International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 6.525, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 2, Issue 1, 2017

IMPROVE THE PERFORMANCE OF AODV UNDER BLACKHOLE ATTACK IN MANET

G. Vennila* & D. Arivazhagan**
Department of Information Technology, AMET University, Chennai, Tamilnadu

Cite This Article: G. Vennila & D. Arivazhagan, "Improve the Performance of AODV under Blackhole Attack in Manet", International Journal of Engineering Research and Modern Education, Volume 2, Issue 1, Page Number 150-154, 2017.

Abstract:

The Mobile Ad-hoc Network is an infrastructure-less network in which each mobile node can communicate with other node without any fixed network. In view of this, the networks are vulnerable to various kind of attacks such as black hole attack, gray hole attack etc. The black hole attack is one of the cruel attacks in Mobile Ad-hoc NETwork (MANET). The simulation is carried out using MATLAB and analyzes the black hole attack in Ad-hoc On-demand Distance Vector (AODV) routing protocol and compared the performance of packet delivery ratio and delay with existing algorithm Hash_DSR. The result shows that the Hash_AODV is better than the Hash_DSR.

Key Words: AODV (Ad-Hoc On-Demand Distance Vector), MANET (Mobile Ad-hoc Network), Black Hole Attack, Delay, RREQ, RREP, Hash_DSR & Hash_AODV

Introduction:

Mobile Ad hoc Networks (MANET) is one of the vital areas in the field of research in wireless network at present. MANET is a collection of mobile devices that communicate with one another without any fixed network. The wireless Ad-hoc network allows the mobile node to join as well as to leave from the network at any point of time [1]. Each mobile device in Mobile Ad-hoc Network can perform as router and as a host to share the resources to other device willingly [3]. The AODV protocol is an on-demand routing protocol, which has two important phases: Route Discovery and Route Maintenance, which works mutually to permit the nodes to determine and maintain routes to destination. The black hole attack is a kind of network layer attack [2] in which any node itself promotes that has shortest path to reach destination and it consumes packets. The proposed secure hash algorithm is implemented under Ad-hoc On-Demand Distance Vector routing protocol (H_AODV) to analyze the performance metrics packet delivery ratio, delay and compared the performance with existing algorithm H_DSR.

Related Works:

Isaac Woungang et al [4] proposed a novel method DBA-DSR; it identifies and avoids black hole attack before the routing mechanism established to acquire the fake node details. Jaydip Sen et al. [5] proposed a technique to detect a black hole attack in AODV protocol. It detects the malicious activities that protect the mobile ad-hoc ad hoc network. Watchara Saetang et al. [6] proposed a solution called Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol to remove the black hole attack. Jaisankar N et al [7] proposed a technique called Next hop information scheme to eliminate the single black hole attack in Mobile ad-hoc network under Ad-hoc on-demand distance vector routing protocol. In this scheme, The PDR is enhanced by 40- 50% and packets dropped is decreased by 75- 80%. Isaac Woungang et al [8] proposed a solution to detect black hole attack under DSR protocol in mobile ad-hoc network & improve the performance metrics such as PDR and routing overhead. K. Rama Abirami et al [9] proposed a protocol called Efficient Secure Enhanced Routing Protocol (ESERP) to detect the co-operative black hole node in Mobile Ad-hoc Network

Kanika Bawa and Shashi B. Rana et al [10] proposed Genetic Algorithm & Bacterial Foraging Optimization to prevent the black hole attack to improve the performance of Mobile ad-hoc network. Ali Dorri et al [11] proposed Extended Data Routing Information table (EDRI) to detect and eliminate black hole attack. It improves the performance of Mobile ad-hoc network with the presence of co-operative black hole nodes. Vimal Kumar et al [12] proposed an approach called Adaptive Approach for Detection of Black hole Attack in Mobile Ad hoc Network. The Packet delivery Ratio increased by 96.3 % with the presence of black hole nodes. The throughput increased by 336.14 kbps with the presence of black hole nodes. Vennila et al [13] Proposed Hash based Technique to Identify the Selfish Node in Mobile Ad-hoc Network. The packet delivery ratio increased up to 70% and time delay reduced up to 80% compared to the standard Dynamic Source Routing (DSR) protocol.

AODV Protocol & Effects of Black Hole Attack:

The Ad-hoc On-demand Distance Vector Routing Protocol is an on-demand routing protocol in Mobile Ad-hoc Network. It establishes route whenever the user wants to communicate from source to destination. It has two phases Route Discovery, Route Maintenance.

Route Discovery:

The route discovery initiates the process to discover the path from source to destination. The Source Node (SN) wants to communicate with Destination Node (DN). First, it initiates the route discovery process by

sending the RREQ message to its neighbor node (X). The node X checks its routing table whether it has a path or not. If the node X has a path, it sends Route Reply message that has route information in reverse order. Otherwise, it forwards the same RREQ to its neighbor node until it reaches the destination. The neighbor node Y doesn't have path and it is not destination, it rebroadcast the RREQ to its neighbor node (DN). If the node is Destination Node (DN), it sends RREP to its next node(Y). The node Y accepts the RREP, hence it is not source. It forwards the RREP to its next node X. If the node X is not a source, it also forwards the RREP to its next node (SN). The Source Node (SN) receives RREP message that consists of route information in reverse order (DN-Y-X-SN). Therefore, the Source Node (SN) starts to communicate with Destination Node (DN). The Route Discovery Process is shown in Fig.1.

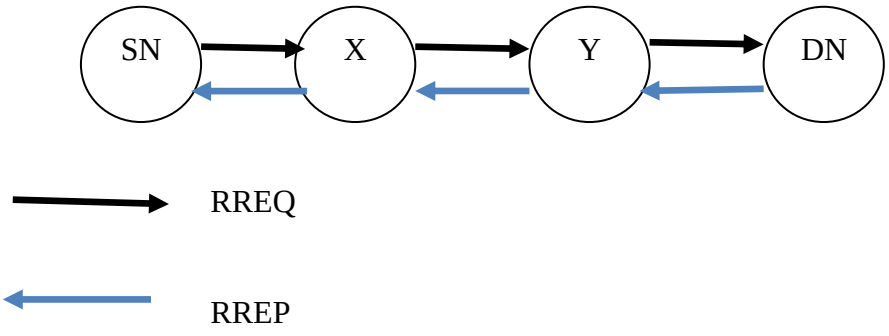

Figure 1: Route Discovery

Route Maintenance:

The Route Maintenance is a phase to maintain the path from source to destination. If the link failure occurs between the sender and receiver, it sends Route Error (RERR) message. The source node validates the successful transmission from source to destination, by sending the message Acknowledgement (ACK) [14].

Effects of Black Hole Attack:

The black hole attack is an attack in which the mobile node that endorses itself has a path to reach destination. Consequently, it consumes the packet from source. There are two types of black hole attack:

Single Black Hole Attack:

Only one node can act as a malicious node in network and it drops the packet from Source node is known as single black hole attack. The Source Node (SN) wants to communicate with Destination Node (DN). Therefore, it sends RREQ to all the nodes present in the network including M (Malicious Node). The Destination Node and Malicious Node (M) send RREP that contain path information to Source Node. The Source Node sends packet whose RREP contains highest sequence number. The Malicious node sets highest sequence number than the other node present in the network. Consequently, the malicious node consumes the packet from Source and not forward to any other node. This mechanism is shown in Fig.2.

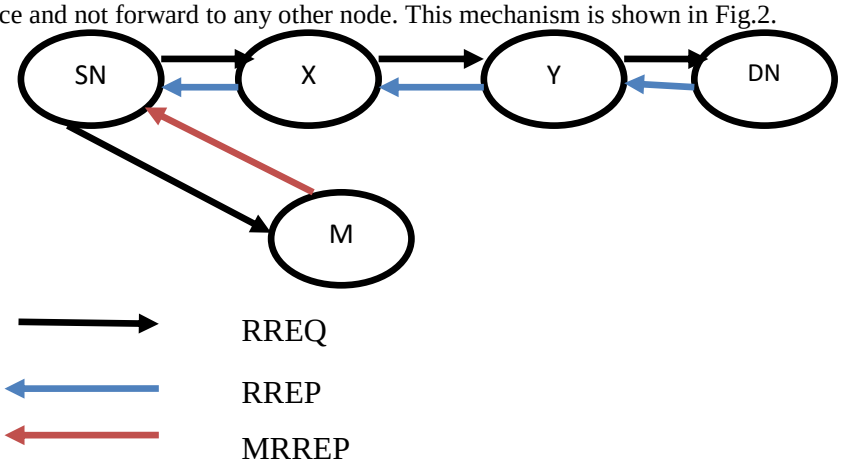

Figure 2: Single black hole attack

Co-Operative Black Hole Attack:

More than one node can act as a malicious node in network and it drops the packet from Source node is known as co-operative black hole attack. The Source Node sends RREQ to node X, Y, DN and also M1, M2 are malicious nodes. The Source Node sends packet to node whose RREP has highest sequence number. The M1 and M2 has highest sequence number than the node X, Y, DN. Therefore, the Source node sends packet to malicious node-1(M1) and drops the packets. This is shown in Fig.3.

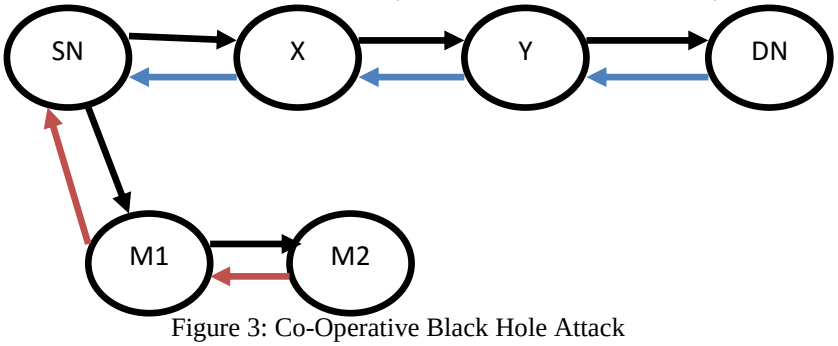

Figure 3: Co-Operative Black Hole Attack

Proposed Work:

The proposed algorithm use one cryptographic technique called secure hash algorithm to improve the performance of Ad-hoc On-demand Distance Vector Routing protocol (AODV). The secure hash algorithm is a cryptographic hash function used to authenticate the message and validate the message coming from legitimate node. Therefore, the algorithm used secure hash value generated by secure hash function and secret key encryption used in AODV protocol. The algorithm consists of four stages as follows:

RREQ Generation at Source:

Step 1:

Initialize the Number of Nodes
SN – Sender Node
DN – Destination Node
MN – Malicious Node
SHC – Sender Hash Code
DHC- Destination Hash code
MNI- Malicious Node identifier

Step 2:

Source Node sends RREQ to its neighbor node

Step 3:

If (Node = = Destination)
Sends RREP to Source Node
Then
Source Node sends packet to Destination Node
Else if (node! = Destination)
Checks its Route catch that has a route to Destination Node
Then
It sends RREP to Source Node
The Source Node sends packet to destination
Else
It sends RREQ to its neighbor node until reach Destination Node

RREP Generation at Destination:

Step 1:

The Destination Node receives RREQ from source

Step 2:

It generates hash code by using the secret key shared between the sender and receiver.

Step 3:

Then assign the generated hash code to DHC and it appends the hash code in RREP

Step 4:

The Destination Node sends RREP to Source Node

MNI and Packet Transmission:

Step 1:

The source node receives RREP from Destination
Then it generates the hash code and assigns it to SHC

Step 2:

If (DHC==SHC)
The node is genuine node
It sends Packet from SN to DN
Else
The node is malicious node
Source node sends MNN message to every nodes present in the network

Performance Analysis:

The proposed algorithm is implemented under AODV Protocol called as Hash based AODV. The hash based AODV shows better performance than the hash based DSR. The simulation was done in MATLAB to estimate the performance of AODV in terms of Packet delivery ratio and delay.

Packet Delivery Ratio (PDR):

The proportion of numbers of packets sent by the source and numbers of packets received in destination. The performance of Packet delivery ratio compared with existing Hash_DSR shown in Fig 4. The packet delivery ratio decreases when the number of nodes increases in the network. The proposed hash based AODV conserves high packet delivery than hash based DSR.

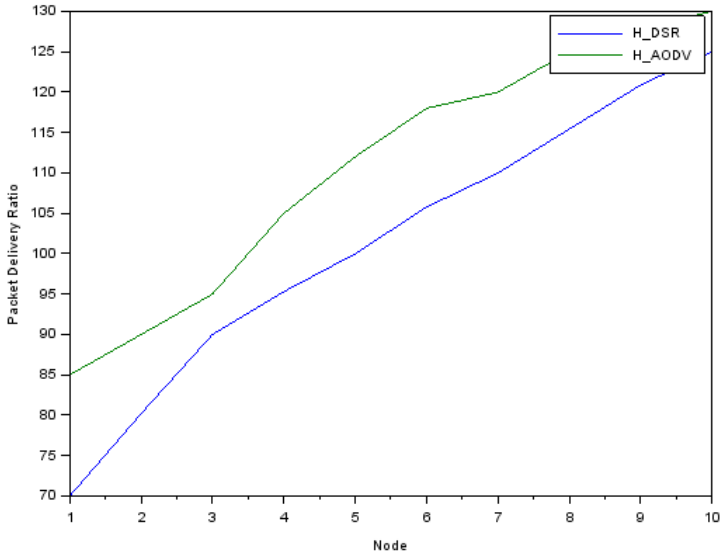

Figure 4: Packet Delivery Ratio (PDR)

Delay:

The time taken to transfer the packets from source to destination is called as delay. The performance of Delay compared with existing Hash_DSR shown in Fig 5. The proposed hash-based AODV relatively reduces the delay compared with the hash based DSR.

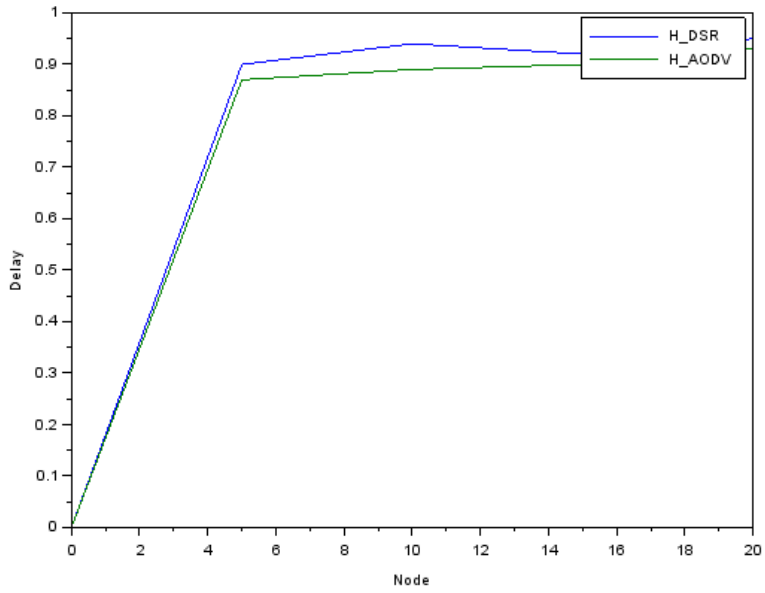

Figure 5: Delay

Conclusion:

This paper use secure hash algorithm to generate the hash code before obtaining the path details for data transmission and it is appended in RREP implemented in AODV protocol using MATLAB. The challenges exist in black hole is to find multiple malicious nodes effectively during communication in Mobile Ad-Hoc Network. The hash based AODV algorithm used to identify the black hole nodes efficiently between source and

destination during route establishment process. In future, this secure hash algorithm may apply to other types of attacks such as worm hole attack, grey hole attack etc to analyze the performance of routing protocols.

References:

1. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010.
2. G. Vennila, D. Arivazhagan, N. Manickasankari, "Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm", International Journal of Engineering and Technology (IJET), Vol 6 No 5 Oct-Nov 2014
3. G. Vennila, D. Arivazhagan, N. Manickasankari, "A Survey of Sinkhole Attack on DSR in MANET", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 5, pg.239 – 244, May 2014.
4. Isaac Woungang," Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks", IEEE, 2012
5. Watchara Saetang, Sakuna Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks", In: International Conference on Computer Networks and Communication Systems (CNCS 2012), 2012.
6. Jaydip Sen, Sripad Koilakonda, Arijit Ukil," A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks" , In: Proceedings of IEEE International Conference on Intelligent Systems, Modelling and Simulation, 2011.
7. Jaisankar N, Saravanan R, Swamy KD ," A Novel Security Approach for Detecting Black Hole Attack in MANET" ,International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, March 2010.
8. Woungang, S.K. Dhurandher, Mohammad S. Obaidat (GE) and R.D. Peddi," A DSR-based routing protocol for mitigating black hole attacks on mobile ad hoc networks," Security and Communication Networks,2013.
9. K. Rama Abirami , M.G. Sumithra, J. Rajasekaran, "An Efficient Secure Enhanced Routing Protocol for DDoS Attacks in MANET," International Review on Computers and Software (IRECOS), January 2014.
10. Kanika Bawa and Shashi B. Rana "Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization", IJCET,vol.5, no.4, 2015.
11. Ali Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET "‖,Wireless Network, DOI 10.1007/s11276-016-1251-x.
12. Vimal Kumar , Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network ",International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) 1877-0509 , 2015, Elsevier B.V.
13. G. Vennila, D. Arivazhagan, "Hash based Technique to identify the Selfish Node in Mobile Ad-hoc Network", Indian Journal of Science and Technology, Vol 8(14), 70696, July 2015
14. Bai R, Singhal M. DOA: DSR over AODV Routing for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing. 2006 Oct; 5(10).