A Combined Efficient Approach to Handle Black Hole Attack for AODV in MANET

Mr. Hardik Talsania[1] Prof. Zishan Noorani[2]
[1]Lecturer [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]R.C.T.I, Ahmedabad, Gujarat, India

Abstract*—*Providing proper security for MANETs with devices that can configure themselves without a strict intervention by network administrators is a challenging task. Due to its dynamic network topology and decentralized administration, MANETs are more susceptible to various attacks like Black Hole and Gray Hole where a malicious node drops the packets it receives on purpose. This paper focuses on proposing a combined technique for Fake RREQ and Permutation-based Acknowledgement to handle Black Hole attack for AODV protocol in MANET. The proposed combined method works in a secure multipath AODV network environment. It will enhance the efficiency & performance of the network in terms of Packet Delivery Ratio, Throughput and Routing Load as compared to the individual techniques.

Keywords—AODV, MANET, Black Hole Attack, SAODV, AOMSR, PBA, Packet Delivery Ratio, Throughput, End-to-end Delay

I. INTRODUCTION

There are 2 kinds of wireless networks: infrastructure-based & infrastructure-less. One of the examples of infrastructure-less network is MANET (Mobile Ad-hoc Networking) [9]. MANET's routing protocol locates routes between nodes and allows forwarding of data packets via the nodes of other network to destination [4]. Various challenges in routing of Mobile Ad-hoc Networks are found, some of them being dynamic topology, interference and lack of security mechanisms.

Two types of Ad-hoc routings algorithm are available: proactive and reactive routing algorithms. While, DSDV is a proactive routing algorithm, AODV & DSR are the examples of reactive routing protocols. AODV (Ad-hoc On-demand Distance Vector) is an on demand routing protocol, which establishes the path when it is needed [1].

A. Types of MANET Protocols

The mobile ad hoc network (MANET) has three kinds of protocols: Proactive, Reactive and Hybrid protocols [16].

1) Proactive Protocol:

Proactive protocols are also known as table-driven protocols in which the nodes sustain and update the routing tables regularly even when there is no communication.

Examples: DSDV (Destination-Sequenced Distance Vector), OLSR (Optimized Link State Routing).

2) Reactive Protocol:

Reactive protocols or also called On-Demand Protocols are the ones in which the routes are discovered on the demand basis of the source node.

Examples: AODV (Ad-hoc On-demand Distance Vector), DSR (Dynamic Source Routing).

3) Hybrid Protocol:

Hybrid protocols have the combined characteristics of both the reactive and proactive protocols.

Example: ZRP (Zone Routing Protocol).

II. AODV ROUTING PROTOCOL

As stated above, AODV is a reactive routing protocol that establishes a route on demand. In AODV, when a source wants to communicate with a destination, the source node broadcasts a RREQ (route request) message. When any intermediate node or destination node has a route to the destination node, it sends back RREP (route reply) message to the source node. If there is breakage in the link between two nodes in this route, a RERR (route error) is sent, informing the source about the lost link [14]. The routing discovery in AODV is shown in Fig. 1 below.

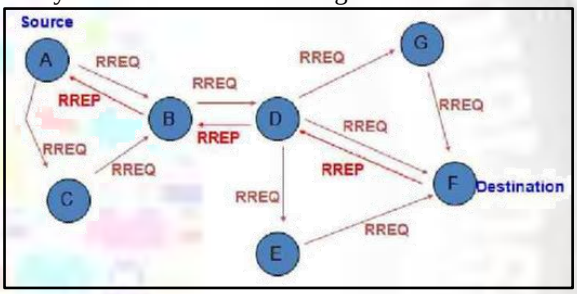

Fig. 1: Routing Discovery in AODV

Sequence number plays a key role in AODV protocol. If source node receives a reply packet (RREP) that has highest sequence number with small hop count, it updates its routing information and starts using better route. AODV is a routing protocol, hence that deals with routing table management. Routing table entry includes following fields: Destination IP Address, Destination sequence number, Next hop IP address, Life time, Hop count [15]. When a source node receives multiple RREPs, it will select the RREP with the highest destination sequence number (DSN). If DSNs are identical, then it will select the RREP with the lowest hop count.

III. BLACK HOLE ATTACK IN AODV

Black hole attack is a well-known attack in wireless ad hoc networks that can occur especially in case of on-demand routing protocols such as AODV. It is an attack in which a malicious node acquires route from a source node to a destination node by falsification of sequence number or hop count or both. A black hole node builds a route reply with fake larger sequence number and shorter hop count (usually 1) of a routing message in order to forcefully acquire the route and then listen or drop all data packets that pass through that route [11]. Demonstration of black hole attack in an AODV network can be seen in the Fig. 2 below.

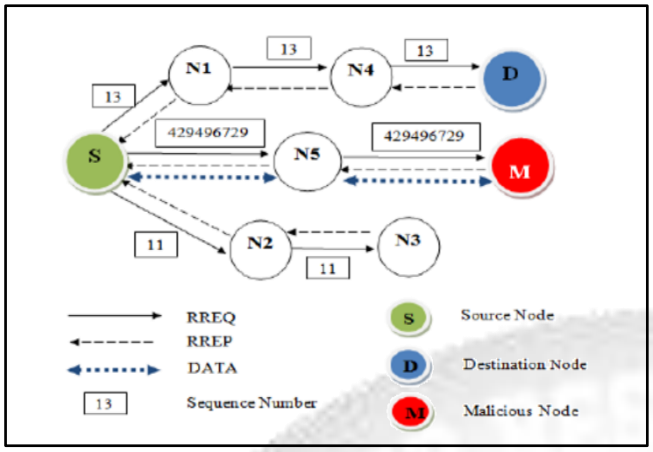

Fig. 2: Black Hole Attack Demonstration

As shown in the Fig. 2 above, Node M is a malicious node on the network. When it receives the RREQ message, it replies immediately to the source node (Node S) with its RREP message without following the routing protocol. The black hole's RREP message includes S_Addr and D_Addr values that are copied from the RREQ message, the lowest Hop_Count (shortest path), and the highest DSN value [17].

IV. Literature Review

As a part of literature review, existing research and survey papers were studied related to research area. Researchers have proposed several mechanisms to minimize the effect of black hole attack in the past 5-7 years span. However, no method guarantees transmission of all the packets without loss after the mitigation of the black hole attack and there is always a scope of improvement in the existing technology.

Balachandra et al. [] proposed SAODV (Secure Ad-hoc On-demand Distance Vector) routing protocol which makes digital signatures and hash chains to authenticate the non-mutable fields and hop counts respectively in the RREQ and RREP packets. They also proposed 'Watchdog Mechanism' as an intrusion detection technique.

Neha Sharma et al. [3] proposed a system to work in 2 phases: Route Discovery Phase and Monitoring Phase, wherein the route discovery phase makes use of 'Fake RREQ' sent by a source node to trap a malicious node for a fake reply in return while the monitoring phase works in the promiscuous mode to monitor the neighboring node's activity for assured packet transmission.

A. K. Jain et al. [] presented a system based on first RREP (Route Reply) caching mechanism, which is used to count the number of RREP packets received by the source node. The Proposed system – SAODV (Secure AODV) – ignores the first RREP packet that reaches the source node.

Dhaval Dave and Pranav Dave [6] proposed a technique named AOMSR (Ad-hoc On-demand Multipath Secure Routing) which is the enhancement of 'Adaptive Acknowledgement (AACK)' and 'TWO-ACK' techniques which makes use of multiple paths to transfer data packets and receive their acknowledgements from the destination on other paths – decided through permutations.

S. Banerjee et al. [] proposed a method that works in 2 phases: Black hole node identification and Black hole node removal, wherein the identification phase sends an extra RREQ packet after the initial one with a higher sequence number than the previously received to identify the malicious node in the network, while the removal phase stores the IP address of the black hole node identified in the previous phase in a malicious node table.

Sathish M et al. [] presented a method that makes use of 'Fake RREQ' technique and maintains Black Hole List and Collaborative Black Hole List. It makes use of average of DSNs (Destination Sequence Numbers) of all malicious RREPs in case of collaborative black hole attack and use of digital signatures and trust value to prevent black hole attack in the network.

We concluded from the review of different papers that we can improve the performance of the network in terms of PDR, throughput and routing load by proposing a method that combines the techniques of two of the earlier researches.

V. Proposed Work

Out of the many techniques proposed by different researchers in their proposals, we have identified two of them as our base papers. Hence, for us, those are the existing systems, for which we want to improve the performance by combining them and proposing a new technique.

First of the existing system is the one mentioned in the paper [3] by N. Sharma et al. in which they used the 'Fake RREQ' technique to detect black hole nodes in a network and promiscuous mode to prevent the future occurrences of such malicious nodes in the network. Second of the existing system is mentioned in the paper [6] by D. Dave et al. in which they used the 'Permutation-based Acknowledgement' technique to detect black hole nodes and created an AOMSR (Ad-hoc On-demand Multi-path Secure Routing) environment for it. We propose a system by combining both these techniques to increase the efficiency of the network in terms of both PDR, throughput and routing overhead.

The model of the proposed system is given in Fig. 3 below:

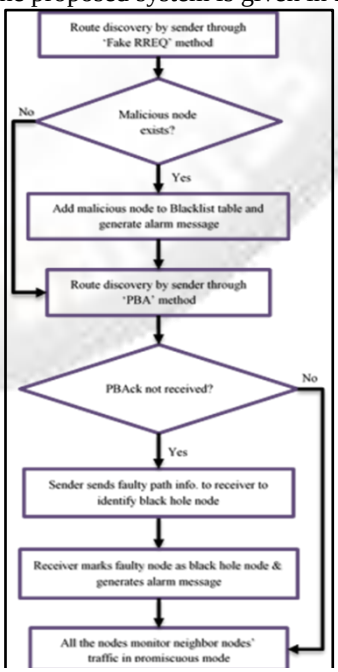

Fig. 3:Model for Proposed System

A. Steps performed in this system

- Sender: Performs route discovery through 'Fake RREQ' technique mentioned in [3].
- Sender (if malicious node exists): Adds the malicious node to the BlackList table and generates an alarm message.
- Sender: Performs route discovery and sends data packets through 'PBAck' method mentioned in [6].
- Sender (if does not receives all PBAck in time): Sends faulty path info. to the receiver to identify black hole node.
- Receiver (on receiving faulty path info.): Identifies the black hole node and generates the alarm message.
- All nodes: Monitor the traffic of the neighboring nodes in promiscuous mode.

VI. SIMULATION

Initially, we implemented a wireless network in NS-2 by taking 25 sample nodes with one being the sender, one being the receiver, one of them as a malicious node and setting up remaining simulation parameters as listed in [6]. Gradually we raised the number of senders, receivers and malicious nodes from 1 to 4. We show here the simulation of the proposed system with 4 malicious nodes in Fig. 4 below.

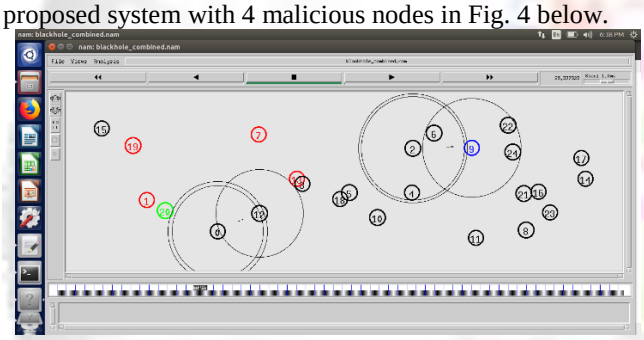

Fig. 4:Simulation of Proposed Technique with 4 Black-Hole Nodes

The results of the simulations are recorded in terms of 3 analysis parameters: packet delivery ratio, throughput and routing load for both existing systems and our proposed system. Again, results of the proposed combined technique can be seen with 4 malicious nodes in the Fig. 5 below.

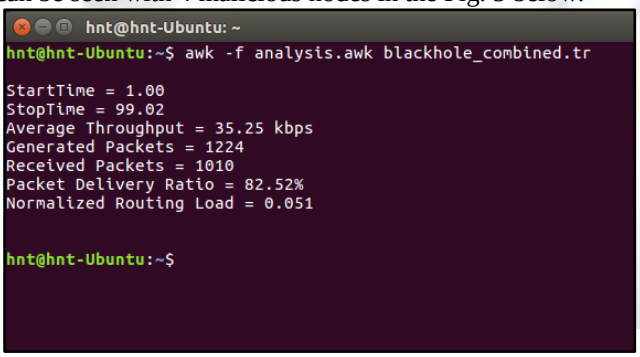

Fig. 5:Results of Proposed System with 4 Black-hole nodes

VII. ANALYTICAL RESULTS

First, the results of all the systems is compared for packet delivery ratio and shown in Table 1 below and the graph for the same is shown in Fig. 4 after that.

Next, we show the results of all the systems in terms of throughput as in Table 2 and the graphical comparison is shown in Fig. 5 below that.

Also, the result comparison is done in tabular and graphical format for routing load which can be seen in Table 3 and Fig. 6 further.

Network Scenarios	No. of Black Hole Nodes			
	1	2	3	4
Black Hole Attack	39.23 %	23.14 %	20.64 %	15.43 %
Existing System 1	55.42 %	44.71 %	45.56 %	48.29 %
Existing System 2	63.21 %	60.11 %	54.19 %	58.63 %
Proposed System	83.86 %	81.74 %	78.45 %	82.52 %

Table 1: Performance of Systems for PDR

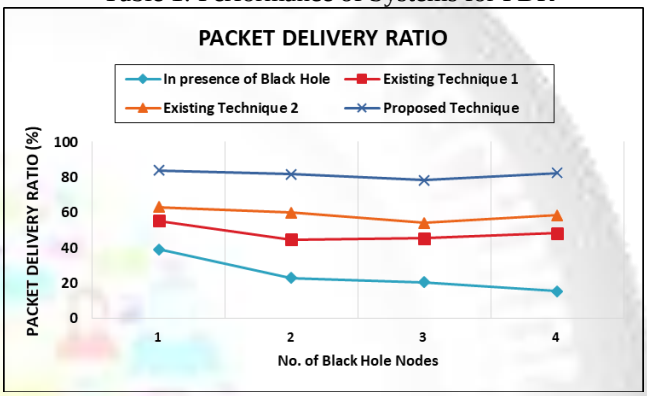

Fig. 6: Graph showing Performance of Systems for PDR

Network Scenarios	No. of Black Hole Nodes			
	1	2	3	4
Black Hole Attack	20.1	19.48	18.12	15.43
Existing System 1	28.32	25.71	23.88	26.68
Existing System 2	31.41	27.19	21.46	25.37
Proposed System	38.67	33.74	30.45	35.25

Table 2: Performance of Systems for Throughput (KBPS)

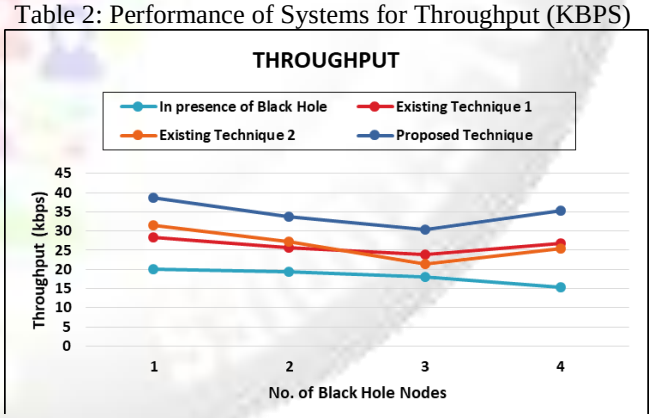

Fig. 7: Graph showing Performance of Systems for Throughput

Network Scenarios	No. of Black Hole Nodes			
	1	2	3	4
Black Hole Attack	0.116	0.125	0.134	0.123
Existing System 1	0.087	0.093	0.097	0.095
Existing System 2	0.062	0.071	0.088	0.075
Proposed System	0.044	0.056	0.063	0.051

Table 3: Performance of Systems for Routing Load

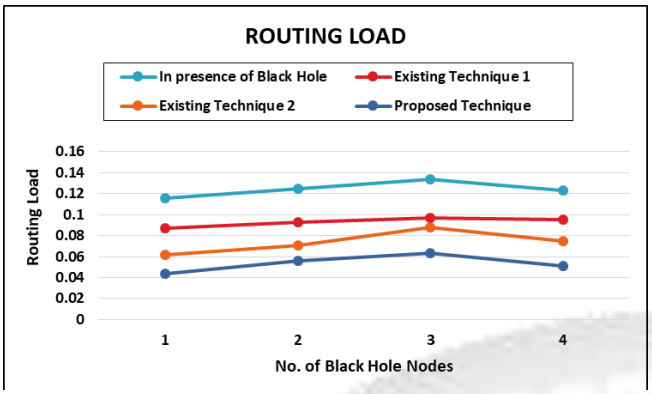

Fig. 8: Graph showing Performance of Systems for Routing Load

VIII. FUTURE WORK

As there can be always a scope of the enhancements, the research work presented in this thesis also can be improved and enhanced. We can implement our proposed system in the advanced version of the network simulator (like NS-3 or later) in the future. We can also implement our system in real-life scenarios with possible and required changes in simulation parameters if possible instead of using simulation software to produce results and compare performance.

We have compared the results of simulation of different scenarios and produced graphs in MS Excel. However, we can produce the graphs in XGraph software in future. Moreover, we can compare the results of the systems in terms of other analysis parameters like End-to-end Delay, Packet Drop, etc.

IX. CONCLUSIONS

The objectives of the research work have been potentially accomplished with the development of a model that improves the performance of the affected network as compared to the existing systems. The developed model has been implemented in NS-2, which has attained satisfactory overall improvement as compared to other systems in terms of three analysis parameters with average packet delivery ratio being 81.64%, average throughput being 34.53 kbps and average routing load being 0.05.

Hence, all the results obtained are comparatively better than the existing systems. However, the developed model endures certain limitations which could be eliminated by several enhancements as discussed in the previous section.

REFERENCES

[1] R. Kumar, A. Quyoom and Devki Nandan Gouttam, "To mitigate black hole attack in AODV," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 307-311.

[2] Sathish M, Arumugam K, S. N. Pari and Harikrishnan V S, "Detection of single and collaborative black hole attack in MANET," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 2040-2044.

[3] N. Sharma and A. S. Bisen, "Detection as well as removal of black hole and gray hole attack in MANET," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 3736-3739.

[4] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using trust with AODV in MANET," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 470-474.

[5] Balachandra and N. P. Shetty, "Interception of black-hole attacks in mobile AD-HOC networks," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-5.

[6] D. Dave and P. Dave, "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET," 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, 2014, pp. 1690-1696.

[7] S. Dhama, S. Sharma and M. Saini, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2993-2996.

[8] Gupta, "Mitigation algorithm against black hole attack using Real Time Monitoring for AODV routing protocol in MANET," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 134-138.

[9] K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-6.

[10] Jain, U. Prajapati and P. Chouhan, "Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-4.

[11] Imran M., Khan F.A., Abbas H., Iftikhar M. (2015) "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks". In: Garcia Pineda M., Lloret J., Papavassiliou S., Ruehrup S., Westphall C. (eds) Ad-hoc Networks and Wireless. ADHOC-NOW 2014. Lecture Notes in Computer Science, vol 8629. Springer, Berlin, Heidelberg.

[12] Banerjee S., Sardar M., Majumder K. (2014) "AODV Based Black-Hole Attack Mitigation in MANET". In: Satapathy S., Udgata S., Biswal B. (eds) Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. Advances in Intelligent Systems and Computing, vol 247. Springer, Cham.

[13] Jaisankar N., Saravanan R., Swamy K.D. (2010) "A Novel Security Approach for Detecting Black Hole Attack in MANET". In: Das V.V. et al. (eds) Information Processing and Management. Communications in Computer and Information Science, vol 70. Springer, Berlin, Heidelberg.

[14] N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection

mechanism," 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, 2015, pp. 1-4.

[15] K. Madhuri, N. K. Viswanath and P. U. Gayatri, "Performance evaluation of AODV under Black hole attack in MANET using NS2," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-3.

[16] H. P. Singh and R. Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol," 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2014, pp. 1-8.

[17] S. Tan and K. Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-Based MANETs," 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, 2013, pp. 1159-1164.

[18] Lo NW., Liu FL. (2013) A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET. In: Juang J., Huang YC. (eds) Intelligent Technologies and Engineering Systems. Lecture Notes in Electrical Engineering, vol 234. Springer, New York, NY.

[19] http://www.tutorialsweb.com/ns2/NS2-1.htm

[20] Ei Ei Khin and Thandar Phyu, "Enhancing AODV Routing Protocol to Eliminate Black Hole Attack in MANET," 2015 International Journal of Computer Science and Business Informatics, 2015, Vol. 15, No. 2.

[21] https://www.ietf.org/rfc/rfc3561.txt