ReverseRoute: An Application-layer Scheme for Detecting Blackholes in MANET using Mobile Agents

Amar Taggu, Abhishek Mungoli
NERIST, Nirjuli
Arunachal Pradesh, India
ataggu@gmail.com, mungoliabhishek81@gmail.com

Ani Taggu
RGU, Doimukh
Arunachal Pradesh, India
anitaggu@gmail.com

***Abstract*—Mobile Ad-Hoc Networks (MANETs) are prone to many security attacks. One such attack is the blackhole attack. This work proposes a simple and effective application layer based intrusion detection scheme in a MANET to detect blackholes. The proposed algorithm utilizes mobile agents(MA) and $wtracert$(modified version of Traceroute for MANET) to detect multiple black holes in a DSR protocol based MANET. Use of MAs ensure that no modifications need to be carried out in the underlying routing algorithms or other lower layers. Simulation results show successful detection of single and multiple blackhole nodes, using the proposed detection mechanism, across varying mobility speeds of the nodes.**

I. Introduction

A MANET is a decentralized, self-configuring and infrastructure-less wireless network of mobile devices. In MANET, each node can independently move in any direction and acts as a router helping in forwarding the network traffic. However, since there is no centralized control, MANET is susceptible to many MANET-specific attacks and hence, detection and mitigation of such attacks is crucial for successful functioning of MANET. Standard techniques like Intrusion Detection Systems(IDS) no longer applies to MANETs due to their infrastructure-less setup.

A blackhole refers to a malicious node which takes advantage of vulnerability in the routing protocols and causes huge drop in throughput and packet delivery ratio in a network. The malicious node informs other users in the network through route reply that it has a valid shorter route to destination node even though the route may be spurious. Once the victim node starts sending packets through the route containing the blackhole node, those packets are dropped. Malicious node responds to route requests normally but when packets are sent to it for transmission, it drops them. Thus it is a kind of Denial-of-Service (DoS) attack. Since black hole behaves normally to route requests, it's detection is hard. In this paper, an application-layer scheme ReverseRoute Detection is being proposed, which works primarily in the application layer. It uses mobile agents which work in the Application Layer, and hence, requires no lower-layer modifications. $wtracert$ application, which is a modification of standard Traceroute application, has been developed especially for MANET. It can be used to detect broken links in the network and also to find a reverse route from a destination node to the source node, if such a route exists, which is explained later in the paper. To the best of our knowledge, this is the first time that MAs have been used to detect blackholes in a MANET. In addition, use of a separate application-layer entity (MAs) ensures that no changes need to be made in the underlying routing protocols, which itself is non-trivial and impractical in a real-world scenario.

The rest of this paper is organized as follows: Section II consists of short review of related works. Section III elaborates on the Blackhole Attack. ReverseRoute is discussed thoroughly in Section IV. Section V presents the simulation results and analysis. Section VI indicates the possible directions for future work and also, concludes the paper.

II. Related Work

Taggu and Taggu [1] proposed TraceGray, a MA-based grayhole detection in MANET, which has influenced the current work to a large extent. The use of MA which uses a simple mechanism of two-steps-forward and one-step-backwards is a novel way of using MA for intrusion detection in MANETs. Taggu and Taggu [2] also proposed $wtracert$ which is a modified version of Traceroute application developed especially for MANET. $wtracert$ is much faster and more efficient for Wireless Ad-hoc network than the original Traceroute. The same is used in the current work for Blackhole attack detection. Kachirski and Guha [3] proposed a mobile agent based distributed multi-sensor IDS. Zhang et al [4] proposed a distributive and cooperative IDS architecture for MANET such that every node participates in the detection process by locally running an IDS agent and also participate in global

978-1-5386-7573-1/18/$31.00 ©2018 IEEE

intrusion detection. Many proposed schemes detect malicious nodes by enhancing the underlying routing algorithms. Marti et al [5] proposed two extensions to the DSR algorithm: the watchdog and the pathrater, that rely on the promiscuous mode in DSR algorithm to identify misbehaving nodes. In [6] and [7], Sen et al proposed algorithms in which every node monitor its neighbours to identify any abnormal activity and invokes a distributed algorithm to verify if a neighbour is malicious. In [8], Wei et al propose a solution against the gray hole attack using two related algorithms: a key management algorithm based on gossip protocol and the detection algorithm based on aggregate signatures. In [9], D. Djenouri and N.Badache propose a protocol wherein a component resides in network layer while the other component works in the MAC layer. Onashoga et al [10] have reviewed many of the existing current MA-IDSs. More recently, Mohamed A. Abdelshafy et al [11] proposed a Self-Protocol-Trustiness concept which clarifies that the detection of a malicious intruder is accomplished by complying with the normal protocol behaviour and lures the malicious node to give an implicit avowal of its malicious behaviour. In [12], Elbasher Elmahdi et al uses encryption to detect blackholes in MANETs running AOMDV protocol. The basic idea of this scheme is to split a message into many parts before the message is transmitted. Each part is then encrypted using homomorphic encryption method. The receiver decrypts the message send in parts. The proposed method claims to mitigate the blackhole attack.

III. Blackhole Attack

Intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR, when a node requires a route towards the destination. The node sends a RREQ and an intruder advertises itself as having a fresh and possibly, shorter route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The intruder, once chosen as an intermediate node, drops the packets instead of forwarding or processing them, creating a blackhole in the network. The way the intruder initiates the blackhole attack and captures the routes, may vary in different routing protocols. For example, in AODV, the destination sequence number (dest_seq) is used to represent the freshness of the route. A higher value of dest_seq means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new dest_seq number larger than the current dest_seq number. In this way, the intruder becomes part of the route to that destination. A blackhole attack is one of the most devastating attacks in MANETs. It is also one of the most difficult attacks to detect due to the nature of the attack wherein all the packets are dropped.

IV. ReverseRoute: The Proposed Blackhole Attack Detection Mechanism

ReverseRoute Detection implements intrusion detection using mobile agents primarily because of the facility of code migration provided by mobile agents. Some custom enhancements are implemented over a typical MA design as described below. The proposed scheme requires only the next hop information and does not rely on any kind of promiscuous monitoring. ReverseRoute Detection mechanism can detect multiple black holes in a MANET. The proposed scheme succeeds in scenarios where a traceroute-like application fails. Use of $wtracert$ greatly improves the performance of the detection mechanism since the MAs are started only from the last working node in the route, instead of the original source node (sender).

A. Mobile Agents

Mobile agents(MA) are software entities that can physically travel across a network, and perform tasks on machines that provide agent hosting capability. This allows processes to migrate from computer to computer, or processes to split into multiple instances that execute on different machines, and to return to their point of origin, which is called the home context. Migration of MA essentially implies that some code with required data is transferred to another node for remote execution. In the current implementation, each mobile agent has been enhanced with a timer. This timer is currently a function of MA code size + MA data size where the values of MA code size and MA data size are shown in Table I. The basic premise in assigning the timeout period is based on the observation that during change of context of a MA, the size of the mobile code and data required for remote execution determines how large the timeout interval should be.

B. Pre-requisites

ReverseRoute requires that the next hop information be available to a node. With DSR routing, the proposed scheme uses route cache information to obtain the next hop information. Although the entire source route is available for a destination in the route cache, only the first hop node is used to avoid false positives. Furthermore, it is assumed that the intrusion detection process will start after a node suspects some abnormal activity, like extremely high packet dropping in the network. Many mobile agents can be started by the nodes at the same time or at different times, as required.

C. Blackhole Detection Algorithm

A node that suspects abnormal activity runs $wtracert$ to trace the current path upto the destination node to check the correctness of the whole route as shown in Fig. 1. $wtracert$ gives a clear picture of the current route till the last working node. If the entire route till the destination node is traced successfully using $wtracert$, then it means the route is up and destination is ready to receive the packets. However, if $wtracert$ fails to trace the complete route upto the destination, then it can either mean that

1. The route is broken because of which the $wtracert$ was unsuccessful in tracing the complete route, OR,
2. One of the nodes is a blackhole node and hence, it is dropping all packets including the ICMP packets (used in $wtracert$)

In either case, ReverseRoute is initiated to come to a conclusion. The algorithm is given below.

Algorithm ReverseRoute Algorithm

```
1: From the last working node as returned by running $wtracert$, a MA is started to go to the next one-hop node (Fig. 2)
2: Once the MA reaches the next hop node successfully, it attempts to go back to the previous node
3: if MA can reverse back to its original sender node (the previous node) then
4:     The current sender node of the MA is a blackhole (Fig. 3)
5: else
6:     Route Broken (Fig. 4)
7: end if
```

Step 3 of the above algorithm is explained further here. A blackhole node is usually configured to drop routing packets. When a MA, which is not a routing packet, is received at the blackhole node, the MA will initiate its reverse routing from the blackhole node to the previous node. Since the route is not broken (as the MA just reached the blackhole node), the MA will be able to go back to to previous node. Thus, the current node will be labelled as a blackhole.

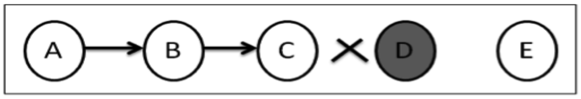

Fig. 1. Working of $wtracert$

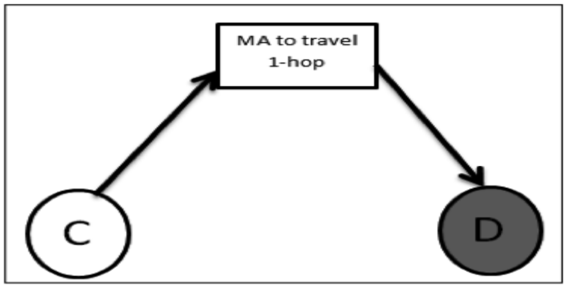

Fig. 2. Node C initiates MA to travel 1-hop distance to Node D

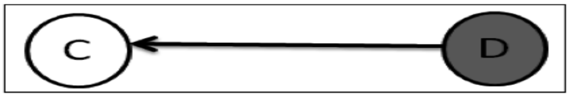

Fig. 3. MA attempts reverse routing from Node D(Blackhole)

V. Simulation and Results

ReverseRoute has been implemented in the NS-2 simulator with Mobile Agent implementation modified according to our requirements. Two metrics used in analysing the results are:

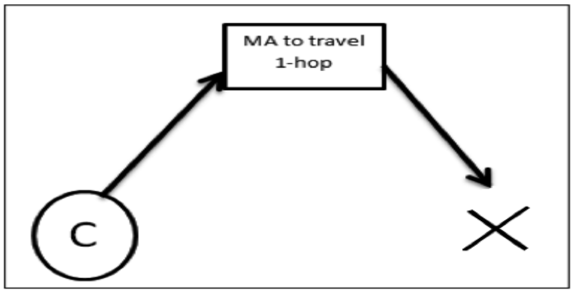

Fig. 4. Broken route

TABLE I
Simulation Environment

Parameter	Value
Simulator	NS-2 (2.35)
Simulation Area	1000x1000 sqm
Simulation Duration	10000 seconds
Number of mobile nodes	100
Tranmission Range	250 m
Maximum Speed	20 m/s
Tranmission Range	250 m
Traffic Type	CBR
Data Payload	250 bytes/packet
Packet Rate	40 packets/sec
Mobile Agent Code Size	100 bytes
Mobile Agent Data Size	5000 bytes
Tranmission Range	250 m
Maximum number of Blackholes	20%

- Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.
- Throughput: The number of data bits delivered to the application layer of destination node in unit time measured in bps.

In normal network without any blackholes, PDR and throughput are very high. Fig. 5 and Fig. 6 respectively show that PDR and throughput decreases abruptly in the presence of blackhole node. With increase in the number of blackhole nodes, PDR and Throughput shows further drop. This is as expected since the attack is targeted specifically at dropping packets at the blackhole. More malicious nodes result in higher packet drop. Fig. 7 shows how the detection time varies with respect to increasing number of blackhole nodes across varying mobility speeds. Detection time is the time to detect the blackhole node in the network. Detection time is improved to great extent by using $wtracert$ instead of standard Traceroute application. Total detection time taken by ReverseRoute detection mechanism is the sum of time taken by $wtracert$ plus MA to travel 1-hop distance and perform its task. As expected, detection time increases with increase in the number of nodes in the network and increase in mobility of nodes as shown.

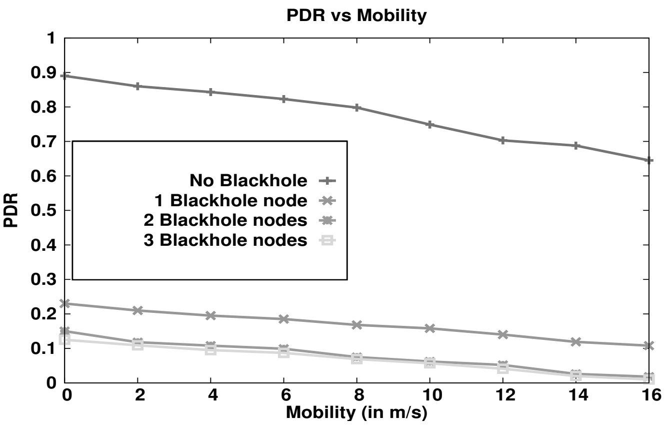

Fig. 5. PDR vs Mobility

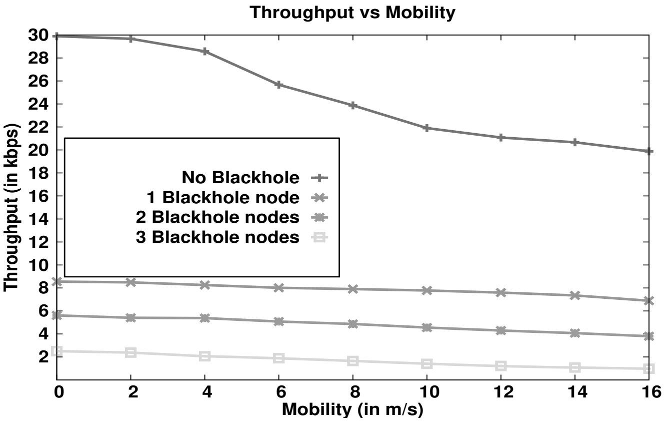

Fig. 6. Throughput vs Mobility

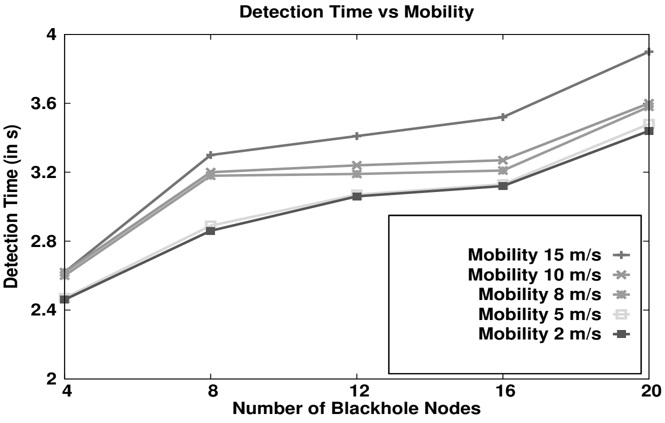

Fig. 7. Detection Time vs Number of Blackhole Nodes

VI. Conclusion and Future Work

To make the process of intrusion detection more accurate and faster, $wtracert$ is run prior to detecting the presence of blackholes in the network. Next, ReverseRoute detection mechanism is utilised to detect blackholes in the network, if any. Use of light-weight mobile agents which are Application-layer entities is an idea which can used in detecting other attacks in MANETs. Since no underlying lower layer protocols need to be modified, the proposed mechanism could be incorporated as practical security add-on in real-world implementation. The simulation results show that ReverseRoute can detect multiple blackholes in the network successfully across varying mobility speeds and the ingenious use of $wtracert$ prior to running the ReverseRoute algorithm has significantly improved the detection time of malicious nodes in the network.

ReverseRoute may be used to detect other attacks in MANETs, in particular and any wireless ad-hoc networks, in general. Owing to the use of light-weight application-layer mobile agents, the usage scenarios of the proposed mechanism are many, especially in the area of security in networks.

References

[1] A. Taggu and A. Taggu, ”TraceGray: An application-layer scheme for intrusion detection in MANET using mobile agents,” 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011), Bangalore, 2011, pp. 1-4.

[2] A. Taggu and A. Taggu, ”Wtracert: An optimal timer based traceroute implementation for wireless networks,” 2012 IFIP Wireless Days, Dublin, 2012, pp. 1-3.

[3] O. Kachirski and R. Guha, ”Effective intrusion detection using multiple sensors in wireless ad hoc networks,” 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the, Big Island, HI, USA, 2003, pp. 8 pp.-.

[4] Yongguang Zhang, Wenke Lee, and Yi-An Huang. 2003. Intrusion detection techniques for mobile wireless networks. Wirel. Netw. 9, 5 (September 2003), 545-556.

[5] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom ’00). ACM, New York, NY, USA, 255-265.

[6] J. Sen, M. Girish Chandra, P. Balamuralidhar, S. G. Harihara and H. Reddy, ”A distributed protocol for detection of packet dropping attack in mobile ad hoc networks,” 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, 2007, pp. 75-80.

[7] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy and P. Balamuralidhar, ”A mechanism for detection of gray hole attack in mobile Ad Hoc networks,” 2007 6th International Conference on Information, Communications and Signal Processing, Singapore, 2007, pp. 1-5

[8] C. Wei, L. Xiang, B. Yuebin and G. Xiaopeng, ”A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks,” 2007 Second International Conference on Communications and Networking in China, Shanghai, 2007, pp. 366-370.

[9] Djenouri D., Badache N. (2006) Cross-Layer Approach to Detect Data Packet Droppers in Mobile Ad-Hoc Networks. In: de Meer H., Sterbenz J.P.G. (eds) Self-Organizing Systems. EuroNGI 2006, IWSOS 2006. Lecture Notes in Computer Science, vol 4124. Springer, Berlin, Heidelberg

[10] Saidat Adebukola Onashoga, Adebayo D. Akinde, Adesina Simon Sodiya, “A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems,” Informing Science Institute, Volume 6 2009

[11] M. A. Abdelshafy and P. J. B. King, ”Resisting blackhole attacks on MANETs,” 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2016, pp. 1048-1053.

[12] E. Elmahdi, S. Yoo and K. Sharshembiev, ”Securing data forwarding against blackhole attacks in mobile ad hoc networks,” 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2018, pp. 463-467.