JCSE International Journal of Computer Sciences and Engineering Open Access

Survey paper Volume-4, Issue-5 E-ISSN: 2347-2693

Survey on Black Hole and Gray Hole Attacks in MANET

M. Nachammai[1*] and N. Radha[2]

[1,2] *Department of Computer Science(PG),*
PSGR Krishnammal College for Women, Coimbatore, India

Available online at: www.ijcseonline.org

Received: Apr/21/2016 Revised: May/02/2016 Accepted: May/22/2016 Published: May/31/2016

Abstract— Mobile Ad hoc Network (MANET) is one of the most promising technologies in the recent years. In MANET, a wireless network is quickly formed using mobile nodes. Because of its characteristics such as open and undefined medium, limited resources, offering a secure data transmission in presence of malicious nodes in the network is main issues of the MANET. The black hole and gray hole attacks are major security threats in MANET, in which the packets are dropped in intermediate nodes. The main objective of this paper is to study the techniques used to eliminate the packet drop in intermediate nodes using malicious node detection techniques. In this paper, various malicious node detection methods such as Local anomaly detection and Cooperative anomaly detection , Fuzzy and wavelet transform based IDS system , Modified DSR protocol , Kullback-Leibler divergence approach, FireCol , hash function based method and cooperative bait detection scheme (CBDS) are studied and analyzed. The findings of this work proved that the cooperative bait detection achieves better results than the other approaches in terms of packet delivery ratio and end-to-end delay.

Keywords— *MANET, Black Hole Attack, Gray Hole Attack and Bait Detection Mechanism*

I INTRODUCTION

Mobile Ad hoc Network (MANET) is a wireless network in which all mobile nodes are combined to form a network and it can be changed dynamically. MANET has some characteristics such as limited bandwidth and battery power. Each node in a network may act as a sender or receiver and it may transmit and receive the data due to its mobility in nature. The nodes transmit the packets with each other within the radio range through wireless links.

MANETs are having numerous security issues due to their intrinsic nature like open medium, dynamically changing topology, insufficient battery power and limited bandwidth. Hence, there will be number of attacks survived or launched on adhoc networks. Since wireless networks came into survival, the routing process is difficult task.

Black hole and gray hole attacks are the possible attacks in MANET. **Black hole attack** is a one kind of attacks in Manet. It is also called as packet drop attack in which so many packets are dropped**.** In this process, if any node is malicious, it will wait for the neighbours RREQ. A malicious node receives RREQ packets, then it sends the false RREP packet to source node. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets anywhere. The packets are transferred besides this path. After receiving data packets the attacker node drops these packets and doesn't send them to destination.

Gray hole attack is an another type of attacks in Manet. In gray hole attack, the node gets RREQ packets from source and forward to destination. After creating route, it drops some of data packets. This type of dropping against black hole, does not drop all data packets which was send by source node. **Attacker drops the packets occasionally.** It means attacker sometimes acts like a normal node and other times as a malicious node.

II BACKGROUND STUDY

Jaydip Sen [1] introduced a new gray hole detection Mechanism for Gray Hole Attack in MANET. The gray hole node selectively drop and forwards the packets to particular destination. To identify the gray hole nodes the detection mechanism involves both local and cooperative detection. The mechanism consists of four security procedures which are invoked sequentially. The security procedures are: (1) Neighborhood data collection, (2) Local anomaly detection, (3) Cooperative anomaly detection, and (4) Global alarm raiser. The node that initiates the local anomaly detection procedure as the Initiator Node (IN). Based on the RREQ and RREP message the malicious nodes are detected. The main objective of the cooperative anomaly detection is to increase the detection reliability by reducing the probability of false detection of local anomaly detection procedure.

Yu Chen [2] proposed a collaborative detection scheme for the detection of DDoS attacks in the multiple network domains. The approach utilizes a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). It utilizes the changes in the traffic across the networks at the earliest time for detecting DDoS. At the early stage of a DDoS attack, the traffic changes are difficult to detect because low traffic fluctuations are not observable. Monitoring the Internet traffic at individual flow level is cost prohibitive to cover all possible flows. CAT is possible to be implemented in the router levels and hence the detection of DDoS is efficient.

Bharat Bhargava [3] addressed the collaborative attacks in the wireless adhoc networks. The major contribution includes the discovery of collaboration among the attackers. It utilizes the IDS for collaborative work with the networks to identify the attacks. The IDS system introduces the techniques for preventing the black-hole, gray hole, and worm hole attacks which are possible to occur in collaborative manner. However the approach seems to be not feasible as there are no specific machine learning approaches like Support vector machine (SVM) in IDS**.**

Weichao Wang[4] proposed a defense mechanism for preventing collaborative packet drop attacks in MANETs. The proposed hash function based method is utilized to generate the node behavioral proofs that contain the information from both the data traffic and forwarding paths. The approach is based on audit based detection of collaborative packet drop attacks such that only the hash calculation is conducted on the received packet. Thus the approach does not allow the generation of node behavioral proofs before receiving the data packets correctly and hence reduces the overhead in the intermediate nodes.

Vishnu[5] proposed a complete protocol for the prevention of the cooperative black/gray hole attack in MANETs. The black/gray hole nodes are detected effectively which results in removal of those nodes from the routing process. Initially a backbone network of trusted nodes is established and the source node periodically requests one of the backbone network nodes to a restricted IP address. Whenever the node wants to transmit, it not only sends a RREQ (Route Request) in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP)also. If any of the routes respond positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

M. Mohanapriya [6] introduced a modified DSR protocol to detect and remove the selective black hloe attacks in MANET. It is one kind of black hole attacks which are dropping the data packets selectively. In this method the source node sends the RREQ packets to destination for route discovery. To eliminate gray hole attack, when the destination nodes receives data packets from the source node, it starts the process of finding the presence of any gray hole nodes in the path. In this approach, when the source node has data packets to send to the destination, it divides the data to be transmitted into various blocks and sends one block of data at a time to the destination. It also intimates the number of data packets it sends in a block to the destination before the actual transmission of the data using various route. When the destination node discovers that the actual number of data packets it receives from its previous hop node, is significantly less than the number of data packets the source node sends, then it starts the gray hole node discovery process.

Yang Xiang [7] introduced the detection mechanism for the low-rate DDoS attacks detection and also trace back of attacker information. The major contribution of the detection mechanism is that the introduction of newer information metrics, such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks. This approach helps in detecting the difference between the legitimate traffic and attack traffic in order to discover the attacker nodes. Then the Kullback–Leibler divergence approach is used to adjust the distance and obtain the detection sensitivity. The IP traceback approach traces the attackers by using the IP address of the LANs utilized. Thus the attack and attackers are detected very early with reduced false positives.

Jian-Ming Chang [8] proposed CBDS, a Cooperative Bait Detection Scheme for the hybrid defense of the MANET against malicious nodes. The approach detects malicious nodes launching black/gray hole attacks and cooperative black hole attacks by adapting for the dynamic topology of the MANET. The CBDS approach integrates the proactive and reactive defense architectures and randomly cooperates with a stochastic adjacent node and uses the address of the adjacent nodes as the bait and utilizes reverse traceback for preventing the attacks. CBDS effectively reduces the wastage of resources and aids in the detection of the attackers with maximum accuracy.

Jerome Francois [9] proposed the FireCol which is a collaborative protection network for the detection of the flooding DDoS attacks. FireCol is designed with an approach of service customers for the participating IPs along the path of subscribed customer collaboration. The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high. Using this way of measurement, the overall traffic is measured which allows the detection of possible attacks. FireCol also helps in detecting other flooding scenarios, such as flash crowds and botnet-based DDoS attacks. However the supportability for different IP structures is a area of concern that needs extensive research.

Jian-Ming Chang [10] introduced a Cooperative Bait Detection Approach in DSR protocol. In this process malicious nodes such as grayhole/collaborative black hole attacks are launched in a routing path. To detect these malicious nodes cooperative bait detection scheme (CBDS) is introduced. In this method the neighbouring node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are perceived using a reverse tracing method. The detected nodes are kept in black hole list. Then it can be sent alert to the neighbouring nodes. It only used to detect malicious nodes, but it does not consider the security of data.

III SUMMARY OF THE BACKGROUND STUDY

S. No	**Title**	**Author Name**	**Methods Used**	**Merits**	**Demerits**
1	A mechanism for detection of gray hole attack in mobile ad hoc networks	Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar	Local anomaly detection and Cooperative anomaly detection	High detection rate	False positive rate needs to be improved
2	Collaborative detection of DDoS Attacks over multiple network domains	Yu Chen, Kai Hwang and Wei-Shinn Ku	CAT (change aggregation trees)	Acceptable detection rate	Better mechanism needed to improve the network performance
3	Addressing collaborative attacks and defence in ad hoc wireless networks	Bharat Bhargava, Ruy De Oliveira, Yu Zhang and Nwokedi C.Idika	Fuzzy and wavelet transform based IDS system	High detection rate	It seems to be not feasible as there are no specific machine learning approaches in IDS.
4	Defending against collaborative packet drop attacks on MANETs	Weichao Wang, Bharat Bhargava and Mark Linderman	Hash function based method	Low overhead	It does not achieves higher detection rate
5	Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks	Vishnu.K., Amos J. Paul	Gray/Black hole removal process	It detects and remove Black/Gray Holes	False positives may occur
6	Modified DSR protocol for detection and removal of selective black hole attack in MANET	M. Mohanapriya, Ilango Krishnamurthi	Modified DSR protocol	High packet delivery ratio Low end to end delay	Packet loss needs to reduced
7	Low-rate DDoS attacks detection and trace back by using new information metrics	Yang Xiang, Ke Li and Wanlei Zhou	Kullback-Leibler divergence approach	It detects the attacks easily	Low detection rate
8	CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based	Jian-Ming Chang, Po Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen	Cooperative Bait Detection Scheme	Reduces wastage of resources	Better mechanism is needed to improve network performance

	on hybrid defense architecture				
9	FireCol : A collaborative protection network for the detection of flooding DDoS attacks	Jerome Francois, Issam Aib and Raouf Boutaba	FireCol	Low overhead	It is difficult to support different IP structures
10	Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach	Jian-Ming Chang, Po-Chun Tsou, Issac Woungang, Han-Chieh Chao and Chin-Feng Lai	Cooperative Bait Detection Scheme	High packet delivery ratio Low routing overhead	It does not consider security of data

IV CONCLUSION

Malicious behavior of the nodes affects network performance severely. Hence providing security in presence of these malicious nodes is the major constraint for deployment of the MANET. In this paper, methods proposed to detect and/or prevent these attacks are discussed. Based on this survey a Cooperative Bait Detection Approach achieves better performance than the other approaches in terms of packet delivery ratio and end-to-end delay.

V SCOPE FOR FUTURE ENHANCEMENT

In future, after the completion of malicious node detection, Key Distribution Scheme can be used along with shuffling Algorithm for secure packet/data transmission in MANET. An improved Cooperative Bait Detection approach which incorporate the CBDS with message security schemes in order to construct a comprehensive secure routing framework to protect MANETs.

REFERENCES

[1] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, ”A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks”,IEEE, January **2007.**

[2] Yu Chen, Kai Hwang, and Wei-Shinn Ku, "Collaborative detection of DDoS attacks over multiple network domains", IEEE Transactions on Parallel and Distributed Systems, Volume **18**, Issue **12,** pp. **(1649-1662),** December **2007**.

[3] Bharat Bhargava, Ruy De Oliveira, Yu Zhang, and Nwokedi C. Idika, "Addressing collaborative attacks and defense in ad hoc wireless networks" IEEE International Conference on Distributed Computing Systems Workshops (ICDCS), pp. **(447-450)**, June **2009.** ISBN : **978-0-7695-3660-6**

[4] Weichao Wang, Bharat Bhargava, and Mark Linderman, "Defending against collaborative packet drop attacks on MANETs", International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009), New York, USA, Volume **27, 2009.**

[5] Vishnu, K and Amos J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks", International Journal of Computer Applications, Volume **1**, Issue **22** pp. **(38-42)**, February **2010**.

[6] Mohanapriya, M, Ilango Krishnamurthi , “ Modified DSR protocol for detection and removal of selective black hole attack in MANET” , Elsevier, pp. (530-538), February **2014**.

[7] Yang Xiang, Ke Li, and Wanlei Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics", IEEE Transactions on Information Forensics and Security, Volume **6**, Issue **2**, pp. **(426-437)**, January **2011**.

[8] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, and Jiann-Liang Chen, "CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture", Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), 2nd International Conference, pp. **(1-5)**. IEEE, February **2011**.

[9] Jerome Francois, Issam Aib, and Raouf Boutaba, "FireCol: a collaborative protection network for the detection of flooding DDoS attacks", IEEE/ACM Transactions on Networking (TON) Volume **20**, Issue **6** pp. **(1828-1841)**, April **2012**.

[10] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai (2015), "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" IEEE systems journal, Volume **9**, Issue **1**, pp. **(65-75)**, January **2015**.

AUTHORS PROFILE

Ms. Nachammai M, received Bachelor of Computer Application (BCA) and Master of Information Technology (M.Sc IT) from Bharathiar University, Coimbatore, India. She is Currently pursuing M.Phil Degree in the Department of Computer Science(PG), PSGR Krishnammal College for Women, Coimbatore, India. Her research interests include Advanced networking and network security.

Dr. N. Radha, She is an Assistant professor in the department of Computer Science (PG) at PSGR Krishnammal college for women, Coimbatore, India. She has more than 20 years of teaching experience. She has more than 10 publication in National Journals and has more than 25 publications in International Journals. Her Research area includes Data mining, Biometric and Information Security. She has also attended and presented in both the International and National level Seminars.