ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

A Cooperative Bait Detection Approach for Detection of Malicious Node in MANET

K. Naveeda[1], B. Saraswathi[2]

PG Student [CS], Dept. of ECE, Pavendar Bharathidasan College of Engg. & Tech., Tiruchirappalli, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, Pavendar Bharathidasan College of Engg. & Tech., Tiruchirappalli, Tamilnadu, India[2]

ABSTRACT: In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malicious nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge. This paper attempts to resolve this issue by designing a Adhoc on demand distance vector routing (AODV)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defence architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the simulation done in the NS-2 simulation and X-graph shows the comparison of previous techniques.

KEYWORDS: AODV, CBDS, grayhole attacks, malicious node, mobile ad hoc network (MANET)

I.INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Many research works have focused on the security of MANETs.

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 blackholeattacks (see Fig. 1.2), 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

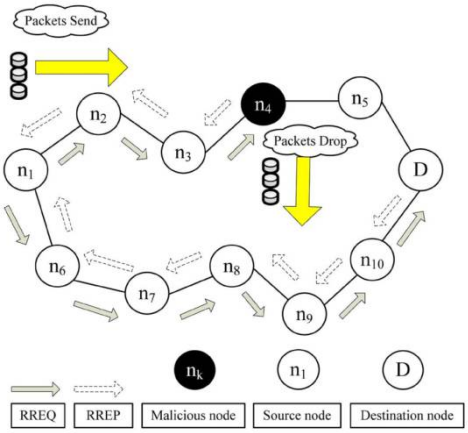

Fig.1 Blackhole Attack

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 WORKS

With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results in the rapid development of the technology. Due to the reason that MANET doesn't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent [11]. TBONE introduce an ad hoe wireless mobile network that employs a hierarchical networking architecture. The network uses high capacity and low capacity nodes. Present a topological synthesis algorithm that selects a subset of high capacity nodes to form. a backbone network. The latter consists of interconnected backbone nodes that intercommunicate across high power links, and also makes use of (airborne, ground and underwater) Unmanned Vehicles (Uvs) [12-13]. [15] A mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Preventing cooperative blackhole attacks in mobile ad hoc networks [6] a solution to identifying and preventing the cooperative black hole attack. Our solution discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. In this paper, via simulation, we evaluate the proposed solution and compare it with other existing solutions in terms of throughput, packet loss percentage, average end-to-end delay and route request overhead. A major advantage of MANET is its wireless nature as can be deployed more rapidly and less expensively than wired networks. Despite its mobility, decentralized control and dynamic topology MANET is vulnerable to wide range of attacks. It is very difficult to detect some attacks when it becomes part of network. Ad hoc on demand distance vector (AODV) is a popular routing protocol but exposed to well known packet dropping attack, where a malicious node intentionally drops packets without forwarding them to destination [7].

The model [8] due to the open structure and scarcely available battery-based energy, node misbehaviours may exist. One such routing misbehaviour is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs [12]. By the implementation of Misbehaviour Report Authentication (MRA) scheme, EAACK is able of detecting malicious nodes despite the existence of false misbehaviour report and compared it against other popular mechanisms in different scenarios during simulation.

In [3], Xue and Nahrstedt proposed a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path (measured in terms of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining "good" routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a AODV-based routing scheme able to detect gray-hole/collaborative blackhole attacks in MANETs.

III. PROPOSED APPROACH

This paper proposes a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs. 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. Our CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage.

However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a blackhole attack. To resolve this issue, the function of message is added to the CBDS to help each node in identifying which nodes are their adjacent nodes within one hop. This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, except that their destination address is the bait address. The CBDS scheme comprises three steps: 1) the initial bait step; 2) the initial reverse tracing step; and 3) the shifted to reactive defense step, i.e., the AODV route discovery start process. The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.

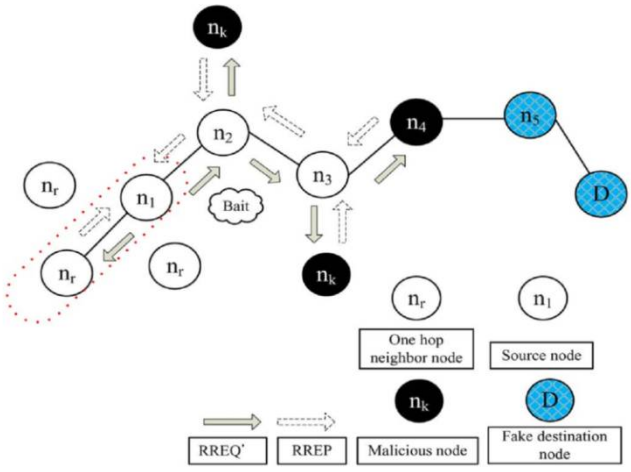

Fig. 2 Random selection of a cooperative bait address

A. Initial Bait Step

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ' that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. The bait phase is activated whenever the bait RREQ is sent prior to seeking the initial routing path.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

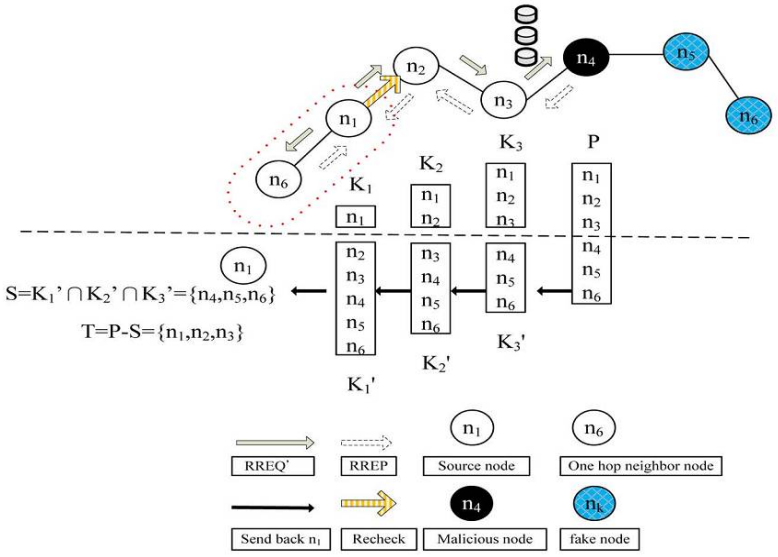

Fig. 3. Reverse tracing program of the CBDS

The follow-up bait phase analysis procedures are as follows. First, if the nr node (Adjacent node) had not launched a blackhole attack, then after the source node had sent out the RREQ', there would be other nodes' reply RREP in addition to that of the nr node. This indicates that the malicious node existed in the reply routing.

Second, if nr was the malicious node of the blackhole attack, then after the source node had sent the RREQ', other nodes (in addition to the nr node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. Fig. 3 Therefore, the reverse tracing program in the next step would be initiated in order to detect this route. If only the nr node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase.

B. Initial Reverse Tracing Step

The reverse tracing program is used to detect the behaviors of malicious nodes through the route reply to the RREQ_ message.

If a malicious node has received the RREQ_, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

Indeed, when a malicious node, for example, nm, replies with a false RREP, an address list P = {n1 . . . nk, nm . . . nr} is recorded in the RREP.

If node nk receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list Kk= {n1, . . .nk}, where Kkrepresents the route information from source node n1 to destination node nk. Then, node nkwill determine the differences between the address list P = {n1 . . . nk . . . nm . . . nr} recorded in the RREP and Kk= {n1 . . . nk}..

$$K'_k = P - K_k = \{n_{k+1}, \ldots n_m, \ldots n_r\} \qquad (1)$$

The set difference operation of P and S is conducted to acquire a temporarily trusted set T, i.e., T = P − S. To confirm that the malicious node is in set S, the source node would send the test packets to this route and would send the recheck message to the second node toward the last node in T.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

$$S = K_1' \cap K_2' \cap K_3' \ldots \cap K_k'. \quad (2)$$

$$T = P - S. \quad (3)$$

C. Shifted to Reactive Defense Phase

After the above initial proactive defence (steps A and B), the DSR route discovery process is activated. When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency.

The CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP.

In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not. As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a grayhole attack would be detected by the CBDS the same way as those launching blackhole attacks are detected.

IV. PERFORMANCE EVALUATION

A. Simulation Parameters

The NS-2 simulation tool is used to study the performance of our CBDS scheme. We employ the IEEE 802.11 MAC with a channel data rate of 11 Mb/s. In our simulation, the CBDS default threshold is set to 90%. All remaining simulation parameters are captured below discussion. The network used for our simulations is depicted in output screenshots; and we randomly select the malicious nodes to perform attacks in the network.

B. Modules

1. Implementation of Wireless Network

In this module, a wireless network is created. All the nodes are configured and randomly deployed in the network area. Fig. 4 shows our network is a wireless network, nodes are assigned with mobility (movement). A routing protocol is implemented in the network. Sender and receiver nodes are randomly selected and the communication is initiated. All the nodes are configured to CBDS and reverse tracking among all the nodes.

2. Performance Analysis

In this module, the performance of the network after CBDS is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters are considered here and X-graphs are plotted for these parameters.

3. Implementation of CBDS *coding scheme*

In this module, To enable all the nodes to get the global AODV, we propose a dynamic threshold algorithm, with an emphasis on calculation the total node packet delivery ration and reverse tracking the node information. The proposed encoding strategy is based on CBDS default threshold coding which has very low complexity. CBDS scheme involves misbehaviour nodes in the MANET

4. Performance analysis

In this module, the performance of the proposed CBDS method is analyzed. Based on the analyzed results Fig. 5 shows the X-graphs are plotted. Throughput and packet delivery ration of the basic parameters considered here and X-graphs are plotted for these parameters. Finally, the results obtained from this module is compared with previous results and comparison X-graphs are plotted.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

SIMULATION PARAMETERS

Parameter	Value
Application Traffic	*10 CBR*
Transmission rate	*10 packets/s*
Packet Size	*512 bytes*
Channel data rate	*10Mbps*
Pause time	*0s*
Simulation time	*10s*
Number of node	*25*
Area	*1200X1200*
Threshold	*Dynamic*

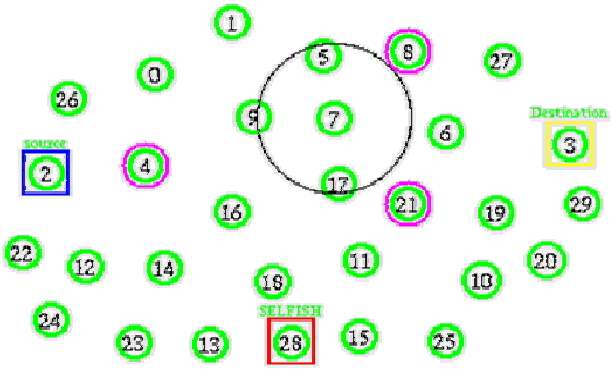

Fig. 4 Output NAM window network deployment

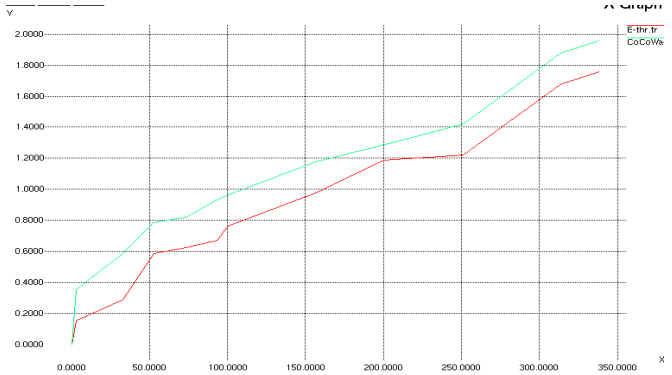

Fig. 5 X-graph of Throughput vs. PDR

V. CONCLUSION & FUTURE WORK

In this paper, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. Reactive and Proactive schemes to design a DSR-based routing scheme able to detect grayhole/collaborative blackhole attacks in MANETs. CBDS scheme merges the proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage. As future work, we intend to 1) In 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

REFERENCES

[1] Baadache A. and Belmehdi A. "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1.,2010
[2] Chang C, Wang Y, and Chao H , "An efficient Mesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239,2007
[3] Corson S and Macker J , RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations".,1999
[4] Deng H, Li W, and Agrawal D , "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10,2002
[5] Johnson D and Maltz D, "Dynamic source routing in ad hoc wireless networks," Mobile Compute., pp. 153–181.
[6] Po-Chun Tsou, Jiann Ming Chang, Han-Chieh Chao and Jiann.-Liang Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun, VITAE.,2011
[7] Rubin I, Behzad A, Zhang R, Luo H, and Caballero E , "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf. vol. 6, pp. 2727–2740,2002
[8] Wang W, Bhargava B, and Lindeman M, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009
[9] Weerasinghe H and Fu H, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.
[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.