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

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach

Sarvesh S. Joshi,Sagar Ghodechor, Amol Barbade, Prof. Rahinj P.L

B.E Student, Dept. of Computer Engineering, RGCOE, Savitribai Phule Pune University, Takali Dhokeshwar, Parner, Ahmednagar, Maharashtra

Assistant Professor, Dept. of Computer Engineering, RGCOE, Savitribai Phule Pune University, Takali Dhokeshwar, Parner, Ahmednagar, Maharashtra

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 black hole attack in which malicious node falsely claiming itself as having the fresh and shortest path to the destination. Mobile Ad-hoc Networks (MANET) are used for communication among Mobiles and roadside equipment's. MANET, is a form of Mobile ad-hoc network, to provide communications among nearby Mobiles and between Mobiles and nearby fixed equipment, usually described as roadside equipment. Each Mobile equipped with MANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network 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 defence architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Proposed system helps us in defending against the black hole attack without any requirement of hardware and special detection node.

KEYWORDS: CBDS: - Cooperative Bait Detection Scheme, DSR Based Routing: - Dynamic Source Routing, MANET: - Mobile Ad hoc Network, Collaborative Black Hole Attacks, Gray Hole Attacks, Proactive defense, Reactive defense, Reverse Tracing.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) consists of a collection of mobile nodes which are not bounded in any infrastructure.Nodes in MANET can communicate with each other and can move anywhere without restriction. This non-restricted mobility and easy deployment characteristics of MANETs make them very popular and highly suitable for emergencies, natural disaster and military operations.

Nodes in MANET have limited battery power and these batteries cannot be replaced or recharged in complex scenarios. To prolong or maximize the network lifetime these batteries should be used efficiently. The energy consumption of each node varies according to its communication state: transmitting, receiving, listening or sleeping modes. Researchers and industries both are working on the mechanism to prolong the lifetime of the node's battery. But routing algorithms plays an important role in energy efficiency because routing algorithm will decide which node has to be selected for communication.

MANET is a collection of mobile, decentralized, and self-organized nodes. The distributive nature, infrastructure less and dynamic structure make it an easy prey to security related threats. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links.Each device in a MANET is free to move randomly in any direction, and will therefore change its links to other

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

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

devices again and again. Each must forward traffic unrelated to its own use, and therefore can acts as router. The major challenge in building a MANET is making each device to monitor and maintain the information required to traffic routing ..The objective of this paper is to propose a cooperative bait detection scheme to combat sleep deprivation and denial of service attack over MANET. This scheme merges the proactive and reactive defence architecture in MANET by using the first hop neighbour address as destination address to bait the malicious nodes which were causing the attack. A particular system may be vulnerable to unauthorized data access because the system does not verify a user's identity before allowing database to access. MANET is more vulnerable than wired network.

II. RELATED WORK

Chin-Feng Lai et al, IEEE [2014]. In this paper the author[1] tries to solve the issues of blackhole and grayhole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the grayhole and blackhole attacks.[2] Cooperative Bait Detection Scheme (CBDS) has been used to tackle blackhole and grayhole attacks caused by malicious nodes [1]. CBDS combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique.
In Game theory mechanism each node needs to know only its own state information and aggregate effect of the other nodes in the MANET network. It's a fully distributed scheme. In future the mechanism could be extended to multiple attackers and multiple defenders. Some devices in network might be interested in computing some functions of their private inputs without disclosing the inputs to the other devices, such type of computation is Secure Multiparty Computation (SMC) [4]. The solution to this problem could be by modification of data inputs to prevent eavesdropping. Other approach is by making the identity ambiguous to hide it from other parties. The major focus in the paper is made on that how the SMC solutions can be used for preserving the privacy during the computation.

Attacks might be active or passive. According to hierarchy idea of OSI model the security architecture of the MANET can be divided into five layers [5] as infrastructure layer, network security layer, application layer and security layer describing functions of each layer in detail. Security architecture of MANET is designed according to OSI hierarchy. Relations between each layer of security architecture of MANET and that of OSI is provided that helps in planning and designing reliable and secure MANET design.

III. PROPOSED SYSTEM

Each node sends a route request signal (RREQ). The neighbour nodes receive the RREQ signal and reply with a RREP signal. If the RREP signal is received back by the transmitting node, the system is judged as normal and data transmission can begin. However if the transmitting node does not receive back RREP signal delivery hop limit is checked. If the delivery hop limit has not exceeded the threshold, RREQ is resend. Otherwise, the RREQ sending is terminated.

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

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

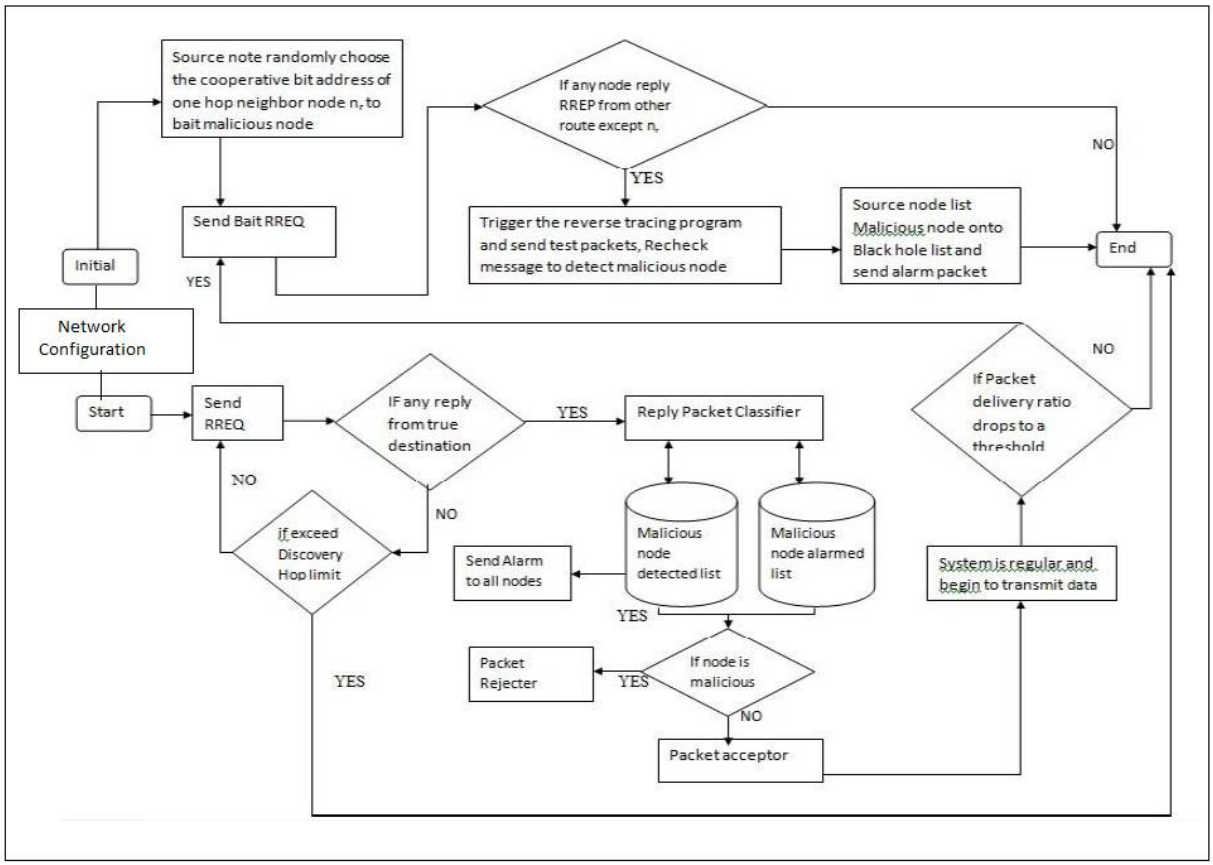

Figure 1. Proposed System

Once the system starts transmitting data signal normally, packet delivery ratio is scanned. If the packet delivery ratio is above threshold limit, then no malicious nodes are present and the process terminates. However if packet delivery ratio drop is detected, a bait RREQ is sent and response is awaited. If there is no response then the packet delivery ratio drop may be due to inefficient routing and so CBDS is terminated. But if the transmitting node receives a RREP response to the bait RREQ, reverse tracing program is triggered and test packets and recheck messages are sent to confirm malicious node detection. On confirmation of malicious node, source node updates its list of malicious node with this new entry and broadcasts an alarm signal inside the network for all the nodes to follow suit. When all the nodes have updated their list of malicious nodes, the detected node is blacklisted and further communication to the node are stopped. In a randomly deployed node topology source node chooses the cooperative bait address randomly from its one hop neighbor nodes and sends the bait RREQ.

IV. PSEUDO CODE

Step 1: Send RREQ
Step 2: if (RREP == D true) \\ If RREP is from true destination
Step 3: system=1; \\ system is working fine
Step 4: else
Step 5: if (Time > T) \\ T is the discovery time threshold
Step 6: end process;
Step 7: else

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

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

Step 8: send RREQ again;
Step 9: end if
Step 10: end if
Step 11: if (PDR < T1) \\ if packet delivery ratio drops to a certain threshold
Step 12: Send Bait RREQ'
Step 13: else
Step 14: end process
Step 15: end if
Step 16: if (RREP == true) \\ if any RREP
Step 17: Trace Mechanism =1 ; \\ Trigger trace mechanism
Step 18: else
Step 19: end process;
Step 20: end if ;
Step 21: Initiate trace mechanism;
Step 22: MN detected;
Step 23: MN = black listed; \\ malicious is black listed
Step 24: Stop

V. SIMULATION RESULTS

The simulation studies involve the deterministic small network topology with 5 nodes as shown in Fig.1. The proposed energy efficient algorithm is implemented with JAVA Technology. We transmitted same size of data packets through source node 1 to destination node 5. Proposed algorithm is compared between two metrics Total Transmission Energyand Maximum Number of Hops on the basis of total number of packets transmitted.
Figure 2 shows the variation of Packet Delivery Ratio (PDR) with malicious node ratio for Denial of Service (DOS) attack. Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol.
PDR = Σ Number of packet receive / Σ Number of packet send

In ideal conditions the PDR value for different malicious node ratio is high. When the system is under DOS attack the PDR value becomes lower than that in ideal conditions. However applying CBDS increases the corresponding PDR value further to ideal conditions.

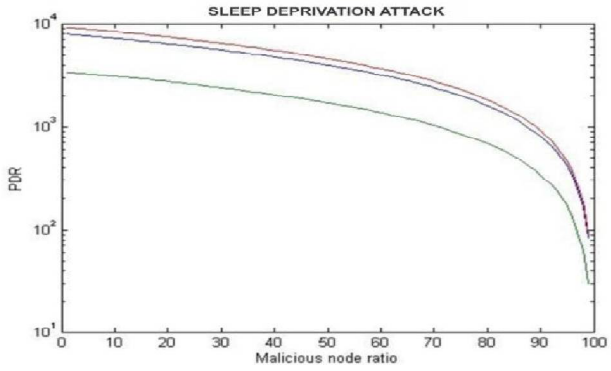

Figure 2: PDR vs. malicious node ratio for gray hole attack

Figure 3 represents the variation of throughput with change in malicious node ratio in case of DOS attack. Throughput is the rate of successful message delivery over a communication channel. Higher the throughput better is the protocol. The throughput is low in case of ideal condition. RCA raises the value of throughput which is further increased by

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

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

CBDS. The throughput after CBDS however shows a varying trend (it is lower than the throughput value before implementing CBDS in some cases while in other it is higher). This too remains an area for further improvement.

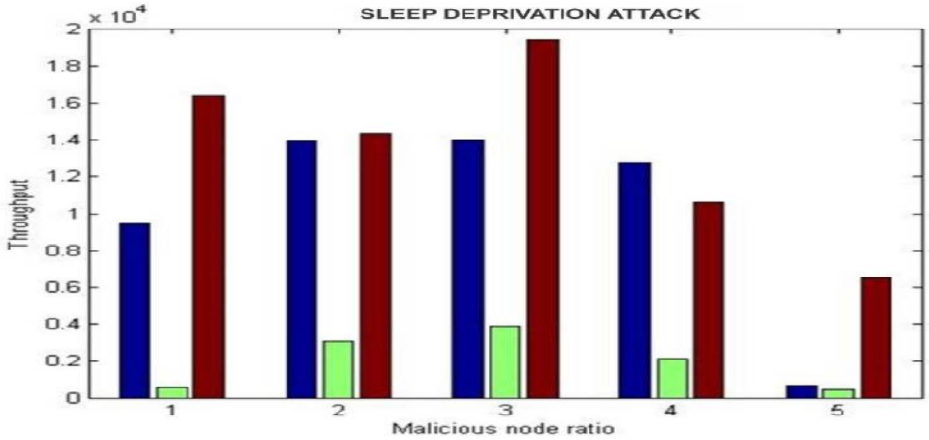

Figure 3: Throughput vs. malicious node ratio for gray hole Attack

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric.In this paper, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. Our simulation results revealed that the CBDS outperforms the DSR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. As future work, we intendto 1) investigate 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 otherwell-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

REFERENCES

1. Chin-Feng Lai, Han-Chieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, *Member, IEEE*.Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.pp. 218-223, 2013
2. BabakHosseinKhala, HamidrezaBagheri, Marcos Katz, Mohammad JavadSalehi, Mohammad Noor mohammadpour, and Seyed Mohammad AsghariPari. A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks. Rakesh kumar Sahu,Narendra S chaudhari "performance evaluation of ad hoc network underblack hole attack 978-1-4673-4805-8/$31.00,IEEE 2012
3. Richard Yu, Helen Tang, Minyi Huang and Yanwei Wang, *Member, IEEE.* A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks. pp. 218-223, 2012
4. Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India), 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.pp. 218-223, 2010
6. Anjum Asma and Gihan Nagib,'Energy Efficient Routing Algorithms for Mobile Ad Hoc Networks–A Survey', International Journal of Emerging Trends & Technology in computer Science, Vol.3,Issue 1, pp. 218-223, 2007.
7. Hong-ryeol Gil1, Joon Yoo1 and Jong-won Lee2 ,'An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks', Proceedings of the 2nd International Conference on Human. Society and Internet HSI'03, pp. 302-311, 2003.