ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Cooperative Bait Detection Approach with Dynamic Source Routing in VANET

Prashant Mahadev Kadam,Vanita Raut

Student, Dept. of CS, G.H Raisoni College of Engineering and Technology, Wagholi, Savitribai Phule Pune University, Pune, India

Professor, Dept. of CS, G.H Raisoni College of Engineering and Technology, Wagholi, Savitribai Phule Pune University, Pune, India

ABSTRACT: Wireless networks are computer networks that are not connected by cables of any kind. The use of wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Wireless networks are susceptible to many attacks. One such specific attack is a blackhole attack in which malicious node falsely claiming it as having the fresh and shortest path to the destination. 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. Proposed system helps us in defending against the blackhole attack without any requirement of hardware and special detection node. In this context, preventing or detecting malicious nodes launching grayhole or collaborative blackhole in challenge. This project attempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defense architectures. Our CBDS system 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 CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

KEYWORDS: Cooperative bait detection scheme (CBDS), dynamic source routing (DSR), Twice Acknowlegement (2 Ack), grayhole attacks, malicious node, mobile ad hoc network (VANET).

I.INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (VANETs), 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. In a VANET, 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. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Many research works have focused on the security of VANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

II.RELATED WORK

1. DEFENDING AGAINST ATTACKS IN VANETS USING COOPERATIVE BAIT DETECTION APPROACH

From This Paper We Refer-

In this approach, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in VANETs under gray/collaborative blackhole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

2. PROTECTING AGAINST ALLIANCE ATTACKS BY MALICIOUS NODES IN VANETS USING CBDS TECHNIQUE WITH ORIGINATING MESSAGE

From this paper we Refer-

Cooperative Bait Detection Scheme With Originating Message is used to reduce the packet loss and the delay and to increase the overall network throughput using the destination check route information

3. COOPERATIVE BAIT DETECTION SCHEME (CBDS) TO AVOID THE COLLABORATIVE ATTACKS OF NODES IN VANET

From This Paper We Refer-

In an attempt to find a lasting solution to the security challenges in VANETs, various researchers have proposed different solutions for various security issues in VANETs. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for VANETs is still a major concern. My approach is based on using cooperative bait detection scheme to detect and prevent malicious nodes attack in VANETs.

4. IMPLEMENTING VANET SECURITY USING CBDS FOR COMBATING SLEEP DEPRIVATION & DOS ATTACK

From This Paper We Refer-

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application

5. A REVIEW ON ROUTING PROTOCOLS IN VANET

From This Paper We Refer-

Vehicular Ad hoc Networks (VANETs) provide a promising approach for an Intelligent Information Transportation System. Several Routing protocols are used in VANETs for Communication in Vehicles to Vehicles (V2V) and Vehicles to Infrastructure (V2I) networks. These routing protocols for VANETs are classified as unicast, broadcast, and multicast.

Based on this strategy VANET routing protocols are comparing using following parameters namely route discovery, forwarding strategy, no of transmission, etc.

III.PROPOSED SYSTEM MECHANISM

In this paper, a mechanism called "cooperative bait detection scheme" (CBDS) is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defence architectures to achieve the aforementioned goal.

IV.SCOPE OF RESEARCH

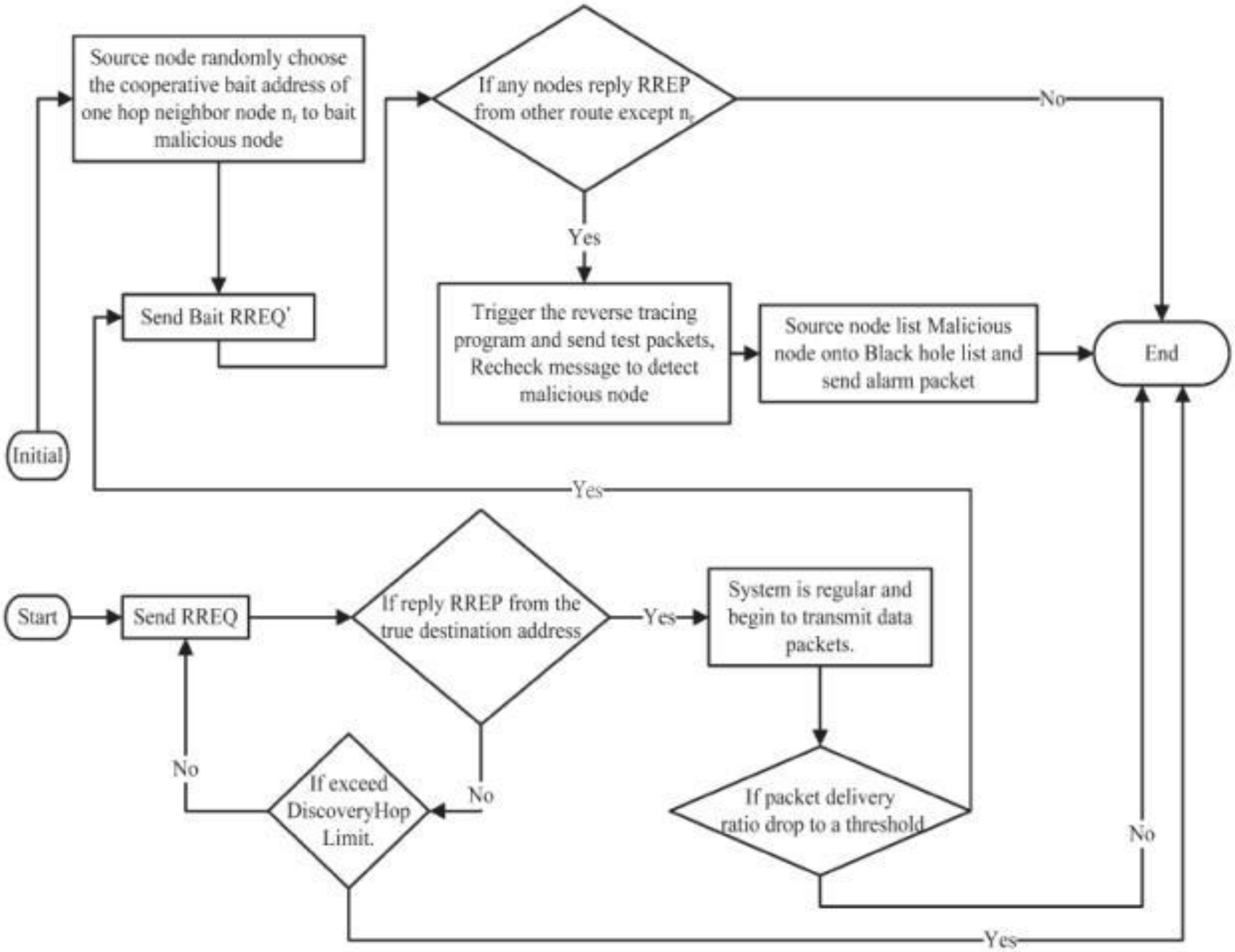
- In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

- 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.

V.WORKING MODULES

1. Network Model.
2. Initial Bait.
3. Initial Reverse Tracing.
4. Shifted to Reactive Defense Phase.
5. Security Module.

VI.SYSTEM ARCHITECTURE


Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
If any nodes reply RREP from other route except n_r
No
Yes
Send Bait RREQ'
Trigger the reverse tracing program and send test packets, Recheck message to detect malicious node
Source node list Malicious node onto Black hole list and send alarm packet
End
Initial
Yes
Start
Send RREQ
If reply RREP from the true destination address
Yes
System is regular and begin to transmit data packets.
No
If exceed DiscoveryHop Limit.
No
If packet delivery ratio drop to a threshold
No
Yes

VII.CONCLUSION

In an attempt to find a lasting solution to the security challenges in VANETs, various researchers have proposed different solutions for various security issues in VANETs. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for VANETs is still a major concern. My approach is based on using cooperative bait detection scheme to detect and prevent malicious nodes attack in VANETs. 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) D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” Mobile Comput., pp. 153–181, 1996.
2) 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

3) 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.

4) M. AhmerUsmani"Defending Against Attacks in VANETs using Cooperative Bait Detection Approach"International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2015.

5) R.Arun, Mr.M.SureshAnand "PROTECTING AGAINST ALLIANCE ATTACKS BY MALICIOUS NODES IN VANETS USING CBDS TECHNIQUE WITH ORIGINATING MESSAGE" 2015 IJIRT | Volume 1 Issue 12 | ISSN: 2349-6002

6) AkinlemiOlushola "Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in VANET" International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

7) NavdeepKaur "Implementing VANET Security using CBDS for Combating Sleep Deprivation & DOS Attack" "International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends" 16(1): 6- 12 (2014)

DOI: 10.15680/IJIRCCE.2015. 0312132