

II. Literature Review

Stephen Dabideen *et al.* [2] performed a work, "An End-to-End Solution for Secure and Survivable Routing in MANETs". Authors present a new approach to secure routing in MANETs and argue that the same approach can lead to more reliable routing in the face of node and link failure. Prior solutions to security in networks are inapplicable to routing in MANETs because of node mobility and the relative scarcity of bandwidth. Furthermore, path discovery does not necessarily translate into data delivery. Authors apply this approach to the design of the Secure Routing through Diversity and Verification (SRDV) protocol, a secure routing protocol that Authors show to be as efficient as unsecured on-demand or proactive routing approaches in the absence of attacks and capable of defending against a variety of attacks.

Xu Xiang *et al.* [3] performed a work, "Providing Efficient Secure DHTs Routing". Authors propose a secure protocol which consists of two phases: detecting malicious nodes and bypassing them. Author present a novel efficient routing strategy called tracer routing to control routing progress, accompanied by a node-ID based signature scheme. Combine these two; the source of every query can verify each step and malicious nodes can be identified. Authors also present a scheme to create a secure path to bypass malicious nodes.

Yanzhi Ren *et al.* [4] performed a work, "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording". In this paper, Authors propose a method to secure the history records of packet delivery information at each contact so that other nodes can detect insider attacks by analyzing these packet delivery records. Author evaluated Presented approach through extensive simulations using both Random Way Point and Zebranet mobility models. Presented results show that Presented method can detect insider attacks efficiently with high detection rate and low false positive rate.

Lanjun Dang *et al.* [5] performed a work, "DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks". In this paper, Authors present a new distributed anonymous secure routing protocol with good scalability for mobile ad hoc networks. The proposed protocol addresses the problems of anonymous routing and later anonymous data transmission via a dynamic identity pseudonymity approach based on Incomparable Public Keys. Good scalability is achieved by using Diffie-Hellman key exchange scheme and symmetric key cryptography, instead of public key cryptography.

Saurabh Gupta *et al.* [6] performed a work, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network". In this paper, Authors propose a protocol for avoiding blackhole attack without the constraint of special hardware and dependency on physical medium of wireless network. BAAP forms link disjoint multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network.

Isaac Woungang *et al.* [7] performed a work, "Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks". In this paper, a novel scheme for Detecting Blackhole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects and avoids the blackhole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes.

Rutvij H. Jhaveri *et al.* [8] performed a work, "A Novel Approach for Gray Hole and Blackhole Attacks in Mobile Ad-hoc Networks". In this paper, Author propose a scheme for Ad-hoc On-demand Distance Vector (AODV) protocol, in which an intermediate node detects the malicious node sending false routing information; routing packets are used not only to pass routing information, but also to pass information about malicious nodes. The proposed scheme not only detects but also removes malicious node by isolating it, to make safe and secure communication.

Rajesh Yerneni *et al.* [9] performed a work, "Enhancing performance of AODV against Black hole Attack". In this paper, a method is proposed called Secure-Ad hoc on demand Distance Vector (SAODV) algorithm that mitigates black hole attack by analyzing destination sequence number and validating the destination by random value. Simulation results show that the proposed protocol provides better security by increasing the packet delivery ratio when compared to AODV in presence of black hole attacks.

III. Proposed Black hole Detection Algorithm

This algorithm is designed to identify and isolate the black hole nodes in the MANET. This algorithm removes the disadvantages of the DBA-DSR algorithm [1] which is the extended version of the DSR protocol. In DBA-DSR algorithm, the source node identifies the black hole nodes in the MANET with the help of fake RREQ and fake RREP. The drawbacks of DBA-DSR are: firstly, resending of ack packets from the source node to the destination to check that if intermediate node is fake or not and waiting for reply of ack packets means increasing in routing overhead packets between the source and destination. Secondly, if the distance between the source node and the intermediate node is long, the delay in the discovery period of the route is high, which causes an overall network performance degradation.

In order to mitigate the drawbacks of DBA-DSR algorithm, we proposed a new algorithm which detects the black hole nodes locally; which means that when the intermediate node unicasts the RREP towards source node, then the previous node of the intermediate node performs the process of detection. In the proposed algorithm, all nodes work in promiscuous mode.

The Algorithm is shown in figure 2.

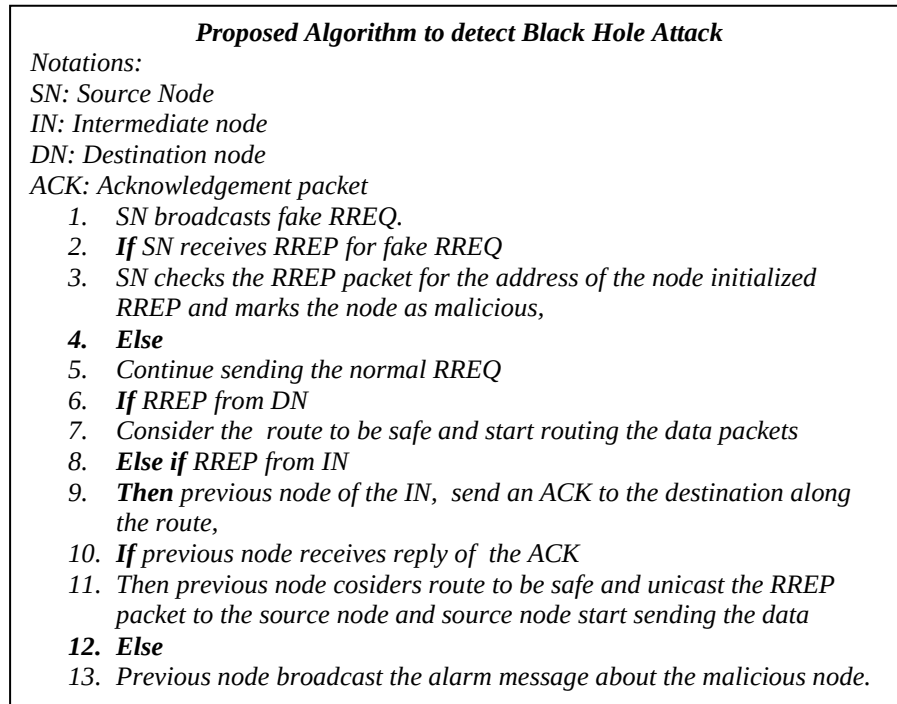


Fig. 2 Proposed Algorithm

Before starting the normal DSR routing, the source node initializes the fake RREQ packet with a random destination address that does not exist. Whenever the malicious node receives the fake RREQ packet, it creates a RREP packet with a fake route to the destination address and replies to the destination node. Thus, when the source node receives the RREP packet in reply to the fake RREQ, it identifies that there is some malicious node in the network and checks the RREP initiator field in the RREP packet to identify the node which initiated the RREP packet in reply to fake RREQ packet. Then source node records the address of malicious node in a blackhole list table. This table stores the addresses of all malicious nodes. The nodes present in the table are prevented to take participation in the routing. The fake RREQ and fake RREP packet is shown in figure 3 and 4 [7]. This is same as the DBA-DSR algorithm but difference the proposed and DBA-DSR starts after the process of fake RREQ and RREP is completed.

Type	Reserved	Hop Count
RREQ ID		
Destination Address (Fake destination address in modified version)		
Source Address		
Path		

Fig. 3 Fake RREQ Packet format

Now, when the process of fake RREQ and RREP is completed, then the normal DSR routing is started. When the source node receives the RREP packet in reply to original RREQ packet, it checks whether the RREP is from destination or from intermediate node. If the reply comes from destination node, then the source node assumes the route is safe. If the RREP comes from intermediate node, then the previous node of the intermediate node sends the ACK packets to destination along the path. If previous node receives the reply of the ACK

packet, then the route is safe and it unicasts the RREP packet to the source node and source node start sending the data. If previous node does receive any reply of the ACK packet, then it broadcast the alarm message through out the network about the malicious intermediate node. Then all the nodes update their black hole list. Thus black hole node can be detected in the network. The proposed solution consists of two mechanisms: one to detect the blackhole node in the initial stage, and the other to find the source route to the destination in the later stage.

Type	RREP initiator Field	Hop count
Destination Address		
Source Address		
Life Time		
Path		

Fig. 4 Fake RREP packet format

IV. Conclusion and Future Scope

In this paper, an algorithm to detect the black hole attacks in MANET has been proposed. The proposed algorithm removes the disadvantages of the DBA-DSR algorithm. In DBA-DSR algorithm, the routing overhead and route discovery period increases. But in the proposed algorithm, the routing overhead decreases and route discovery period also decreases. In future, this algorithm will be implementing on NS2 simulator taking routing overhead and throughput as parameters.

V. References

- [1] N. Shanthi, Dr. Lganesan, Dr. K. Ramar, "Study of Different Attacks on Multicast Mobile Ad Hoc Network" In Journal of Theoretical and Applied Information Technology, 2005-2011 JATIT, pp. 45-51.
- [2] Stephen Dabideen, "An End-to-End Solution for Secure and Survivable Routing in MANETs", 2009 7th International Workshop on the Design of Reliable Communication Networks 978-1-4244-5048-0/09/\$26.00 c_2009 IEEE (pp 183-190)
- [3] Xu Xiang, "Providing Efficient Secure DHTs Routing", 2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 © 2009 IEEE (pp 510-514)
- [4] Yanzhi Ren, "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", 978-1-4244-7265-9/10/2010 IEEE
- [5] Lanjun Dang, "DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks", 2010 IEEE Asia-Pacific Services Computing Conference 978-0-7695-4305-5/10 © 2010 IEEE (pp 454-461)
- [6] Saurabh Gupta, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCTT)-2011 978-1-4577-1386-6/11 © 2011 IEEE (pp 468-473)
- [7] Isaac Woungang, "Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1-4673-1550-0/12 © 2012 IEEE
- [8] Rutvij H. Jhaveri, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", 2012 Second International Conference on Advanced Computing & Communication Technologies 978-0-7695-4640-7/12 © 2012 IEEE (pp 556-560)
- [9] Rajesh Yerneni, "Enhancing performance of AODV against Black hole Attack", CUBE 2012, September 3-5, 2012, Pune, Maharashtra, India. Copyright 2012 ACM 978-1-4503-1185-4/12/09 (pp 857-862)