International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Advanced Mutual Bait Detection Approach to Defend against Combined Attacks in MANET's

M S Sunitha Patel[1], Sneha N P[2]
[1, 2] *Department of Computer Science & Engineering, ATME College of Engineering*

Abstract: ***MANETS are abbreviated as Mobile Ad-hoc Networks; cooperation is primary requirement between the nodes for the communication establishment. Security is the major issue due to the presence of malevolent nodes, as they disturb the routing process. Here grayhole and blackhole attacks are major challenge, which launch malicious nodes which are to be detected and prevented. Advanced Mutual Bait Detection scheme resolves this issue by designing a routing mechanism based on dynamic source routing protocol which integrates the advantages and superiority of proactive and reactive defence architecture respectively. Reverse tracing technique is implemented through CBDS method to find the position of malevolent node.***
Keywords: ***MANET's, gray hole attack, black hole attack, malicious node, RREQ (route request), RREP (route reply).***

I. INTRODUCTION

In wired networks, the major issue in data communication is information security. Earlier, different kinds of steganographic techniques were used to secure information based on hiding data through invisible inks, wax tables, microdots etc. The emergence of wireless network rose security issues, which leads to many different issues in many different layers of network. The assertive digital communication environment for future is MANET's (Mobile Ad-hoc NETwork's).

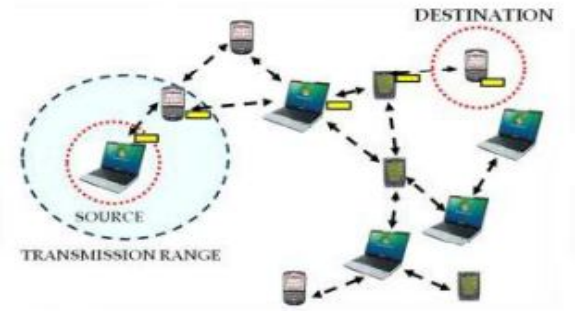

Fig 1: Mobile Ad-Hoc Network

MANET'S are wireless, temporary network which are formed by the collection of dynamic, mobile self-maintainable and self-configurable nodes which can act as both host and router without any centralized entities. The applications of MANET'S are military purpose, sensor networks, disaster networks, personal area network and so on.
In MANET there are many open issues, since MANETS are infrastructure less, security is a major concern due to which different attacks pop-up such as snooping attack, warm hole attack, gray hole attack, poisoning attack, DOS(Denial of service).
In this paper, we focus on gray hole and black hole attack. In both of these attacks of MANET'S, malicious nodes are present which drops the data packet leading to improper communication.
Black hole is a type of malicious nodes which drops all the packet and therefore can be identified and avoided easily before the communication starts, whereas gray hole attacks are difficult to identify which selectively drops the data packet which is challenging to identify.

A. Routing Protocols in MANET's

Routing is one of the issues in MANET because of its highly distributed and non-static nature. Routing protocols are broadly categorized as Novel, Proactive, Reactive and Hybrid protocols as shown in Fig 2.

1) *Novel Protocols:* Novel approach is a routing misbehaviour prevention system, in which a transmission query is designed, inspired by human behaviour, in case where one person investigates on the other through a person who collects the information and the person under investigation. A route selection is done based on gathered information.
2) *Proactive Protocols:* In proactive routing scheme, the malicious nodes are found using a bait address, RREQ (route request) if any node replies with the RREP (route reply), it is marked as a malicious node.

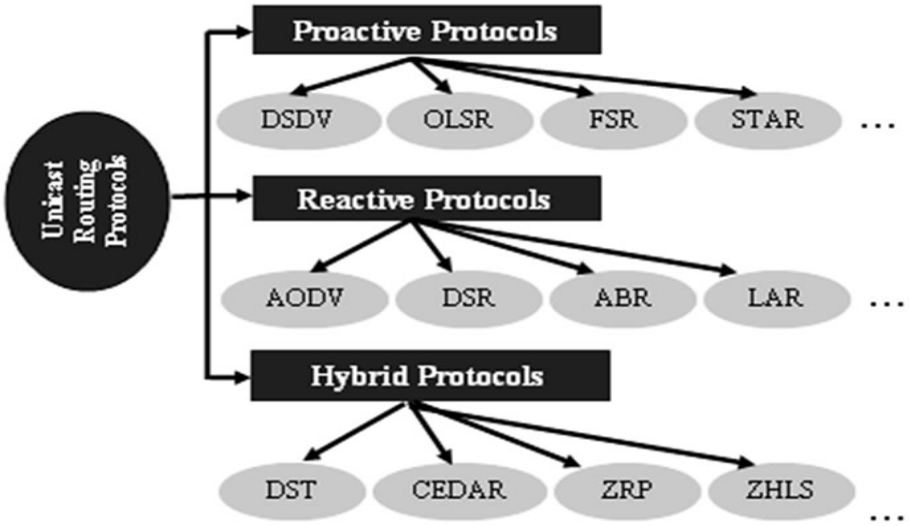

Fig 2: Routing Protocol Classification

3) Reactive Protocols: In reactive routing scheme the gray hole attacks are identified by maintaining the success ratio of data packet transmission and threshold. In both proactive and reactive schemes, malicious nodes are traced using a reverse tracing technique and the malicious nodes are black listed and broadcasted among the network.
4) Hybrid Protocols: Hybrid mechanism uses advantages of both proactive and reactive schemes, finds the malicious node, and defends it.

B. Transmission Mechanism in MANET's

The data transmission in MANET's is carried in the following three phases:

1) Route discovery: When authorized route to destination is no longer valid and if the path to destination in prior unknown and source wants to communicate to destination, it broadcast RREQ to the nodes among MANTEs. To optimize the search, prior hop-wise distance is utilized for former known destination. By expanded ring search it uses increasingly large neighbourhoods to reach destination this technique is authorized by TTL filed in RREQ packet header.
2) Route Maintenance: Each entry in the routing table keeps up expiry time of route, which specifies route's validity. The expiry time is updated with the current time and ACTIVE ROUTE TIMEOUT whenever the data packet is been transmitted through the route. AODV monitors its neighbour nodes that enter into the data packet route by maintaining an active neighbour node list for every entry to the route. All the broken routes to destination are invalidated and neighbouring nodes are informed by RERR packet consecutively each neighbour forwards RERR packet to its active neighbour, which are present in its own list.
3) Data Transmission: Data transmission in MANET is done using selective repeat protocol, which is an end-to-end protocol. The data sent by the source node is acknowledged by destination node within in the time interval set by the source node as soon as it sends a data packet. If the destination node does not acknowledges within the time interval the source node resend the particular packet until it get the ACK packet in reply and starts the timer.

C. Security Issues In MANET

The security attacks in MANET's are shown in Fig 3. The subsequent list of issues indicates the inadequacies and restrictions that have to be overwhelmed in a MANET environment [2]

Restricted wireless transmission range: The radio group will be restricted in the wireless networks and as a result data amounts it can provide much slighter than what a bound network can provide. This involves routing procedures of wireless network that must be used in bandwidth. This can be achieved through protecting the overhead as minimum as conceivable. The restricted transmission range also enforces restraint on routing procedures for sustaining the topographical information. Particularly in MANETs because of regular variations in topology, preserving the topological data for every node includes more controller overhead which results in additional bandwidth depletion.

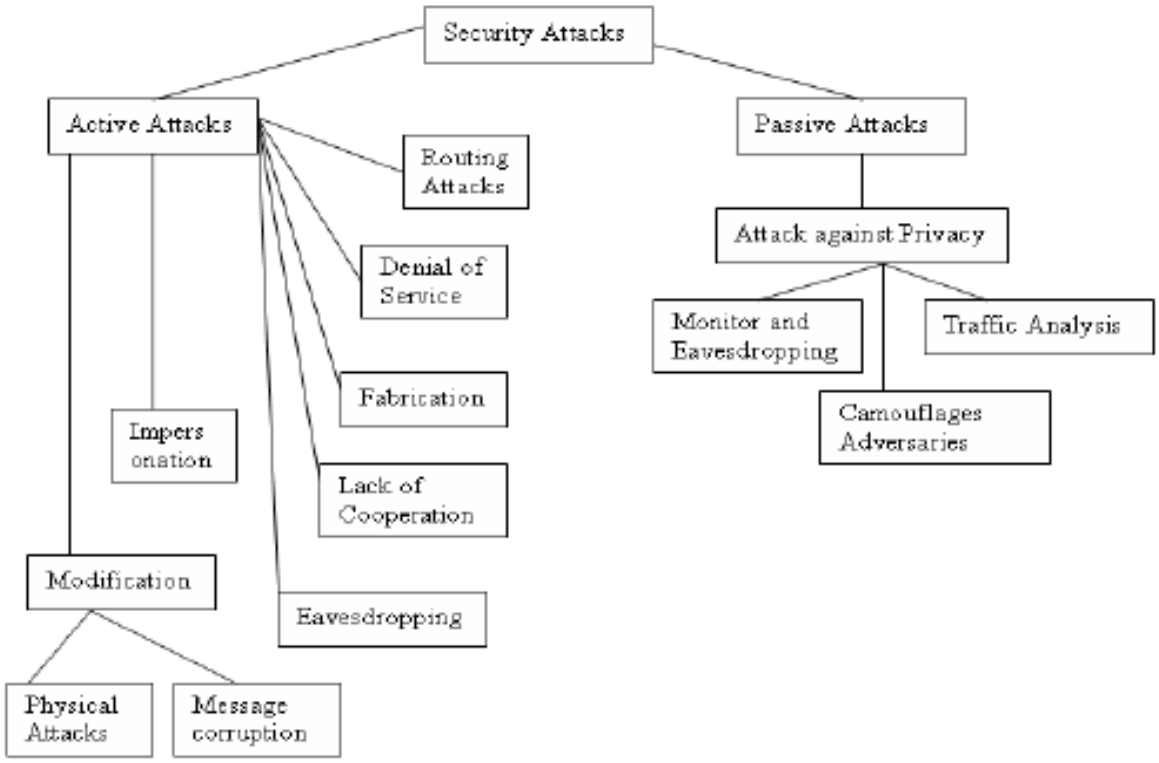

Fig 3: Security issues in Mobile Ad-Hoc Network

Time-varying wireless link characteristics: Wireless channel is liable to a range of broadcast disorders such as path harm, declining, intervention and obstruction. These features resist the series, data rate, and consistency of these cordless transmissions. The range of which these features disturb the transmission that rest on atmospheric situations and flexibility of receiver and transmitter. Even two dissimilar key restraints, Nyquist's and Shannon's theorems that rule over capability to communicate the information at diverse data degrees can be measured.

Broadcast nature of the wireless medium: The broadcast nature of the radio channel, such as transmissions prepared by a device is established by all devices that are in its straight transmission covering area. When a device receives data, no other device in its neighbourhood, apart from the sender, must transfer. A device can acquire access to the mutual medium when its communications cannot disturb any constant session. Meanwhile several devices may resist for medium contemporarily, chance of data-packet crashes is very tall in wireless networks. Even the network is liable to concealed terminal issue and transmits storms. Concealed terminal issue mentions to the smash of data-packets at a receipt device because of immediate transmission of the nodes which are outside the straight communication series of the transmitter, but are inside the communication series of the receiver.

Packet losses due to transmission errors: Ad hoc wireless networks practices very advanced packet damage due to reasons such as extraordinary bit error rate (BER) in the wireless channel, enlarged crashes because of the existence of unseen terminals, occurrence of interventions, position reliant controversy, single directional associations, regular pathway breakages due to device movements, and the integral declining characteristics of the wireless passage.

Mobility-induced route changes: The system topography in ad hoc wireless network is extremely active because of node movement; as a result, a constant meeting undergoes numerous pathway breakages. Such position often results in regular path alterations. So flexibility administration is massive investigation theme in ad hoc networks.

Mobility-induced packet losses: Communication contacts in an ad hoc network are insecure such that consecutively conservative procedures for MANETs over a great damage frequency will suffer from performance deprivation. Though, with large frequency of inaccuracy, it is problematic to supply a data-packet to its target.

Battery constraints: It is due to restricted resources that arrange main limitation on the mobile devices in an ad hoc network. Nodes which are contained in such network have restrictions on the supremacy foundation in order to preserve movability, dimension and capacity of the node. Due to accumulation of power and the processing capacity make the nodes heavy weight and less portable. Consequently only MANET devices have to use this resource.

Routing: In MANETs routing is an important challenge for the performance degradation due to unicasting, multicasting and geocasting demands by the network nodes in contrast to single hope wireless networks. It's because of rapid change in network topology and with different mobility speeds.

Quality of Service: In MANETs quality of service is an important challenge for the differed kind of quality level demands by the network nodes. Its becomes very difficult to fulfil the different levels or priority demands related to quality of service so these network required best control of QoS specially in case of multimedia .

Security: In MANET, security is one the important challenge due to its wireless environment. The data of users from one node to another node must be transferred safely and completely. The least privilege principle can also enhance the security of MANET systems as proposed for organizations. Moreover, there are hybrid models are also available that are offering benefits of two access control models with implementations.

II. PROPOSED SYSTEM

The main objective is to implement advanced mutual bait detection to defend against combined attacks in MANET's, which involves two scheme proactive and reactive defense that is, the system merges the advantage of proactive detections and the superiority of reactive response, in order to reduce the resource wastage. The proactive scheme is used to prevent malicious node, before the communication starts, an initial bait detection is used to make sure that there is no malicious node using the one hop neighbouring node as its bait address to find malicious node if any malicious node presence is marked, reverse tracing technique is triggered once the communication has been started the source node maintains a success ratio and threshold, during data transmission, if the success ratio comes to threshold, a reverse tracing technique is used to find the position of the particular malicious node. Thereby detected and prevented from participating in the communication improving the security. The flowchart for the proposed scheme as shown in Fig 4.

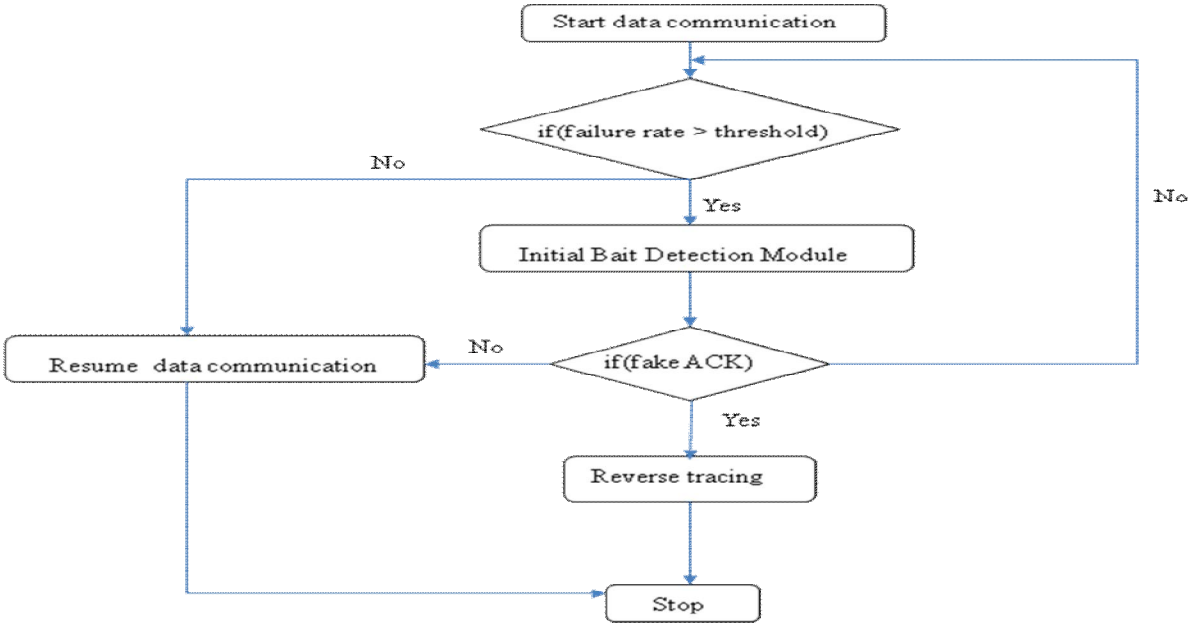

Fig 4: Two-way bait detection approach

Initial Bait Detection: In this module following steps are followed:
The source node uses its one hop neighbouring node as bait address.
Send route request (RREQ) to find bait address node.
ny node other than the bait address node replies then that node is marked as malicious node.
Initial Reverse Tracing: In this module following steps are followed:
Node is marked as malicious in previous module. That particular node's position is been detected in this module using reverse tracing technique.
Which is black listed.
And an alarm packet is broadcasted over the network informing not to include in any communication.
Shifted to reactive defense: In this module following steps are followed:
This mechanism, the malicious node selectively drop the packet which is challenging in identifying the malevolent node.
Hence it maintains success ratio and threshold level, once the success ratio reaches below threshold level the reverse tracing technique is triggered and follows the previous mechanism

III.RESULTS AND DISCUSSION

The following snapshots shows the detection of malicious nodes during file transfer using advanced mutual bait detection approach to defend against combined attacks in MANET's.

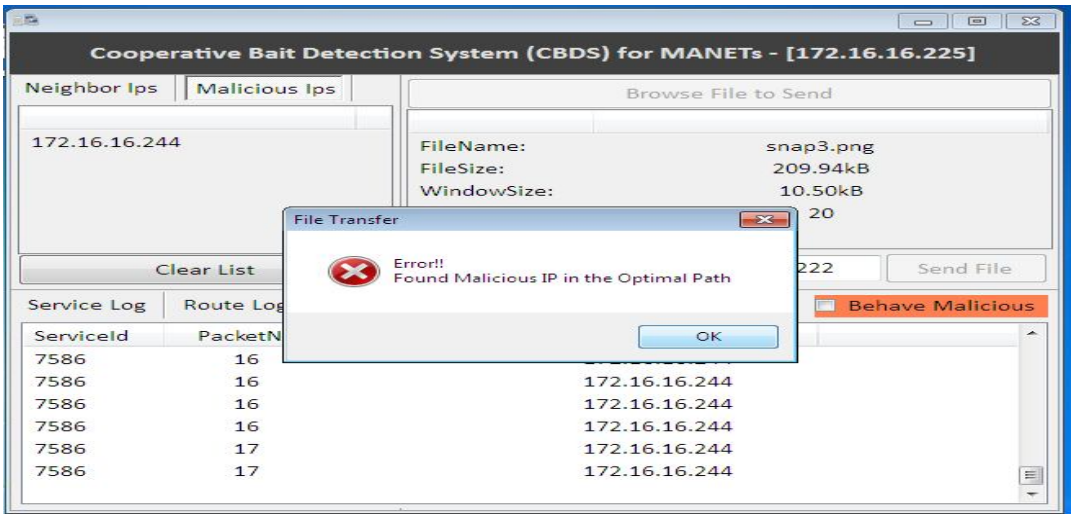

Fig 5: Dialogue box displayed when malicious node is

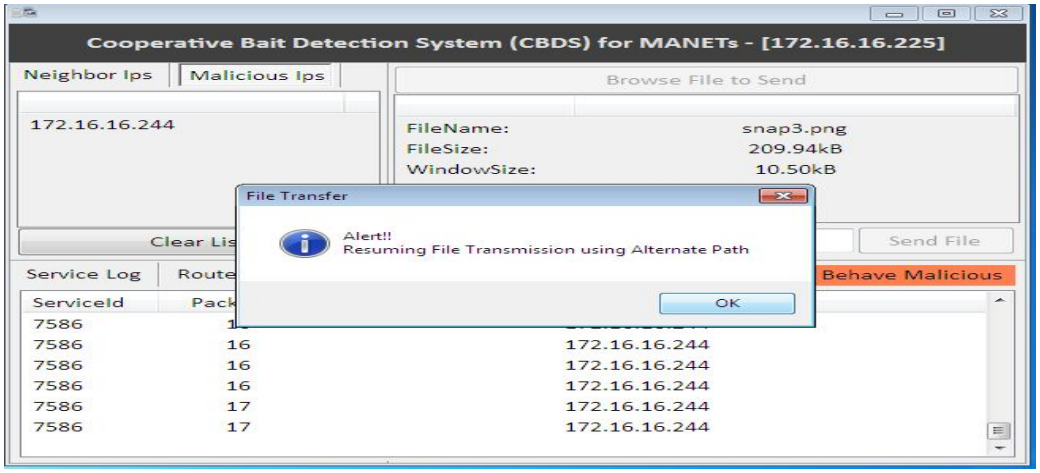

Fig 6: Alert message displayed when transmission is resumed

IV. CONCLUSIONS

Security in MANET is a huge challenge and also research work is at initial levels. Routing protocols are vulnerable towards the collaborative blackhole or grayhole attacks in MANET. Here, advanced mutual bait detection approach uses proactive defense and reactive defense architecture to detect the malicious nodes, which launch the collaborative black hole or gray hole attacks and proposed advanced mutual bait detection approach uses AODV protocol to reduce lower routing overhead named as advanced mutual bait detection using AODV. Advanced mutual bait detection approach using DSR has performed more effectively than DSR protocol and CBDS using AODV perform better in terms of throughput and packet delivery ratio than advanced mutual bait detection using DSR.

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.
[2] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation considerations, Jan. 1999. (Last retrieved March18, 2013). Online].Available:http://www.elook.org/computing/rfc/rfc2501.html
[3] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput.
[4] 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
[5] S. Marti, T. J. Giuli , K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000.
[6] 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
[7] 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, May 2007
[8] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.
[9] 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.