Securing Against Collaborative Blackhole Attack in Wireless Ad-Hoc Network

Mr. Deepesh Dilip Jagdale, Mr. Siddhesh Khanvilkar

Abstract— The Networks which are not connected cables of any kind are term as Wireless Networks. The introduction of cables is expensive. Therefore, Enterprises incorporate Wireless Networks into buildings or as a connection tool between entirely different equipment locations. The vulnerability of these networks to several attacks is an issue to be a tackle. A prerequisite in the design of mobile ad hoc networks (MANETs) is the establishment of communication among nodes i.e. the nodes must collaborate with one another. Within the prevalence of malicious nodes, this demand might result in serious security concerns; for instance, such nodes might disrupt the routing method. Considering this one of the biggest challenges is prevention and detection of malicious nodes which launching gray hole or collaborative black hole attacks may be a challenge. This project tries to resolve this issue by planning an Ad Hoc on-demand distance vector routing (AODV) based routing mechanism; i.e. referred as the cooperative bait detection scheme (CBDS), that integrates the benefits of reactive defense architectures. CBDS technique implements a reverse tracing method to assist in achieving the projected goal. Thus, with the blend of CBDS with different well-known message security scheme named hash coding, securing routing framework is attain.

Index Terms— Blackhole Attack, Collaborative Blackhole Attack, Wireless Ad-hoc Network.

1 INTRODUCTION

A wireless ad hoc network (WANET) is like distributed type of wireless network. The network is ad hoc because it does not depend on a pre-existing setup, like as routers used in wired networks or access points used in managed wireless networks. Instead, each node contributes in routing by sending data to other nodes. In addition to the classic routing, ad-hoc networks can use flooding for forwarding data.

The quick development of Internet has made communication an integrated and critical influence of computing. In today's culture with the development of wireless devices, it has become essential to stay online all the time. In demand to stay online all the time it must be possible to set up a network quick and profitable when moving between different setups, ad hoc networks deals with this types of issues.

An ad-hoc network is a pool of wireless mobile nodes dynamically establishing a temporary network without the support of any traditional setup or central management. Routing protocols in the mobile ad-hoc network helps node to send and receive packets.

In a MANET, every single node not only works as a host but can similarly act as a router. While receiving data, nodes also want support with each other to forward the data packets, by this means making a wireless local area network.

- *Deepesh Jagdale is currently working as a lecturer in Dept. of Information Technology at Pillai HOC College of arts, Science & Commerce,Rasayani, Maharashtara, India. E-mail:deejagdale@live.com.*
- *Siddhesh Khanvilkar is currently working as aAsst. Professor in Dept. of Information Technology at Pillai HOC College of Engineering & Technology,Rasayani, Maharashtara, India. E-mail: khanvilkar.siddhesh770@gmail.com.*

These excessive features also drive with severe shortcomings from a security point of view. For instance, the presence and association of malicious nodes in the network may interrupt the routing process, important to a malfunctioning of the network operations.

Cooperative Black Hole Attack:

In AODV routing protocol, the source node S, wish to communicate with the destination node D. Then Source node S broadcasts the route request (RREQ) packet to their neighboring active nodes and fills in their routing table with an entry for the source node S. Then checked if it is the destination node or has the new route to the destination node. If it does not have, then the intermediate node fill in the RREQ (by increasing the hop amount) and passes the RREQ to the destination node D till it finds their destination or any other in-between node which has a new route to D, as described by example in Fig.1. The destination node D or the in-between node with a new sufficient route to D, initiates a route reply (RREP) in the opposite path, as defined in Fig.2. The source node S starts sending the data packets to their neighboring node which answered first and discarded the other responses. So this works satisfactorily when the network has no malicious nodes.

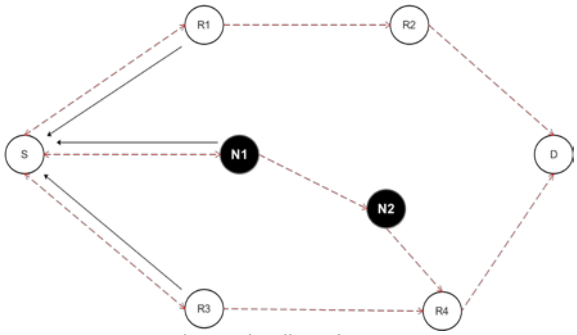

Fig. 1: Flooding of RREQ

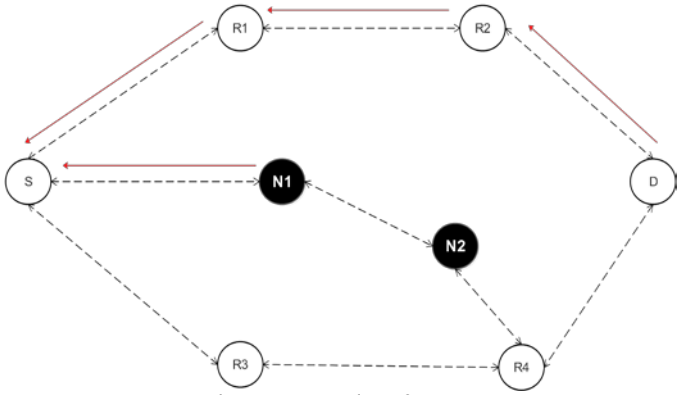

Fig. 2: Propagation of RREP

There are several algorithm and techniques to differentiate and remove a single black hole node. In the case of multiple black hole nodes, meanwhile, in coordination has not been addressed.

For, e.g., when multiple black hole nodes are acting in synchronization with each other, the first black hole node N1 mentions to one of its associative blackhole N2 as the next hop, as described Fig.2. In above, the source node S sends a "Further Request (FRq)" to N2 through an altered route (S-R3-R4-N2) other than via N1. Source node S asks N2 if it has a path to node N1 and a path to destination node D. Because N2 is collaborating with N1, its "Further Reply (FRp)" will be "OK" to both the inquiries. Now node S starts passing the data packets supposing that the route S-N1-N2 is secure. Though, in reality, the packets are consumed by node N1 and the security of the network is conceded.

2 Literature Survey

Cooperative bait detection scheme (CBDS) that aims at identifying and avoiding malicious nodes introduce gray hole/collaborative black hole attacks in MANETs [1]. The strategy was the source node casually selects the neighboring node with which to work together. In the context, that the address of this node is employed as bait destination address to attract malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from taking part in the routing operation, employing a reverse tracing technique. In this scenario, it is expected that once a significant drop happens within the packet delivery ratio, an associate alarm is distributed by the destination node back to the source node to trigger the detection mechanism once more. CBDS theme merges the advantage of proactive detection within the initial stage and also the superiority of reactive response at the succeeding steps so as to reduce the resource wastage.

A secure mechanism, which consists of checking the proper forwarding of packets by an intermediate node, was proposed by the researcher. The suggested solution avoids the black hole and the co-operative black hole attacks by Markley Tree using AODV protocol. A Marklee tree is a binary tree in which, each leaf carries a given value and the value of an internal node (including the root) is a one-way hash function of the node's children values. AODV (Ad hoc On-Demand Distance Vector) is a reactive routing protocol [2].

Two techniques called that increase throughput in an ad hoc network in the presence of nodes that approve to forward packets but fail to do so. To mitigate this difficulty, the author proposes categorizing nodes based upon their dynamically measured performance. The author uses a "watchdog" that identifies misbehaving nodes and a "pathrater" that helps routing protocols avoid these nodes [3].

A mechanism described, to detect and remove the cooperative black hole or gray hole attack in MANET. The method work as follows. At first, a backbone network of trusted nodes is conventional over the ad hoc network. The source node occasionally requests one of the backbone nodes for a limited (unused) IP address. Whenever the node wants to make a communication, not only, it sends a route request (RREQ) in search of destination node but also in search of the limited IP concurrently. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the limited IP (LIP) also. If any of the routes answers confidently with an RREP to any of the limited IP, then the source node starts the detection method for these malicious nodes [4].

All above are schemes for Proactive detection schemes that need to detect regularly. In these schemes, irrespective of the existence of malicious nodes, the overhead of detection is continuously created, and the resource used for detection of the malicious node is a waste. Nevertheless, one of the advantages of these types of schemes is that it can help in avoiding an attack in its initial stage.

Xue and Nahrstedt recommend a new routing service named Best-effort Fault-Tolerant Routing (BFTR). The design goal of BFTR is to provide packet routing service with high delivery ratio and low overhead in the presence of misbehaving nodes [5]. Instead of refereeing whether a path is right or wrong, i.e., whether it contains any malicious node, BFTR calculates the routing possibility of a path to its end-to-end performance (e.g. packet delivery ratio and delay). By continuously noticing the routing performance, BFTR dynamically routes packets via a possible path.

Kozma and Lazos propose a novel misbehavior identification system called Resource Efficient Accountability that provides resource-efficient accountability for node misbehavior. REAct identifies misbehavior nodes based on a series of random audits triggered by a performance drop [6].

Dixit and Singh suggested for the design of hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths. The new method is robust against collaborative attacks described in the paper, and it introduces limited computational overhead on the intermediate nodes. The author proposes to develop a new mechanism for audit based detection of collaborative packet drop attacks [7].

Dynamic Source Routing is a technique in which the sender of a packet determines the complete order of nodes through which to forward the packet. The sender clearly lists

this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.[8]

All above are schemes for Reactive detection schemes that activate when only the destination node senses a significant drop in the packet delivery ratio.

3 Problem Statement

Detecting malicious nodes and packet dropping is necessary for the ad-hoc network to fight against a variety of security attacks such as gray hole attack, black hole attack, and wormhole attack. We consider detecting a collaborative black hole attack because collaborative black hole attack is one of the hardest problems in the mobile ad-hoc network. Using Co-operative Bait Detection Scheme (CBDS), in which the source selects a neighboring node as the bait destination address. However, selecting the adjacent node among the neighbors of the source is not described. If the attacker can find out that adjacent node, it will try to escape the Bait request. The detection of collaborative attack is invoked based on the packet delivery ratio (PDR) metric by the destination node. However, PDR alone will not be sufficient to detect the misbehaving attacks. Moreover, the detection delay will be increased since the discovery process is invoked when only the destination sends an alarm.

4 Proposed System

The proposed system, investigate the integration of CBDS with other well-known message security scheme to secure routing framework. In this work by implementing MD5 cryptographic hash function algorithm to encrypt the message to secure data of the packet.

The proposed scheme comprises three stages:

1) The initial bait setup
2) The initial reverse tracing stage
3) The shifted to reactive defense stage

The first two stages are initial proactive defense stages, whereas the third stage is a reactive defense stage.

4.1 Initial bait setup:

The objective of the bait phase is to invite a malicious node to send a reply RREP by sending the bait RREQ'. It has used to announce itself as having the shortest path to the node that details the packets that were converted. The RREQ' is made up of constructing the mock frame; the mock frame is build by source address, destination address, a message to be sent, and hash code parameters.

The following method is designed to generate the destination address of the bait RREQ':

1) The source node stochastically selects a neighboring node, within its one-hop neighborhood nodes and collaborates with this adjacent node by taking its address, as the destination address of the bait RREQ'.

2) The bait phase is triggered whenever the bait RREQ' is sent before seeking the initial routing path.

The follow-up bait phase analysis as follow:

1) If the nr node has not launched a black hole attack, then after the source node had sent out the RREQ', there will be other nodes reply RREP in addition to that of the nr node. It indicates that the malicious node is present in the reply routing, as shown in Fig 3.

2) Therefore, the reverse tracing stage in the next step would be initiated to detect this route.

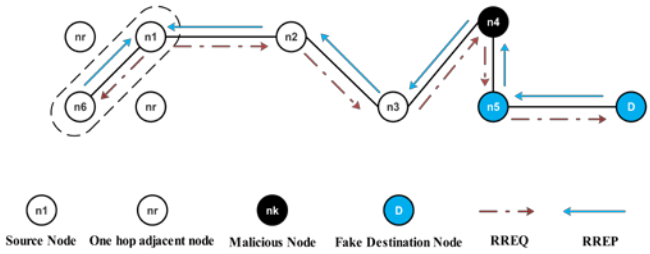

Fig. 3: Selection of one hop next node

3) If only the nr node has sent the reply RREP, it means that there was no other malicious node present in the network.

4) If the nr node is the malicious node of the black hole attack, then after the source node has sent the RREQ', other nodes (in addition to the nr node) would have also sent reply RREPs.

5) It would indicate that malicious nodes existed in the response route. In this case, the reverse tracing stage in the next step would be initiated to detect this path.

6) If nr intentionally gave no reply RREP, it would be directly listed on the blackhole list by the source node.

4.2 Initial Reverse tracing:

The reverse tracing stage is used to notice the behaviors of malicious nodes through the route reply to the RREQ' message. If the malicious node has received the RREQ', it will reply with a false RREP. Accordingly, the reverse tracing process will be conducted for nodes receiving the RREP, with the goal to reduce the duplicate path information and the temporarily trusted zone in the route.

It should be a highlight that the CBDS can detect more than one malicious node simultaneously when these nodes send reply RREPs. Each node which is contributing in the process will maintain the table as follow:

Next Hop id	Count

Following operation will processes:

1) Source node or any intermediate node acknowledges to next hop whether the frame is forwarded or not. If

acknowledgment message does not come within the timer then increase the Count
2) If Count Value exceeds the threshold value, then alarm message sent to source node with misbehaving node id.
3) Source node maintains a blacklist of such misbehaving node and informs all other nodes to terminate their operation with this node via broadcasting an alarm message packet.
4) So when next route discovery phase starts then source node removes the path which having blacklisted nodes.

4.3 Shifted to Reactive Defense phase:

After above steps, AODV route discovery process is activated. When the route is established, and if the node is a malicious node which launches packet dropping or delays attack then detection scheme is triggered again to detect malicious node.

4.4 Algorithm:

1) Source node S creates the mock packets.
2) For each packet to be sent by S: Construct mock data frame with Source node address, Destination node address, message to be sent and hash code
3) When a source node sends data frame, it encrypts that frame.
4) Source node or any intermediate node starts Attack Prevention Timer (APT) while forwarding the frame.
5) Source node or any in-between node acknowledges to its next hop whether the frame is forward or not. If acknowledgment message does not come within the timer then increase the Count
6) If Count Value exceeds the threshold value, then alarm message sent to source node with the misbehaving node id. Alarm message sent such way the RERR is forwarded to Source node.
7) Source node maintains a blacklist of such misbehaving node, so when next route discovery phase starts then, source node removes the path which having blacklisted nodes.
8) Intermediate node decrypts the frame & checks whether the destination address is matched with its address if not then it forwards frames to next hop.
9) If destination address field matched with node address then packets are reconstructed at destination & hash value is computed if it matches then the path is ok, but if it does not match then the path is not malicious node free, then destination node sends an acknowledgment to Source node.
10) Source node maintains the path of the blacklist node.
11) Source node starts route discovery process.
12) If any path matches that path of the blacklist and includes nodes from node blacklist, then source node discards the route.
13) If the path is ok, then source node starts sending packets to the destination node.

5 Result Analysis

5.1 Simulation Model and Parameters:

The Network Simulator (NS2), is used for simulation. In the simulation, 30 mobile nodes are deployed in a 1000 meter x 1000 meter region with a simulation time of 100 seconds. All nodes in the simulation have the same transmission range of 250 meters. The traffic is Constant Bit Rate (CBR).
The simulation settings and required parameters are shown in Table-1.

TABLE-1
SIMULATION SETTINGS

No. of Nodes	5,10,15,20,25,30
Area Size	1000 X 1000
Protocol	AODV, SCA, AODVWA
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512
Rate	150 kbps

5.2 Performance Metrics:

The proposed system Secured Collaborative Attack Scheme (SCA) for detecting collaborative attacks is compared with CBDS [1]. The performance is calculated mainly, according to the following metrics.

1) **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.

2) **Routing Overhead:** It is the ratio between the amount of routing-related control packets transmissions to the amount of data transmissions.

3) **End-to-End Delay:** It is the time taken for a packet to transmission from the source to the destination.

4) **Throughput:** It is the total amount of data that the destination receives them from the source divided by the time it takes for the destination to get the final packet.

5.3 Results:

The proposed system Secured Collaborative Attack Scheme (SCA) is evaluated with AODV and AODVWA.

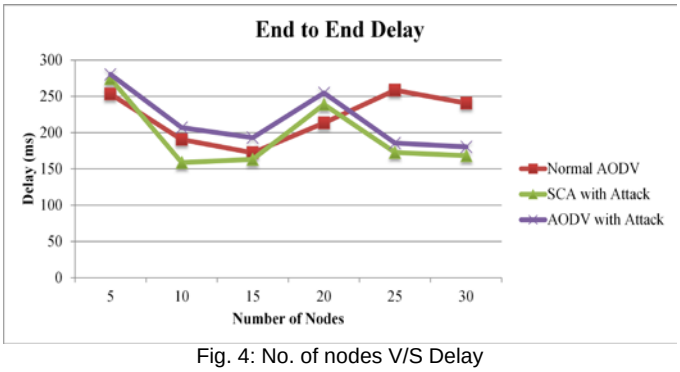

Fig. 4: No. of nodes V/S Delay

In Fig. 4 No. of nodes is compared with an end to end delay so as a result SCA algorithm produce less delay at the time of

execution than other two algorithms i.e. Normal AODV and AODVWA.

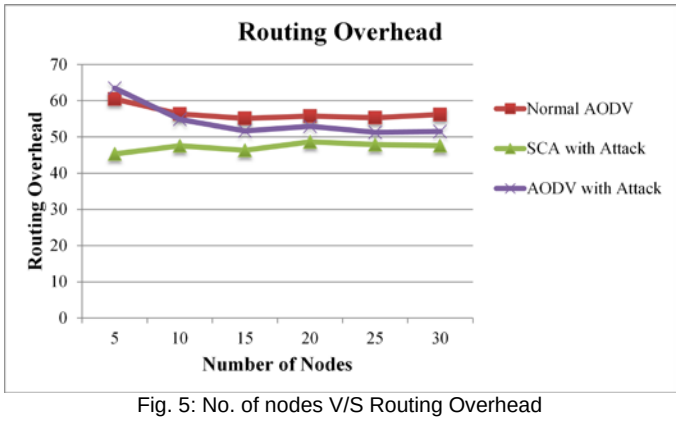

Fig. 5: No. of nodes V/S Routing Overhead

In Fig.5, Number of nodes are compared with overhead so as a result SCA algorithm produce less overhead at the time of execution than other two algorithms i.e. Normal AODV and AODVWA.

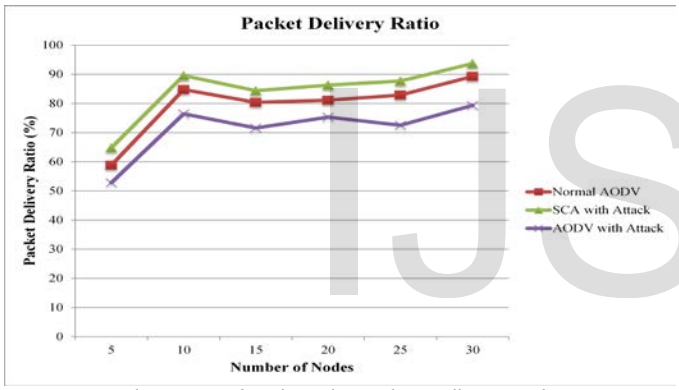

Fig. 6: No. of nodes V/S Packet Delivery Ratio

In Fig.6, Number of nodes is compared with packet delivery ratio so as a result SCA algorithm delivers the maximum packet to the destination at the time of execution than other two algorithms i.e. Normal AODV and AODVWA.

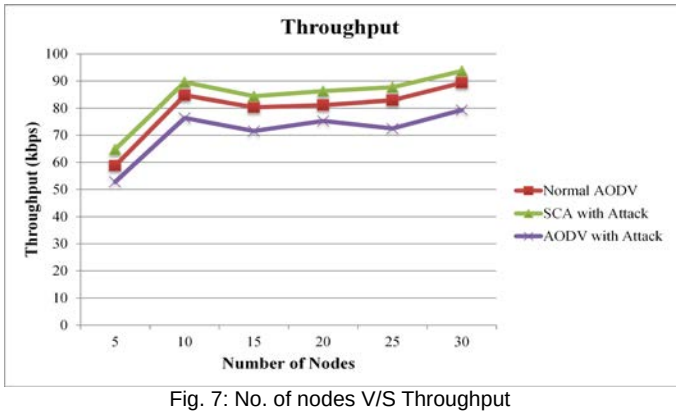

Fig. 7: No. of nodes V/S Throughput

In Fig.7, Number of nodes is compared with throughput so as a result SCA algorithm provides maximum throughput at the time of execution than other two algorithms i.e. Normal AODV and AODVWA.

6 Conclusion

This paper proposes the combination of CBDS with alternative well-known message security theme to construct a comprehensive secure routing framework to safeguard wireless Ad-hoc Network. The proposed system established and recognized the shortcomings of the existing approach. Henceforth there is a requirement of SCA approach. A Secure Collaborative Attack (SCA) algorithm with AODV protocol for Wireless Ad-hoc Network is established. Based on the strength and path-delay, the node is updated in the table for confirmation of node whether it is infected or not. Using APT timer mechanism the dependability and path information is found. Once a malicious node is detected, route discovery method started and because the maintenance of blacklist path at source node secure route can be discovered. To achieve this, a secure hash function is generated using the MD5 cryptographic hash function. The comparative analysis of message security algorithm also suggests the use of the simplest suitable algorithm.

7 References

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chen-Feng Lai, "Defending Against Collaborative Blackhole Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," IEEE Systems Journal, 2014, pp 1 to 11.

[2] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255 to 265.

[4] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28 to 32, 2010.

[5] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers. Communication., vol. 29, pp. 367 to 388, 2004.

[6] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, 2009, pp. 103 to 110.

[7] Ashutosh Dixit and Sandeep Kumar Singh, "Performance Evaluation of DSDV, AODV and DSR Routing Protocol in MANET," Int. Journal of Scientific and Research Publications, Volume 5, Issue 3, March 2015.

[8] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Computation., pp. 153 to 181,1996.