Back Pressure Algorithm with CBDS

S.Jotheeshwaran, A.Kumaravel
PG Scholar, Assistant Prof
Paavai Engineering College, Namakkal

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 malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this algorithm, to protect backpressure algorithm based routing and scheduling protocols against various insider threats. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal.

Keywords: *Mobile adhoc network, Routing, DSR, CBDS*

I. INTRODUCTION

Mobile means 'moving' and ad-hoc means 'temporary without any infrastructure'[13]. Therefore, a mobile ad-hoc network is made up of group of mobile nodes, which cooperates to communicate with each other without any fixed central base station [7]. A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network of mobile devices connected by wireless links. MANET is a kind of point to point transmission type and is a group of mobile nodes communicating with each other by wireless [14]. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network [8] [9]. The topology of the network varies rapidly and unpredictable over time because of the mobility of the nodes. Besides, the security of MANET has many defects. These threats make the security of MANET lesser than a cable network and produce many security issues. Because the communication of MANET uses the open medium, attacker can easily overhear message that are transmitted. The design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make MANET vulnerable to diverse types of attacks [11]. One of common attack is Black hole attack that is a malicious node can attract all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination [11]. This is shown in Fig. 1. Black hole attack is a kind of Denial-of-Service attacks and derive Gray hole attack, a variant of black hole that selectively discards and forwards data packets when packets go through it [10]. Cooperative black hole attacks mean several malicious nodes cooperate with each other and work just like a group. This kind of attack results in many detecting methods fail and causes more immense harm to all network [10].

In this paper we propose CBDS which integrates the Proactive and reactive defense architectures, and randomly establishing a cooperation with adjacent node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program [11]. Finally the detected malicious node is listed in the black hole list and notifies the remaining nodes in the network to halt any communication with them. As a result, my proposed scheme can reduce packets loss that can be cause by malicious nodes and have better throughput [1] [2].

II. RELATED WORK

In this section, we use an example to introduce the backpressure algorithm and its vulnerabilities, then formulate the backpressure algorithm, and finally discuss attack models. The backpressure algorithm
[1]–[4] is an optimal routing and scheduling policy that stabilizes packet queues with capability to achieve the maximum throughput. The backpressure algorithm dynamically selects the set of links to activate and flows to transmit on these links depending on queue backlogs and channel rates. In the following, we consider its application to a time-slotted wireless network. Fig. 1 shows an example of how the backpressure algorithm works: nodes A, B, C, and D form a three hop wireless network with two flows. Each node has the same transmission rate and cannot transmit and receive at the same time slot. At a given time slot, the backlog of each node for each flow is illustrated in Fig. 1.

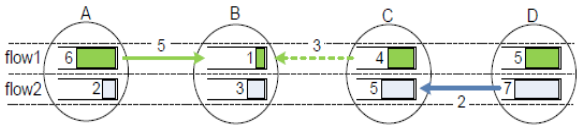

Fig. 1. Example of the Backpressure Algorithm.

The backpressure algorithm works as follows. First, compute the maximum differential queue backlog between each node pair as a link weight; i.e., A→B is 5 for flow 1,

C→B is 3 for flow 1, and D→C is 2 for flow 2, and select these three links. Second, list all non-conflicting link sets, i.e., {A→B for flow 1, D→C for flow 2} and {C→B for flow 1}. Finally, choose the set that maximizes the sum of all link weights, i.e., {A→B for flow 1, D→C for flow 2}. Now suppose node C is malicious and declares that its queue backlog for flow 1 is 100. Then, the maximum differential queue backlog between nodes B and C becomes 99, which makes backpressure scheduling choose only one link {C→B for flow 1}, thereby giving all the transmission opportunity to the malicious node C.

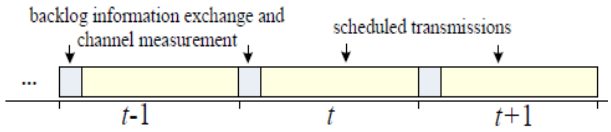

Fig. 2. Information Exchange and Transmission Scheduling in the Backpressure Algorithm.

The backpressure algorithm in (1) is the optimal solution that requires centralized coordination. In practice, a centralized controller (e.g., [10]) will collect information from all nodes then make the scheduling decision. There also exist low-complexity, distributed solutions (e.g., [3], [5]–[7], [6]) with performance close to the optimal solution (1). As our focus is not to solve (1) optimally in a distributed way, but to develop a generic framework that provides security guarantee integrated into the backpressure framework, we choose to integrate security into the optimal formulation (1). In other words, we consider a centralized scenario (e.g., [10]) in which there exists a centralized controller in a multi-hop wireless network. Accordingly, our theoretical results are based on the optimal backpressure scheduling formulation.

To this end, we adopt a generic implementation model for the backpressure algorithm shown in Fig. 2: at the beginning of each time slot, nodes send information to the controller for centralized coordination (e.g., [17]). The information includes queue backlogs for computing the differential queue backlog wi,j (t) in (2) and channel state information based on channel measurements for obtaining the best channel rate ui,j(t) from any node i to node j in (1). Then, scheduled transmissions occur at the rest of the time slot.

Note that our security solution based on the global optimization (1) does not require extra centralized or global information, but introduces new local information. Therefore, it can be readily extended to distributed versions that rely on exchange of local information only.

III. COOPERATIVE BAIT DETECTION SCHEME

This paper proposed a malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes causing black or gray hole attacks and cooperative attacks. It merges the proactive and reactive defense structure, and the source node randomly establishing cooperation with the adjacent node. Using the address of the adjacent node as the destination bait address, it baits malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again, which can achieve the capability of maintenance and immediately reactive response[2][10]. Accordingly, our proposal merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, our mechanism doesn't like the method that just use reactive architecture would suffer black hole attack in initial stage. Although DSR can know the all address of nodes among the route after the source node receives the RREP. Nonetheless, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss. In comparison to DSR, the function of Hello message like AODV was added to help the nodes to identify which nodes are their adjacent nodes within one-hop[10][3]. This function assists in sending the bait address to entice the malicious nodes and utilize the reverse tracing program of CBDS to detect the exact addresses of malicious nodes. In addition, the baiting RREQ packets were created. infrastructure, security challenges have become a major concern to provide secure communication. Secure communication is guaranteed when the key security principles such as authentication, confidentiality and integrity are present [4]. Absence of centralized administration makes MANETs

vulnerable to various types of security attacks [1] [7] and dealing with these is one of the main challenges for the developers [8] [10].

A. *Proposed System Architecture Overview*

This paper attempts to resolve collaborative black-hole attacks issue by designing a AODV routing as DSR-based routing mechanism, which is called **CBDS** (Cooperative Bait Detection Scheme) that integrates the advantages of both proactive and reactive defense architectures [10]. In my approach, the source node stochastically selects an adjacent node with which to establish cooperation, the address of this node is used as bait destination address [10] to deceive malicious nodes to send a RREP reply message. Malicious nodes are therefore detected and prevented against routing operation, using a reverse tracing technique.

B. *Network Design*

In this design, we are mainly dealing with security side, to check my protocol strength; I have to design the attacker and defender nodes. The attacker node able to check the route request and can give the fake reply to the source and attacker can identify the data packet and it will drop. Legitimated nodes can make the cooperation with neighbor and can make the communication, and forwards the data from one to other nodes, and can try to defend from attacker.

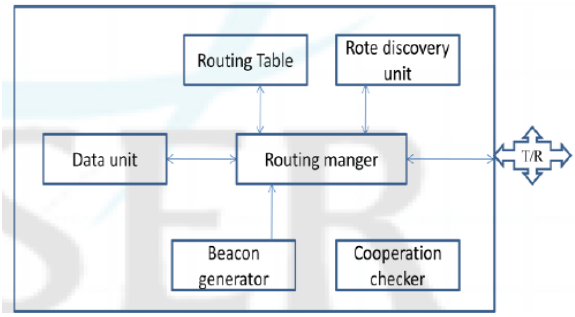

Fig 3: Propose System architecture

C. *Cooperation Checker*

In this module, we have used the timer to keep the time expire and intimates to generate the periodic packet. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is to store the neighbor information into table when it receives the beacon packet from the neighbor. If the time is got expire the neighbor node info will be deleted from the table

D. *Route Discovery*

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In this scheme, we are also going to use same method with different style, such as creating the fake route request. The source will generate fake request with destination address as cooperating neighbor. Source already knows the information, for Freq no reply. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism

E. *Route Maintenance*

In this module, if route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. With secure route discovery model

F. *Expected Output*

We will show the output in two ways:

- Nam (Network animator) window

In this window, I can show the animation of packet transfer, packet drops and mobility.

G. *Analysis*

- Trace file:

Stores the information of network events (ex., packet sent, received, dropped at the time, node moved from which place to which place…)

- Xgraph

In this window, I can show the result like as packet delivery radio, packet loss, and delay as graph

Others include Mamatha et al.[8] who present a security mechanism capable of identifying and isolating nodes that carry out different types of network layer attacks. Detection is known based on the percentage of number of packets dropped. That particular node dropping packets in excess of the threshold is malicious or misbehaving node. According to Obaidat et al.[8] expanded a recently proposed AODV based on Highly Secured Approach against attacks on MANETs to protect routes in the route selection phase. According to Arya et al.[8] identifies diverse ways for detecting indiscipline or malicious nodes in a MANET. According to Raju et al.[6][8] present an authentication scheme for Mobile Ad Hoc Networks that is designed to combat attacks such as injecting harmful packets, alter packets, drop packets etc. In the scheme, every packet is authenticated at every node. According to Sikarwar et al.[13] propose a framework for protecting communication in ad hoc network using dynamic key cryptography and its comparable study with intrusion detection system. According to Vishnu et al.[7] propose a unique protocol for identifying and removal of network black and gray hole nodes with the help of a backbone network of trusted nodes for restricted IP (RIP) address. According to Sahadevaiah et al.[7] propose a security protocol named cryptographic hybrid key management for secure routing in MANETs, to provide self-organized behavior by distributing the public keys and self-signed

certificates among all the nodes to form a network with an initial trust phase. According to Nabet et al. [7] propose an efficient and effective secure routing protocol to ensure routing security in ad hoc networks (ASRP). According to Marti et al. [7] presents a method in which contains Watchdog and Pathrater for detecting black hole. The Watchdog employs neighbor nodes to overhear and identify malicious node. Watchdog depends on overhearing the packets whether be discarded deliberately to identify the malicious node.

IV. SIMULATION RESULTS

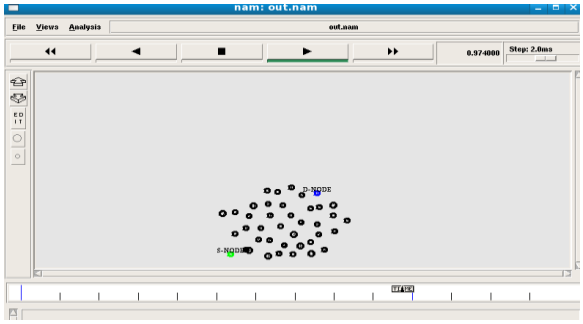

Fig. 4: Source to Destination Transmission

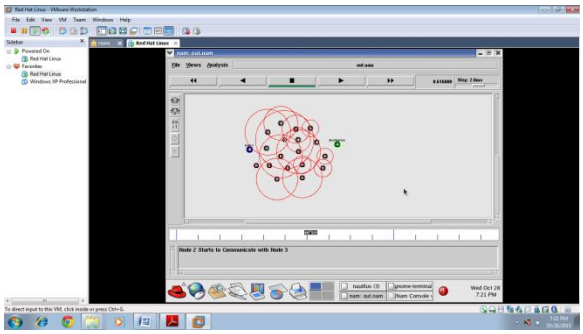

Fig. 5: Path Analyzing to Transfer Data

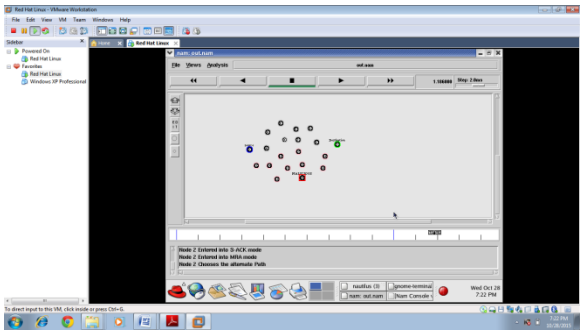

Fig. 6: Choosing the Alternative Path

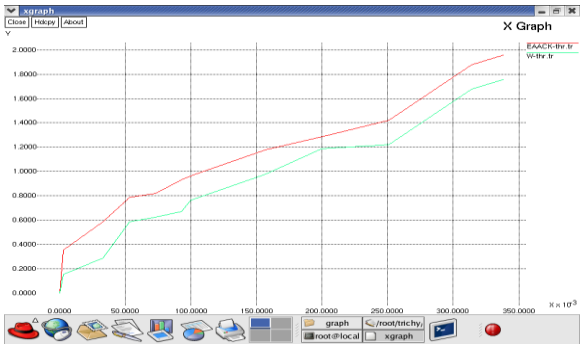

Fig. 7: Throughput Ratio (Existing vs Proposed)

V. CONCLUSION

In an attempt to find a lasting solution to the security challenges in MANETs, various researchers have proposed different solutions for various security issues in MANETs. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for MANETs is still a major concern. My approach is based on using cooperative bait detection scheme to detect and prevent malicious nodes attack in MANETs. My proposal merges the advantage of proactive detection that can avoid just using reactive architecture that would suffer malicious node attack in initial stage and the superiority of reactive response that can reduce the waste of resource.

REFERENCES

[1] A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journal of Computer Science and Information Security," Vol. 7, No. 1, 2010.

[2] V. K and A. J PAUL, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks," 2010 International Journal of Computer Applications, Vol. 1, No.22, 2010

[3] Scalable Network Technologies (SNT). QualNet.http://www.qualnet.com

[4] Durgesh Kumar Mishra Mahakal Singh Chandel, Rashid Sheikh. "Security Issues in MANET: A Review".

[5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China.Research on MANET Security Architecture design.

[6] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," IEEE Trans. Automatic Control, vol. 37, pp. 1936–1948, Dec. 1992.

[7] M. Alresaini, M. Sathiamoorthy, B. Krishnamachari, and M. J. Neely, "Backpressure with adaptive redundancy (BWAR)," in Proc. of IEEE INFOCOM, 2012.

[8] A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practical differential backlog congestion control for wireless networks," in Proc. of IEEE INFOCOM, 2009.

[9] H. Seferoglu and E. Modiano, "Diff-Max: Separation of routing and scheduling in backpressure-based wireless networks," in Proc. of IEEE INFOCOM, 2013.

[10] L. Huang, S. Moeller, M. J. Neely, and B. Krishnamachari, "LIFO-backpressure achieves near optimal utility-delay tradeoff," ACM/IEEE Trans. Networking, pp. 831–844, June 2013.