] simulator and evaluated the performance based on three parameters that are Packet Delivery Ratio (PDR), Average End-to-End Delay (Avg E-E Delay) and Normalized Routing Overhead (NRO). PDR is the ratio of data delivered to the destination to data sent out by the source and Avg E-E Delay is the delay caused by the transmission.

We have considered various network contexts that were formed by varying Network Size, Traffic Load (total sources), and Mobility for the purpose of proper evolution.

A. Impact of Mobility

We evaluated the performance of AODV normal, AODV under attack and $AODV_R$ under attack in the context of variation in mobility that are listed in Table I (PDR) and Table II (Avg E-E Delay) and depicted consequently in Figure 3 and Figure4.

TABLE I. PDR (%) VS MOBILITY (m/s) FOR AODV & $AODV_R$

Method	Mobility(m/s)							
	10	20	30	40	50	60	70	80
AODV normal	100	98	92	86	85	84	86	89
AODV under attack	10	18	16	20	25	26	42	45
$AODV_R$ under attack	97	96	88	86	84	80	82	83

As illustrated in figure 3, AODV results in very low PDR under attack while $AODV_R$ exhibits almost same capability (3%-5% ranging from AODV) as normal AODV does. Later, Figure 4 testimonies $AODV_R$ to be delay efficient.

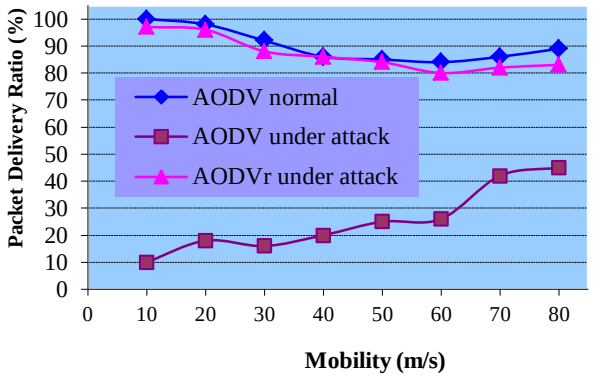

Figure 3. Graph of PDR (%) vs Mobility (m/s) for data in Table 1

TABLE II. AVERAGE END-TO-END DELAY VS MOBILITY (m/s)

Method	Mobility(m/s)							
	10	20	30	40	50	60	70	80
AODV normal	0.01	0.03	0.05	0.05	0.06	0.06	0.07	0.07
$AODV_R$ under attack	0.01	0.04	0.04	0.06	0.06	0.06	0.07	0.07

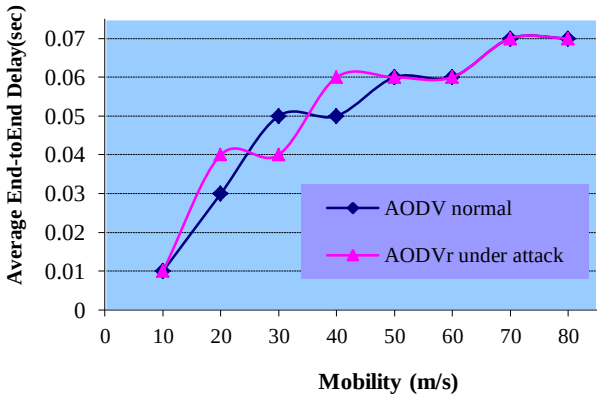

Figure 4. Graph of Average End-toEnd Delay vs Mobility (m/s)

B. Impact of Network Size

Performance of AODV normal, AODV under attack and $AODV_R$ under attack are evaluated in the circumstance of discrepancy in network size (no. of nodes) that are listed in Table III (PDR), Table IV (Avg E-E Delay), Table V (Normalized Routing Overhead) and delineated accordingly in Figure 5, Figure 6, and Figure 7.

TABLE III. PDR (%) VS NETWORK SIZE IN AODV & $AODV_R$

Method	Total nodes					
	10	20	30	40	50	60
AODV normal	100	99	96	97	98	99
AODV under attack	18	16	19	15	17	15
$AODV_R$ under attack	100	95	96	97	95	98

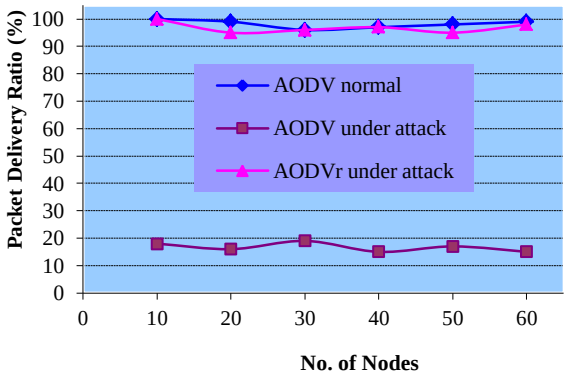

Figure 5. Graph of PDR (%) vs Network Size

TABLE IV. AVERAGE END-TO-END DELAY VS NETWORK SIZE

Method	Total no. of nodes					
	10	20	30	40	50	60
AODV Normal	0.017	0.046	0.048	0.05	0.052	0.052
$AODV_R$ under attack	0.018	0.043	0.046	0.048	0.051	0.052

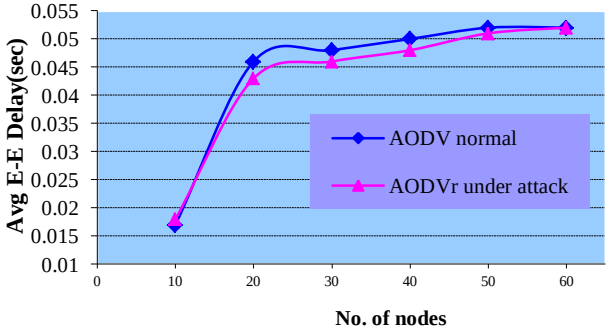

Figure 6. Graph of Average End-to-End Delay Vs Network Size

TABLE V. NORMALIZED ROUTING OVERHEAD (NRO) VS NETWORK SIZE

Method	Total no. of nodes					
	10	20	30	40	50	60
AODV normal	0.01	0.08	0.19	0.23	0.24	0.28
$AODV_R$ under attack	0.0	0.11	0.17	0.24	0.25	0.28

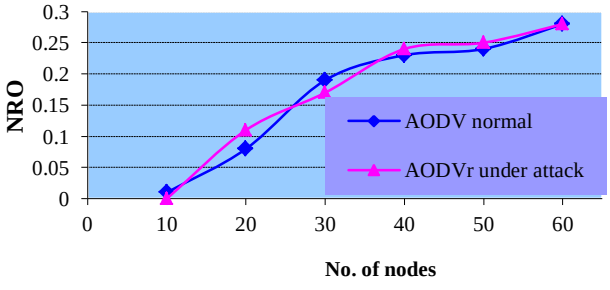

Figure 7. Graph of NRO Vs Network Size

In case of variation in Network size, as demonstrated in figure 5, AODV results in very low PDR under attack however $AODV_R$ exhibit s almost same performance as AODV does. Subsequently, Figure 6 manifests $AODV_R$ to be delay efficient however trivial falls that are negligible. Later Figure 7 testimonies a small increase in NRO that is insignificant.

C. Impact of Traffic Load

We simulated the performance of AODV, AODV under attack and $AODV_R$ under attack in the circumstance of discrepancy in Traffic Load (no. of sources) that are listed in Table VI (PDR), Table VII (Avg E-E Delay), Table VIII (NRO) and depicted accordingly in Figure 8, Figure 9, and Figure 10.

TABLE VI. PDR (%) VS TRAFFIC LOAD IN AODV & $AODV_R$

Method	No. of Sources					
	1	2	3	4	5	6
AODV normal	100	95	90	88	80	82
AODV under attack	10	35	30	30	30	31
$AODV_R$ under attack	100	92	90	80	80	81

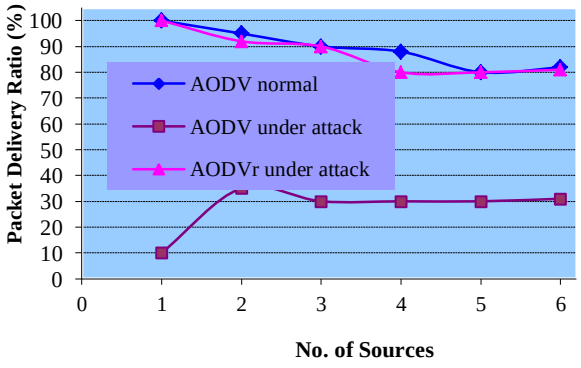

Figure 8. Graph of PDR(%) Vs Traffic Load

TABLE VII. AVG E-E DELAY VS TRAFFIC LOAD

Method	No. of Sources					
	1	2	3	4	5	6
AODV normal	0.04	0.08	0.12	0.14	0.22	0.25
$AODV_R$ under attack	0.05	0.08	0.12	0.13	0.20	0.23

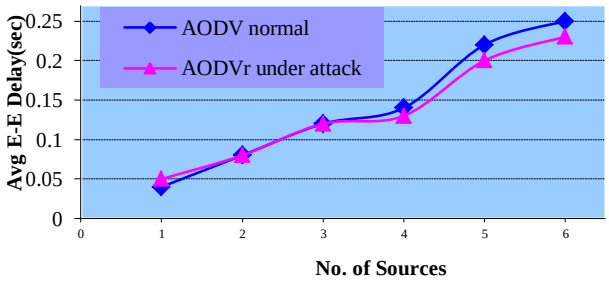

Figure 9. Graph of Average End-to-End Delay Vs Traffic Load

TABLE VIII. NRO VS TRAFFIC LOAD

Method	No. of Sources					
	1	2	3	4	5	6
AODV normal	0.08	0.14	0.20	0.20	0.22	0.24
$AODV_R$ under attack	0.08	0.16	0.21	0.22	0.23	0.25

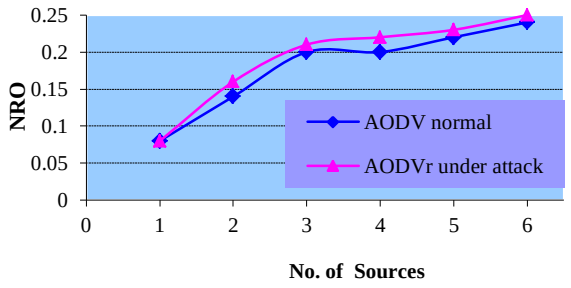

Figure 10. Graph of NRO Vs Traffic Load

In case of different Traffic Load, as depicted in figure 8, it is clear that as the traffic load increases the PDR of $AODV_R$ increases by 60% than AODV under attack that is very close to PDR of AODV normal. Afterward, Figure 9 shows $AODV_R$ to be delay efficient and sometimes better than AODV. Later on Figure 10 demonstrates a small NRO increment that can be ignored without hesitation.

V. CONCLUSION

Proposed $AODV_R$ exhibits appreciable performance dealing with networks with black holes; however the procedure of formulating the threshold is a bit overwhelming. Formulations of correct threshold range keep black holes from intrude; while a wrong formulation may restrict an authentic node thereby disgrace it to be a black hole.

Hence, this value has to be calculated and verified suitably.

REFERENCES

[1] C. E. Perkins, E. M. B. Royer and S. R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, Feb. 2003.

[2] E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Person. Commun., Vol. 6, no. 2, Apr. 1999.

[3] E. Çayırcı, C.Rong, "Security in Wireless Ad Hoc and Sensor Networks," vol. I. New York: Wiley 2009, pp. 10.

[4] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, pp 234–244, Aug.1994.

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

[6] Y. C. Hu, A. Perring, D. B. Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, Feb. 2006.

[7] M. Ilyas, "The Handbook of Ad hoc wireless Networks," CRC Press, 2003.

[8] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," 6th annual international Mobile computing and networking Conference Proceedings, 2000.

[9] 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

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

[11] S. Kurosawa, H. Nakayama, N. Kat, A. Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol.5, No.3, pp 338-346, Nov. 2007.

[12] 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.

[13] Tamilselvan, L.; and Sankaranarayanan, V. (2007). "Prevention of blackhole attack in MANET," The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[14] Y.-C. Hu, D. B. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, Jun. 2002, pp. 3-13.

[15] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[16] Y.-C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, Sep. 2002, pp. 12-23.

[17] M. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV)," Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[18] D. Cerri, A. Ghioni, "SecuringAODV: The A-SAODV Secure Routing Prototype," IEEE Communication Magazine, Feb. 2008, pp 120-125.

[19] K. Mishra, B. D. Sahoo, "A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet," International Journal Of Computer Applications In Engineering, Technology And Sciences (Ij-Ca-Ets), Apr. 2009 – Sep. 2009, pp 443-447.

[20] Chen Hongsong; Ji Zhenzhou; and Hu Mingzeng (2006). "A novel security agent scheme for AODV routing protocol based on thread state transition," Asian Journal of Information Technology, 5(1), 54-60.

[21] http://www.opnet.com

AUTHORS PROFILE

Mohammad Abu Obaida[1] obtained his Bachelor of Science in Engineering degree from Department of CSE, Dhaka University of Engineering & Technology (DUET), Gazipur-1700, Bangladesh. At present wide-ranging research on networks, cryptography and pattern recognition are carried out by him. His key research interests include Cryptography, Networks and Web Security, Wireless networks, Software Architecture, Machine Vision, Artificial Intelligence, Protocol analysis and design.