International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 5; Issue: 6; June-2016

A Secure Cooperative Bait Detection Approach for Detecting and Preventing Black Hole Attacks In MANETS Using CBDS

Shireen Sultana[1], Swati Patil[2]
[1]*PG Student, Department of Computer Science and Engineering,*
[2]*Assistant Professor, Department of Computer Science and Engineering,*
Lingaraj Appa Engineering College, Bidar, Karnataka State, India.

***Abstract*— In MANET, a major necessity to distribute the communication between nodes is that each node should work along with each other. This communication could face many obstacles created by adversary resulting in disconnection. To overcome this problem a new mechanism based on dynamic source routing (DSR) which could be mentioned as cooperative bait detection scheme (CBDS). It merges the favors of both proactive and reactive protection phenomena. This method performs a reverse tracing technique which aids in accomplishing the desire. As a result CBDS perform better than the existing method which includes the DSR and 2ACK protocols with regard to packet delivery ratio and routing overhead. As an extension work, we propose an authentication scheme based on elliptic curve cryptograph (ECC). With this it is possible to enable intermediate nodes authentication.**

***Keywords*— Black hole attacks, gray hole attack, cooperative bait detection scheme (CBDS), mobile ad hoc network (MANET), malicious node**

I. INTRODUCTION

Mobile ad hoc networks (MANETS) play a vital role in networks. In wireless network there may be a serious security issue. The network is decentralized, where discovering the topology and delivery of messages must be executed by the node itself. A MANET is a kind of ad hoc network that can use different location and configure itself in air. The applications for network in MANETs are separate, to large scale, mobile, highly dynamic network.

There is less security in MANET, it is used in military operations and traffic control in networks. In MANET there is no infrastructure, on-demand, dynamic topology. The node is the mobile network, so it is difficult to identify the hacker node. The routing process may disrupt due to the collaboration attacks by malicious node in MANET. The malicious node may cause security problems like gray hole and collaborative black hole attacks. Many research people say about the prevention and detection of MANET. Due to the dynamic topology the mobile nodes will face several attacks. The most frequent attacks are black hole and gray hole attacks.

There are two types of attacks in MANET. They are active attack (black hole) and passive attack (gray hole). Black hole attack is defined as if a source is going to send a data in the mobile ad hoc network its sends through several nodes to reach the destination. The black hole establishes the information to source that it has the shortest path to the destination. The hacker node will attract all the data packets by using fake route reply (RREP) to make shortest route for the destination. The black hole attack is also known as active attack. The gray hole attack which is called as passive attack at first it acts like good node later it behave as malicious node. This is also called as trust based security solution. It does both forwarding and discarding the packets, the gray hole attack is very tough to find in initial stage. These attacks can be resolved by dynamic source routing protocol based on cooperative bait detection scheme.

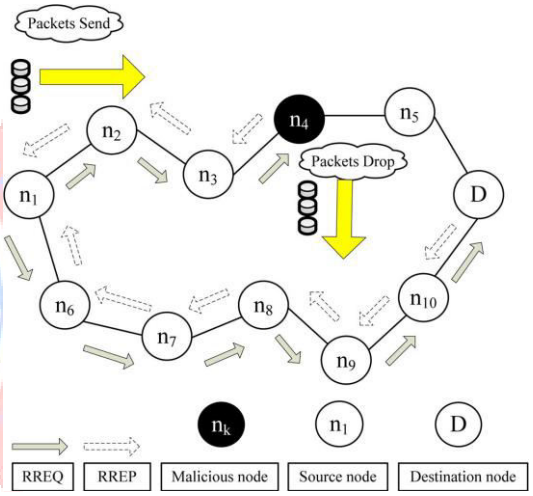

Fig.1 Blackhole attack–node n_4 drops all the data packets

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In blackhole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. In grayhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. In this paper, our focus is on detecting grayhole/collaborative blackhole attacks using a dynamic source routing (DSR)-based routing technique.

II. RELATED WORK

In 2010[2] avoiding black hole attacks in wireless ad hoc network is proposed. The node which is the middle forwarding will act as hacker and leaks the data packet which passes through it, without forwarding them to the following node, this process is called black hole attack. A secure mechanism is found which checks the good forwarding of data packets by the malicious node. The merkle tree is as the secured principle for avoiding the black hole attacks and cooperative black hole attacks.

In March 2011[3] CBDS in hybrid defense architecture is established. The protocol in present AODV, DSR nearly take account in execution. It doesn't have the similar mechanism in finding and response. A technique to find hacker node introducing cooperative black hole attacks and black/gray hole attacks is called as cooperative bait detection scheme (CBDS). It merges the proactive and reactive architectures, and stochastically works with random adjacent node. By using the address of the neighbor node as the bait destination address and finds the malicious node by reverse tracing program and consequently prevent the attacks.

In 2010[4] to detect and remove black/gray hole attack in mobile network is published. At first the source node need to make the packet transmission, so it ask the nearest node for Blocked IP (BIP). The nearest node will get the BIP response to the source node from the unknown IP addresses. The reply RREP is send to both BIP and destination continuously. If the source node gets reply from the normal destination, it means there is no black hole in the path. When source node gets reply from the BIP, it says Black hole attacks are present in the path. Finally the source finds the black hole in the route. After finding the black hole attack, source node sends the dummy data to the destination. The nearby node finds the packet drops and it informs the source node. Here the algorithm finds the location of black hole.

In September 2009 [5] to prevent collaborative pack drop attacks in ad hoc network is introduced. The hash function based mechanism is used for finding packet drops in the network. It holds the knowledge from packet traffic and data forwarding routes. The above method is opposed to the collaborative attacks. The method has helped in order to inquire the security of the proposed mechanism and diminish the overhead.

In 2009[6] REAct is stated. This study reported the difficulty of finding the group of improper nodes which rejects the data packets without forwarding them to destination. To overcome the above problem the method called REAct is introduced. REAct finds malicious node by the number of random audit mechanism on execution drop. A source node and destination can able to find malicious node by using REAct mechanism based on proofs. A Proof is made by using bloom filters and it reduces the communication overhead problem for malicious node detection.

III.COMPARISON OF DSR AND TCP/IP PROTOCOLS

a) TCP PROTOCOL:

Transfer Control Protocol is very popular used commonly in the internet. There are four layers in TCP Protocol

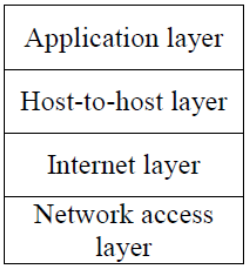

Fig. 2 Four layers of TCP

The network layer is in charge for sending and receiving TCP data packets in the network. The network layer does the work of datalink layer and physical layer which is presented in the OSI model. The internet layer is responsible for packing the data, addressing and routing the packets to the destination. In host-to-host layer the data packets are transported and deliver them to the application layer. The transport layer is used for transporting and sequencing the packets in the network. Finally it recovers the data packets from the source.

Limitation:

- In MANETs, frequent wireless network errors and mobility leads to packet losses as well as congestion
- Due to link failure 80% of packet loss will occur.
- Most of the packet losses in ad hoc are because of path failure.
- To overcome the above limitation we are going for the technique called **DSR** (dynamic source routing technique).

b) DSR PROTOCOL:

Dynamic routing protocol is defined as if the source node wants to send the data to the destination, it doesn't know the path for source node S to the destination node D [1]. The source sends the route request (RREQ) to the entire node which is in the network [1]. The source will get route response (RREP) from each and every node in the network with the source address, destination address and unique route request id (RREQ).

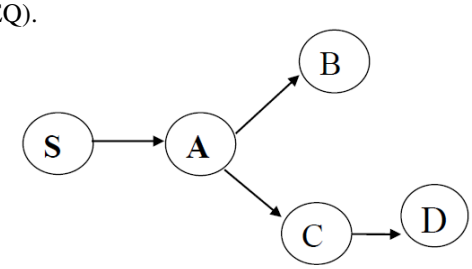

Fig.3 Network Architecture

In the above diagram S is the source A, B, C, are the nodes in the network and D is the destination. Source sends the RREQ to all nodes and gets RREP from the destination. The node S does not sure to find which node in the network has the path information [1] to the node D or the hacker node reply fake RREP. From above content the source node S will send data packets through the malicious path chosen by the hacker node [1]. Which is called as black hole attack, to overcome this CBDS algorithm is proposed.

IV. COMPARISON OF 2ACK SCHEME WITH CBDS ALGORITHM

a) 2ACK SCHEME:

The 2ACK scheme is used to reduce the hacker's effect in malicious node [7]. The general theme of 2ACK algorithm is, if the source node S sends the packets to its neighbor hop successfully, the destination node D of neighbor choose to send a unique two-hop acknowledgement is called 2ACK to specify that the packets received successfully [7]. The 2ACK transmission is used for only a few data packet transmission. The certain node behavior id identified after watching its activity for a few hours [7].

The 2ACK scheme is to find the adversary node which is suppose to forward the data packets from the source node but it oppose to do so when the data packets arrived [7]. The 2ACK will monitor and transmits only when the routing performance is very low and it has very well authentication to check the packets are genuine [7]. The main drawback is, 2ACK scheme is a proactive method to find the malicious nodes.

b) CBDS ALGORITHM:

Initially the detection mechanism is of two types, they are proactive and reactive.

Proactive: proactive mechanism is to find and prevent the network from the malicious node in initial
stage [1].

Reactive: reactive mechanism is to detect that node which will be active only after the destination node finds a packet drop in the packet delivery ratio [1].

Cooperative Bait Detection Scheme is used for preventing and detecting the black hole/gray hole attacks [1]. A black hole attack is defined as if the source node wants to send the data packets to the destination, it losses the data packets before forwarding to the destination [1]. The gray hole is nothing but, initially the node act as the good node, after few minutes it changed into malicious node [1]. By using the CBDS algorithm, at first the source node will select the neighbour node with the cooperation of that node [1]. The address of the selected node is known as bait destination address to trap the malicious node to send a request reply message [1]. By using tracing technique the adversary node is detected and prevented [1]. If any packet drop occurs in the packet delivery ratio, an alarm is send to the source node by the destination node to activate the detection mechanism [1]. The CBDS scheme combines the proactive scheme to find the malicious node in the initial stage and reactive mechanism to find the adversary node later in the network.

V. BASIC IDEA OF THE SYSTEM

Initially the source S choose the cooperative bait address of the one hop neighbor node Nr to detect the malicious node and [1] sends the RREQ to all the nodes in the ad hoc network [1]. If there is no reply from any of the in the network means there is no malicious node in the network. Suppose the source node gets RREP from any node in the network, it triggers the reverse tracing program and sends test packets, recheck message to detect the malicious node in the MANET [1]. The source node lists the malicious node in the black hole attack and sends the alarm packet.

In another case source node sends RREQ to the nodes in MANET [1], if it gets the reply RREP from the original destination address then the system does not contain any adversary it is free from malicious node [1]. Suppose the reply RREP is not from the true destination address, then it exceeds the new hop limit.

VI. MODULES DESCRIPTION

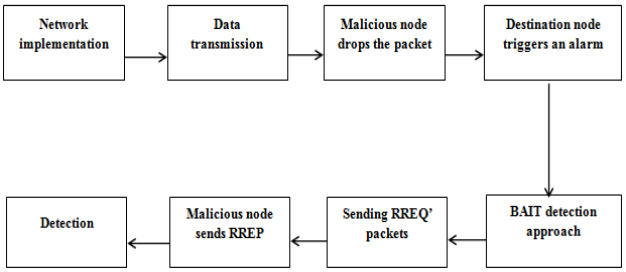

Fig. 4 Block diagram of Proposed System

- Mobile ad-hoc network creation and implementation of malicious nodes

In this module, a Mobile ad-hoc network is created. All the nodes are configured and randomly deployed in the network area. Since our network is a mobile ad-hoc network, nodes are assigned with high mobility (movement). A sample routing is performed to check the connectivity in the network. A node is randomly selected and configured as malicious. This malicious node attracts the data packets towards it and drops them anonymously. The network connectivity is analyzed between the nodes.

- Implementation of BAIT detection approach

In this module, in our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

And as na extension work, for each message, the message sender, or the sending node, generates a source anonymous message authenticator (AMS) for the message. The generation is based on the MES scheme on elliptic curves.At the receiver end, the assigned AMS must be verified by the nodes public keys.

VII. RESULTS

After implementing the proposed system on NS2, the results obtained are as follows:

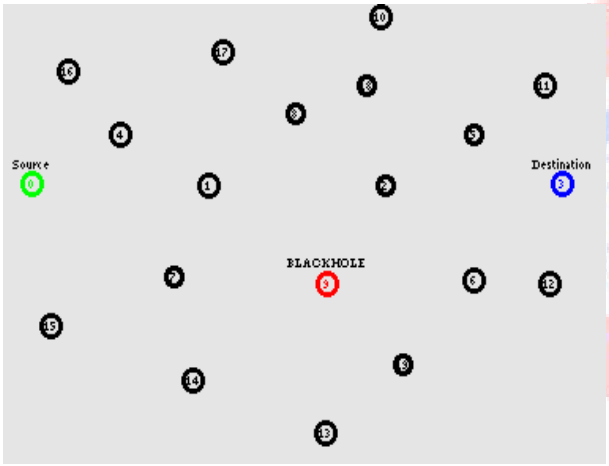

Fig.5 Network Deployment

The figure 5 shows the network creation stage, where we can see the topology of the network and also identifying the nodes like source node, destination and also blackhole present in the network.

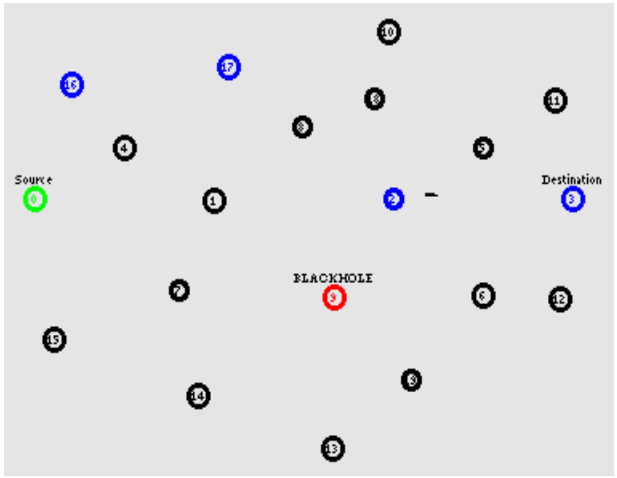

Fig.6 Nodes Communication Stage

In figure 6 communication can been between the source node and destination node by suppressing the effect of presence of blackhole node.

The figure 7 shows the throughput comparison graph drawn using Xgraph function. The graph shows that the performance of proposed system is better than the existing system, i.e. the throughput value is high for proposed system.

The figure 8 shows the energy consumption comparison graph drawn using Xgraph function. The graph shows that the performance of proposed system is better than the existing system, i.e. the proposed system has consumed less energy as compared to existing system.

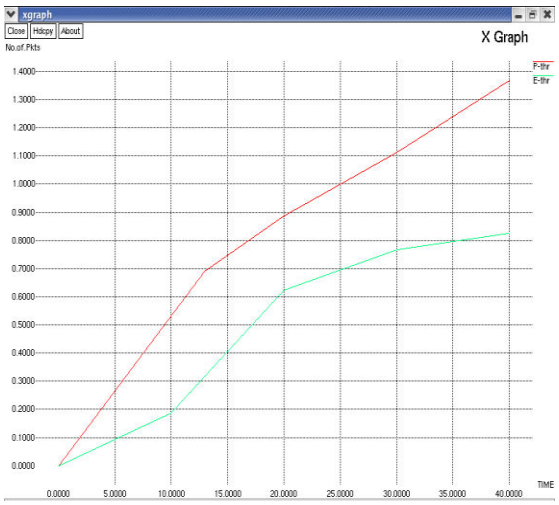

Fig. 7 Throughput comparison graph

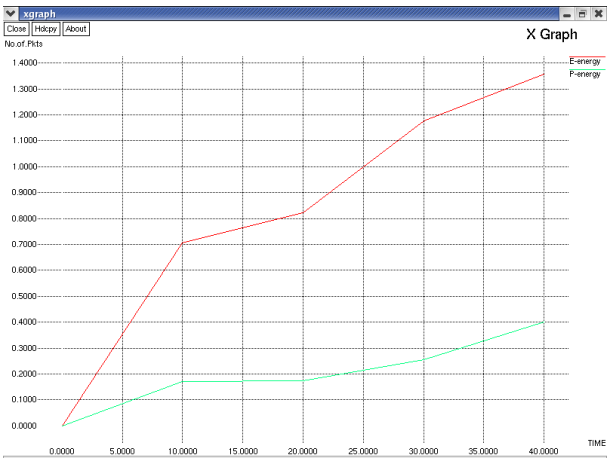

Fig.8 Energy Consumption comparison graph

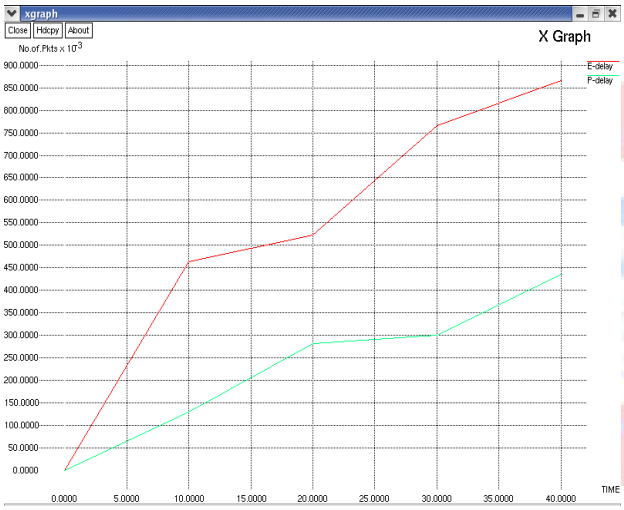

Fig.9 Delay Comparison graph

The figure 9 shows the delay comparison graph drawn using Xgraph function. The occurrence of delay is less in less in case of proposed system as compared to existing system.

VIII. CONCLUSION

In this paper, we have proposed a new technique (called the CBDS) for identification malicious nodes in MANETs under gray/collaborative blackhole attacks. Our simulation results shows that the CBDS performance is better as compared to previous techniques, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. As future work, we intend to 1) investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs and to 2) investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants. And we have also provided more security to the intermediate nodes with the help of elliptic curve cryptography (ECC) technique.

REFERENCES

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[2] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html

[3] C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

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

[7] 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. 255–265.

[8] 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. 28–32, 2010.

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[12] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.

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

[14] 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. 103–110.

[15] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[16] QualNet Simulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com

[17] IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications, pp. i-445.