ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

AN EFFICIENT APPROACH FOR DETECTING MALEVOLENT NODES IN MANETs USING COOPERATIVE BAIT DETECTION SCHEME

Priya.C,
PG Student,
Priyadarshini Engineering College, Vaniiyambadi-635751,
priyacnov15@gmail.com
Santhosh Kumar.C,
Associate Professor,
Priyadarshini Engineering College, Vaniiyambadi-635751,
sanscsk@gmail.com

Abstract

A primary constraint among nodes should be collaborate with each other in Mobile adhoc networks (MANETs). In the presence of malevolent nodes, it leads to serious security concerns and such nodes may disrupt the routing process. In our proposed system we discussed about to resolve the issue by designing a dynamic source routing (DSR)-based on routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that integrates the advantages of proactive and reactive defense architectures. Our CBDS methods implements a reverse tracing technique to help in achieving the stated goal. Cooperative bait detection scheme(CBDS), which aims at detecting and preventing the malicious nodes launching gray hole/collaborative black hole attacks in MANETs.

Keywords: cooperative bait detection scheme (CBDS), collaborative black hole attacks, dynamic source routing, gray hole attacks, malicious nodes, Mobile adhoc Networks(MANETs).

Introduction

Mobile computing is very increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the internet irrespective of the physical location of the node. Mobile computing offers many benefits for organizations that choose to integrate the technology into their fixed organizational information system. Ranging from wireless laptops to cellular phones and Wi-Fi/Bluetooth enabled PDA's to wireless sensor networks, mobile computing has become ubiquitous in its impact on our daily lives. It is a versatile and potentially strategic technology that improves information quality and accessibility, increases operational

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

efficiency, and enhances management effectiveness. The goal of this paper is to point out some of the limitations, characteristics, applications and issues of mobile computing.

Mobile computing is an human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Mobile computing is the ability to use computing capability without any pre-defined location and connection to a network to publish and subscribe to information.

Mobile computing is a generic term describing ability to use the technology that wirelessly connect to and use centrally located information and application software through the application of small, portable, and wireless computing and communication devices.

The term "Mobile computing" is used to describe the use of computing devices, which usually interact in some fashion with a central information system which away from the normal, fixed workplace. Mobile computing technology enables the mobile worker to create, access, process, store and communicate information without being any constrained to a single location. By extending the reach of an organization's fixed information system, mobile computing enables interaction with organizational personnel that were previously disconnected. Mobile computing is the discipline for creating an information management platform, where it is free from spatial and temporal constraints. The freedom from these constraints allows users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform being constrained from a single location. To facilitate the data management activities, users can carry Personal Digital Assistant (**PDA**), laptop, cell phones, etc. At present the current technology only provides limited transaction processing capabilities but soon such facilities will be available on all mobile devices such as cell phones, laptops, palmtops, etc. This discipline allows us to define a connectivity mode, which we refer to as "Mobile Connectivity".

Mobile connectivity: The mobile connectivity between the two nodes exists if they are continuously connected through wireless channel, and it can utilize the channel without being subjected to spatial and temporal constraints.

Technologies Available: There are many communications technologies available today that enable mobile computers to communicate. The most common of these technologies are: (a) Wireless Local Area Networks (WLANs) (b) Satellite (c) Cellular Digital Packet Data (CDPD) (d) Personal Communications Systems (PCS) (e) Global System for Mobile communications (GSM) (f) RAM and ARDIS data networks (g) Specialized Mobile Radio (SMR) service (h) one and two-way paging (i)

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

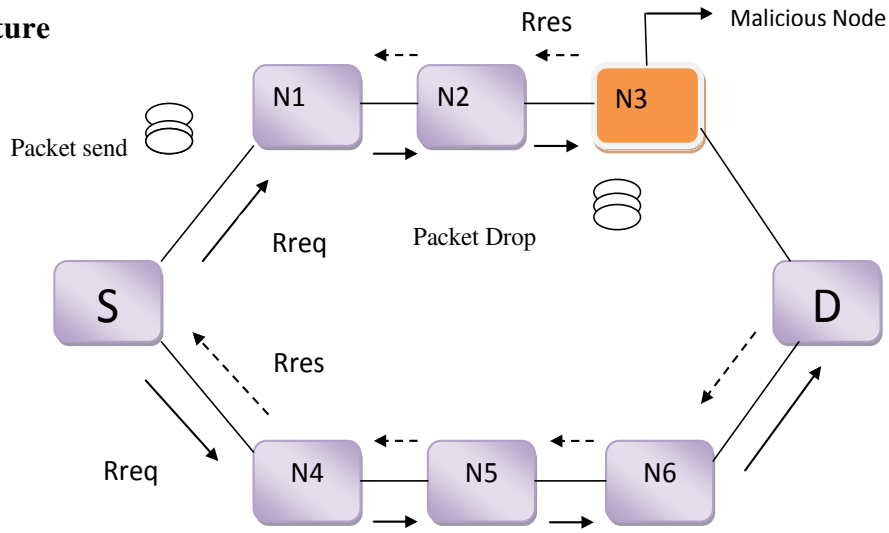
Vol. 2, Special Issue 10, March 2016

plain old telephone system (POTS) (j) Internet (k) infra-red (l) docking (serial, parallel, LAN) and (m) disk swapping. These diverse communications technologies make available to a continuum of connectivity that provides an communications capabilities ranging from manual assisted batch transfers to the high-speed continuous communication.

Related work

Dynamic Source Routing (DSR) is an routing protocol for wireless mesh networks. It is similar to AODV protocol in that it forms a route on-demand when a transmitting node requests one. It uses source routing instead of relying on the routing table at each intermediate device. In the Section[1][3]Dynamic source routing protocol (DSR) is an on-demand protocol designed to a restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The approach of this protocol is during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received. Black hole attacks drop all data packets & cheat the previous node. Gray hole attack drop part of the data & cheat the previous node. As soon as it receive the packet from neighbor the attacker drop the packet it shows in the section [7][8]. It is a type of active attack and in some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior . Due to this behavior it is very difficult for the network to figure out such kind of attacks. Gray hole attack is also named as node misbehaving attack in the section[10][6].

System Architecture



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Proposed approach

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. 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. 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. 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. Cooperative Bait Detection Scheme (CBDS) based on DSR routing protocol to identify malicious nodes launching black or gray hole attack and cooperative attacks. DSR. It identifies and avoids the black hole attack based on merging proactive and reactive defense approach in MANET with virtual and non-existent destination address to deceive or bait malicious nodes to reply RREP.

Conclusion

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.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

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] S.Amaswamy,J. Dixon,H. Fu, K. Nygard,and M. Sreekantaradhya, "Prevention of cooperative black hole attacks in wireless ad hoc networks, "in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[2] D. Agrawal, H. Deng, and W. Li, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[3] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf.Security, vol. 7, no. 1, 2010.

[4] M. Baker, T. J. Giuli, K. Lai, and S. Marti, "Mitigating routing misbehaviorin mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom,2000, pp. 255–265.

[5] K. Balakrishnan, K. Liu, D. Pramod, and K. Varshney, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550,May 2007.

[6] B. Bhargava, M. Linderman, and W. Wang, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp.Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[7]J.-M. Chang, H.-C. Chao, and J.-L. Chen, P.-C. Tsou, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based onhybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun.,VITAE, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[8] C. Chang, H. Chao, and Y.Wang, "An efficient Mesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229–239, Apr. 2007.

[9] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations,Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available:http://www.elook.org/computing/rfc/rfc2501.html

[10] H.Fu, and H. Weerasinghe "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

[11] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc.WiSec, 2009, pp. 103–110.

[12]D. Maltz and D. Johnson, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[13] K. Nahrstedt, and Y. Xue "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367–388, 2004.

[14] A. J.Paul and K. Vishnu, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl.,vol. 1, no. 22, pp. 28–32, 2010.

[15] Qual Net Simulation Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com