Collaborative Attack Detection Using Enhanced Co-operative Bait Detection Scheme for MANET

Rakesh Kumar ER

Asst. Prof. & Head
Computer Science and Engineering,
SAMS College of Engineering and Technology, Chennai, INDIA

Abstract - In mobile ad hoc networks (MANETs), cooperating nodes with each other is a key requirement for the establishment of communication among nodes. In the presence of wicked nodes, this kind of necessity may lead to severe security related concerns. In case, such nodes may interrupt the routing process. For preventing malicious nodes we propose to develop an enhanced co-operative bait detection scheme for detecting collaborative attacks in MANET. In this scheme, source node selects an adjacent node using the random scheduling process. The address of this adjacent node is used as bait destination address to bait malicious nodes in order to send a reply message. After the detection of malicious nodes, the packet delivery ratio (PDR) value is ensured with the threshold value, from this, the again the bait detection process is triggered.

Index Terms –Malicious Node, Collaborative Attacks, Adjacent Node, Bait Detection

I. INTRODUCTION

A. Mobile ad hoc network (MANET)

MANET is a multi-hop wireless network are composed of autonomous nodes that communicate with each other by forming dynamic topology such that nodes can easily join or leave the network at any time without any fixed infrastructure such as access points or base station and maintaining connections in a decentralized manner. The network over radio links are caused due to the self-organization of the mobile nodes. Each device in a MANET is free to move independently in any directions [1].The infrastructure less property and the easy deployment along with the self-organizing nature makes them useful for many applications like military applications, mobile social networks, emergency deployment, intelligent transportation systems and fast response to disasters [2]. MANET also throws a security challenge due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense moderate bandwidth, limited battery power, computational power and limited resources. So mobile ad-hoc networks are vulnerable to several different attacks [3]

B. Collaborative Attacks in MANET

The collaborative attacks are defined as two or more types of attacks such as the black hole attacks and the wormhole attacks, which synchronized simultaneously in the network in a collaborative way [4].It is a synchronized attacks where a system is distributed by more than one attacker simultaneously or involving two or more colluding nodes that can be processed using wired or wireless link and triggered by single or multiple attackers. Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network but not necessarily in collaboration where every attack is launched by a specialized expertise. These attacks can be classified into two different categories [5].

Direct Collaborative Attacks: Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. For examples, Black hole and Wormhole attack [6].

Collaborative attacks in ad hoc networks carriage challenges to the detection system. Malicious nodes may collude to conduct more complex and subtle attacks to prevent detection or identification. To detect against collaborative attacks essential that monitoring and detection agents collaborate efficiently. The collaboration should include each existing node in the network. [7].

C. Problem Identification

In [9], a Co-operative Bait Detection Scheme (CBDS) has been proposed. In which the source select an adjacent node as the bait destination address. But selecting the adjacent node among the neighbors of the source is not described. If the attacker is able to find out that adjacent node, it will try to avoid the Bait REQ requests. The detection process is invoked based on the packet delivery ratio (PDR) metric by the destination. But PDR alone will not be sufficient to detect the misbehaving attacks. Moreover, the detection delay will be increased since the detection process is invoked only when the destination send an alarm.

II. Related Works

Reshma Lill Mathew and P. Petchimuthu [2] have proposed a collaborative watchdog based on contact dissemination with a log file system. The watchdog has detected a selfish node in the network then spread the information to other nodes when contact occurs. The detection of the contacts among the nodes is performed based on the node's watchdog for the detecting the selfish nodes. Log file system have used for reducing the detection time of the selfish node. After forwarding the packets from the neighbor node to next neighbour node, neighbor node could not overhear the packet dropping of next neighbour node either if transmission collides between source and neighbour node or neighbour node is not within the transmission range of next neighbour node. When this happens it could not provide the security.

Tao Gong and Bharat Bhargava [4] have proposed to defend the ad hoc network under collaborative attacks such as the black hole and the wormhole attacks using new tri-tier cooperative immunization from the inspiration of the human immune system. Tri-tier immunization includes native immune tier to recognize known attacks, adaptive immune tier to learn unknown attacks and parallel immune tier is built with the cloud-computing infrastructure for increasing both the efficiency and robustness of immune computation. The approach provides immunization to isolate the nodes under attacks by the network reconfiguration. Still it provides security reconfiguration is not possible.

Mahdi Nouri et al [8] have proposed a collaborative technique for detecting a wormhole attack in that neighborhood using clustering. Monitor node initiates the detection process by passing messages between the nodes and depending on the messages received determine suspected nodes that sent to the monitor node. The suspected nodes receive at least a minimum number of votes or only one vote are finally detected as malicious nodes by inspecting the votes at monitor node and isolate malicious nodes from a group of nodes in routing process. But, using this technique not possible for detecting wormhole attack in the form of out of band attack. When there is congestion or collision, a node may be dropping packets due to overloaded, and so the algorithm will not work properly. And also if a monitor node continuously monitoring the detection process, it may cause exhausting of battery power because of overhead of being the monitor node.

Jian-Ming Chang et al [9] have proposed a cooperative bait detection scheme (CBDS) by designing a DSR based routing mechanism for detecting and preventing malicious nodes that attempts to launching gray hole/collaborative black hole attacks in MANETs that incorporates the advantages of both proactive and reactive response. Using a reverse tracing technique malicious nodes are detected and prevented from participating in the routing operation. 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 and the dynamic threshold value can be adjusted according to the network performance.However, if a lower the value is set, some of neighbors of the suspicious node may not be found.

JaydipSen et al [10] have proposed a distributed protocol for detection of packet dropping attack based on cooperative participation of the nodes in a MANET. The protocol works through cooperation of some security components that are present in each node in the networks such as monitor, trust collector, trust manager, trust propagator and whistle blower by using complementary relationship between cryptographic key distribution and intrusion detection activity. The redundancies in routing information make the detection scheme highly robust and secure and using of controlled flooding technique has very low communication overhead. However, after finding the malicious node it does not consider the technique for isolating the malicious node from participating in routing process.

Chang Wu Yu et al [11] have proposed a distributed and cooperative mechanism for detecting potential multiple black hole nodes through collection of some local information. From the information, nodes evaluate that there exists any suspicious node among their one-hop neighbors. After finding the node as a suspicious, a cooperative procedure will be initiated to further check the potential black hole nodes. Then the global reaction is initiated to form a proper notification system to send warnings to the whole network. However, overhearing for collection of local information does not work always properly in situation like collision or weak signal. It leads to incorrect evaluation of the behaviour of the suspicious node.

Weichao Wang et al [12] have developed a new mechanism for audit based detection of collaborative packet drop attacks using hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths. Intermediate node construct a Bloom filter based on the contents of the packets to generate the behavioral proof. It allow the system to successfully locate the routing segment in which packet drop attacks are conducted. However, other nodes cannot find the difference between an audit packet and a common data packet. Security is based on the value of its behavioral proof. So it is not efficient. If there is no malicious node all packets are delivered to destination without any packet dropping at intermediate node. So it does not analyse any scenario for delivery of packet ratio at destination.

III. ENHANCED CO-OPERATIVE BAIT DETECTION TECHNIQUE

A. Overview

In this paper, we propose to design a Distributed Trust model co-operative Bait detection scheme detecting collaborative attacks in MANET. The Bait detection process is invoked based on the the trust value which is derived using the Bayesian inference. A trust value is estimated for each node from the direct observations. When the trust value of any intermediate node falls below a minimum threshold value, the co-operative Bait detection scheme will be invoked by the source. Moreover if the trust value of any nodes in the random schedule table becomes low, it will be removed from the table.

The source node selects the adjacent nodes based on the random scheduling method. The source node collects the address details of the intermediate nodes from the routing table forming a random schedule table. This table consists of one hop neighbours, their address and a random time stamp value. The address of the adjacent node is used as bait destination address to bait malicious nodes. The source node selects the adjacent node from the random schedule table having latest time stamp value and invokes the bait detection scheme. It then marks time stamp of the selected node as expired so that next time another node from the table can be selected.

B. Bait Detection

After the selection of the adjacent node by the source node, malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique [9].
The Co-operative Bait Detection Scheme (CBDS) comprises three steps: 1) Bait setup phase 2) initial reverse tracing phase; and 3) reactive defence phase

1) Bait Setup Phase

The source node selects the adjacent node in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. The adjacent node is selected from the random schedule table having latest time stamp value and invokes the bait detection scheme. The random scheduling is based upon the routing table. The routing table consists of the distance of one hop neighbours, their address and a random time stamp value.
The timestamp can be calculated from the delay time as follows,

$$\partial = (t_4 - t_1) - (t_3 - t_2) \tag{1}$$

t_1 - timestamp of the request packet transmission
t_2 - timestamp of the request packet reception
t_3 - timestamp of the response packet transmission
t_4 - timestamp of the response packet reception

One hop neighbours	**Distance**	**Address**	**Random time stamp value**

Fig 1 Random scheduling table

The bait setup phase is activated whenever the bait RREQ′ is sent earlier for seeking the initial routing path. The bait analysis procedure is as follows.

a. If n_r node had not launched a black hole attack, then after the source node had sent out the RREQ′, the other nodes has sent the RREP indicates that the malicious node is present in the reply routing. So in order to detect the route a reverse tracing program is initiated.

b. If only the n_r has sent the RREP for the RREQ′ from the source node, there was no other malicious node in the network except the n_r.

c. If both n_r and the other nodes in the network have sent the RREP shows that the malicious node is present in the route reply.

d. If the n_r does not send the RREP intentionally, then n_r would be directly directed into the blackhole list by the source node.

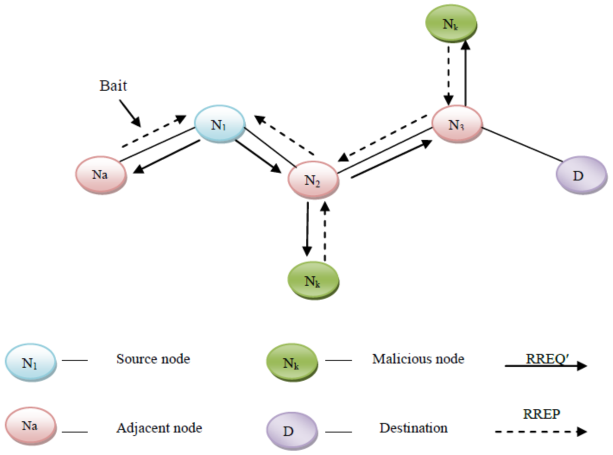

Fig 2 Random selection of a Cooperative bait address

2) Reverse Tracing Phase

Using the reverse tracing phase, the malicious nodes are detected through the route reply RREP for the RREQ′ message. If a malicious node has received the RREQ′, it will reply with a false RREP [9].

Initially an address P-list and a route information K_k list is created,

$$P = \{n_1 \ldots n_k \ldots n_m \ldots n_r\} \quad [9]\ (2)$$

$$K_k = \{n_1 \ldots n_k\} \quad (3)$$

So when a malicious node n_m, replies with a false RREP, this address P-list is recorded in the RREP. If the node n_k receives the RREP, it will separate the P-list by the destination address n_1 of the RREP in the IP field and get the address list $K_k = \{n_1 \ldots n_k\}$, where K_k represents the route information from source node n_1 to destination node n_k. After that, node n_k determines the differences between the address P-list and K_k list.

$$K'_k = P\text{-}K_k \quad (4)$$

$$K'_k = \{n_{k+1} \ldots n_m \ldots n_r\} \quad (5)$$

where K'_k – route information to the destination node

K'_k is stored in the RREP's "Reserve field" and then they are reverted to the source node. The source node receives the RREP and the K'_k list of the nodes which received the RREP. In order to ensure that K'_k does not come from the malicious node, the n_k node after receiving the RREP compares

- A. the source address in the IP fields of the RREP;
- B. the next hop of n_k in the $P = \{n_1, \ldots n_k, \ldots n_m, \ldots n_r\}$;
- C. one hop of n_k;

If A is not the same with B and C, then the received K'_k performs a forward back. Otherwise, n_k have to just forward back the K'_k that was produced by it.

The trusted set T is given by,

$$T = P\text{-}S \quad (6)$$

where S is the Dubious path information

$$S = K'_1 \cap K'_2 \ldots . K'_k \quad (7)$$

C. Representation of malicious node in the route

The below figure shows the operation for the detection of the tracing set up

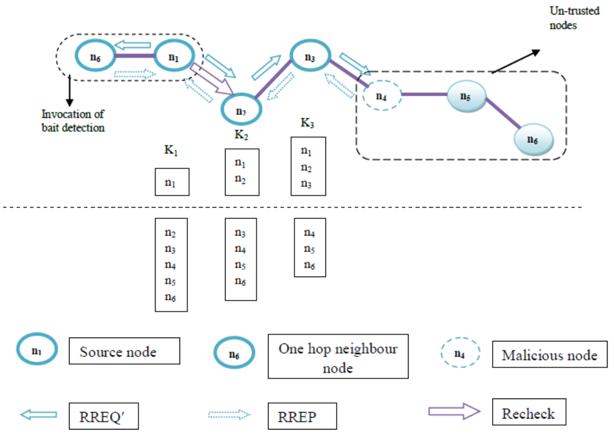

Fig 3 Reverse tracing phase

Let us consider a case such that a single malicious node n_4 is present in the route.

1. Initially the source node n_1 pretends to send a packet to the destination node n_6. While sending the RREQ′, node n4 replies with a false RREP with the address list P= $\{n_1, n_2, n_3, n_4, n_5, n_6\}$.
2. Node n_5 is a random node which is filled by n_4. If n_3 had received the RREP by n_4, it first separates the P-list with the destination address n_1 of RREP in the IP field. From this it gets the address K_3= $\{n_1, n_2, n_3\}$.
3. Next to this n_3 conducts the set difference and acquires K'_3= $\{n_4, n_5, n_6\}$, then replies with K'_3 and RREP to the source node n_1. Similarly n_2 and n_1 performs the same process after receiving the RREP such that K'_2= $\{n_3, n_4, n_5, n_6\}$ and K'_1= $\{n_2, n_3, n_4, n_5, n_6\}$
4. The dubious path information of the malicious node S= $\{n_4, n_5, n_6\}$
5. After this the source node calculates the trust value set T= P-S, from this we can obtain T= $\{n_1, n_2, n_3\}$
6. Next the source node will send the test packets to this path and the recheck message to n_2, requesting it to enter the promiscuous mode and listening to n_3. As the result of the listening phase, it could be found that n_3 might divert the packets to the malicious node n_4; hence, n_2 would revert the listening result to the source node n_1, which would record n_4 in a blackhole list.
7. If nodes n_4 and n_5 were cooperative malicious nodes the trusted set is T= $\{n_1, n_2, n_3\}$, n_2 is requested to listen to which node n_3 might send the packets. Either n_5 or n_4 would be detected, and their cooperation is stopped. Hence, the remaining nodes would be baited and detected.

D. Overall algorithm

1. If the PDR value of any intermediate node falls below a minimum threshold value, the bait detection scheme is invoked by the source node.
2. The source node for this selects the adjacent node using random scheduling process, with the latest time stamp value from the Random scheduling table.
3. The bait detection is started initially such that the bait phase is activated whenever the bait RREQ′ is sent earlier for seeking the initial routing path.
4. From this initial bait setup the malicious node is detected from the route reply.
5. For this a reverse tracing setup is initiated. Here the trust set and a dubious information set is acquired from the nodes sending RREP for RREQ′. From this cooperative malicious nodes were found and their cooperation is stopped and the bait detection is continued for the remaining nodes.

IV. Simulation Result

A. Simulation Model and Parameters

The Network Simulator (NS2) [13], is used for simulation. In the simulation, 100 mobile nodes are deployed in a 1000 meter x 1000 meter region for 50 seconds of simulation time. The node mobility is based on the Random Waypoint Model. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in Table-1.

Table-1 Simulation Settings

No. of Nodes	100
Area Size	1000 X 1000
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	150Kb
Attackers	5,10,15,20 and 25

B. Performance Metrics

The proposed Distributed Enhanced Co-operative Bait Detection Scheme (ECBDS) for detecting collaborative attacks is compared with CBDS [9]. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop**: It refers the average number of packets dropped during the transmission
- **Delay**: It is the amount of time taken by the nodes to transmit the data packets.

C. Results

The number of attackers is varied as 5,10,15,20 and 25 for 100 nodes and the above metrics are evaluated. From figure 4, 5 and 6, we can see that ECBDS attains 12% less delay, 11% higher packet delivery ratio and 33% less packet drop, when compared to CBDS.

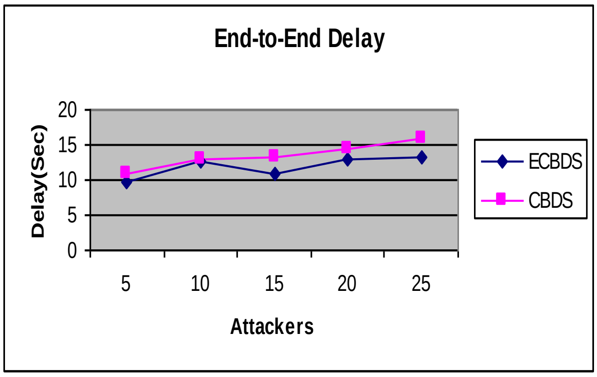

Fig 4: Attackers Vs Delay

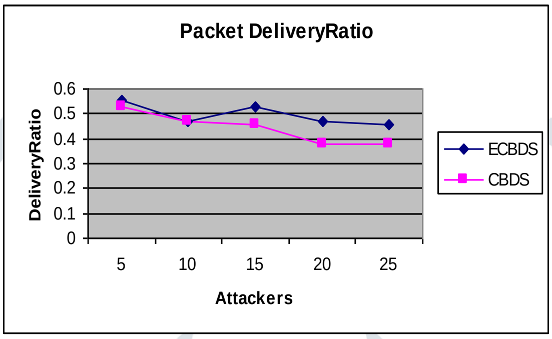

Fig5: Attackers Vs Delivery Ratio

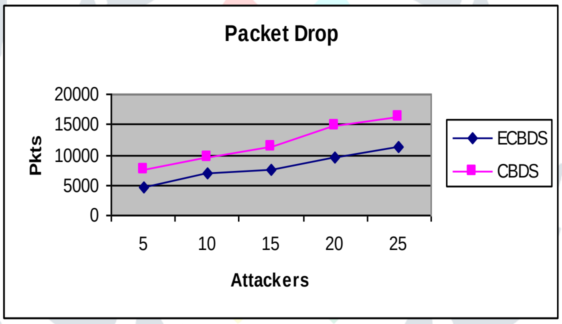

Fig 6: Attackers Vs Drop

V. Conclusion

In this paper we have proposed an enhanced co-operative bait detection scheme for detecting collaborative attacks in MANET. For this, the source node selects an adjacent node using the random scheduling process. This is the address of this adjacent node is used as bait destination address to bait malicious nodes in order to send a reply RREP message. Simulation results show that ECBDS reduces the packet drop and delay while increasing the delivery ratio, when compared to existing CBDS.

References

[1] Meenakshi Patel and Sanjay Sharma, “Detection of Malicious Attack in MANET A Behavioral Approach”, IEEE 3rd International Advance Computing Conference (IACC), pp. 388 – 393, 2012.

[2] ReshmaLill Mathew, P. Petchimuthu, “Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, ISSN: 2277 128X, March 2013.

[3]Umesh Kumar Singh, KailashPhuleria,Shailja Sharma and D.N. Goswami, “An analysis of Security Attacks found in Mobile Ad-hoc Network”, International Journal of Scientific & Engineering Research, vol. 5, Issue 5, ISSN 2229-5518, May-2014.

[4] Tao Gong and Bharat Bhargava, “Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model”, Security and Communication Networks, vol. 6, Issue 1, pp. 58–68, January 2013.

[5] Ajay Dureja and VandnaDahiya, “Performance Evaluation of Collaborative Attacks in Manet”, A Monthly Journal of Computer Science and Information Technology (IJCSMC), vol. 3, Issue. 7, pp. 457 – 465, ISSN 2320–088X, July 2014.

[6] Cong Hoan Vu and AdeyinkaSoneye, "An Analysis of Collaborative Attacks on Mobile Ad hoc networks", LAP LAMBERT Academic Publishing, June 2009.

[7] Bharat Bhargava, Ruy de Oliveira, Yu Zhang and Nwokedi C. Idika, "Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks ", 29th IEEE International Conference on Distributed Computing Systems Workshops, pp. 447 - 450, ISSN :1545-0678, 2009.

[8] Mahdi Nouri, SomayehAbazariAghdam and SajjadAbazariAghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs", International Conference onResearch and Innovation in Information Systems (ICRIIS), pp. 1- 6, 2011.

[9] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, vol. PP, Issue: 99, ISSN: 1932-8184, pp. 1 – 11, 2014.

[10] JaydipSen, M. Girish Chandra, P. Balamuralidhar, Harihara and S.G., Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, pp. 75 - 80, 2007.

[11] Chang Wu Yu, Tung-Kuang Wu, ReiHeng Cheng and Shun Chao Chang, " A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", Emerging Technologies in Knowledge Discovery and Data Mining Lecture Notes in Computer Science,vol. 4819,pp. 538-549, 2007.

[12] Weichao Wang, Bharat Bhargava and Mark Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs", 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS), vol. 27, 2009.

[13] Network Simulator: http:///www.isi.edu/nsnam/ns

.

AUTHOR DETAILS

Rakesh Kumar ER was born in Kanyakumari District, Tamil Nadu, India in 1985. He obtained his B.Sc., M.Sc. M.E. M.Phil. Degrees in Computer Science in the years 2005, 2007, 2010 and 2012 respectively. He has more than 6 years of teaching experience. He has presented 5 research papers in various national and international conferences. He has also published more than 5 research papers in reputed international journals. He has guided several UG and PG students for their project work. His area of interest is Network Security and Wireless Sensor Networks. Currently, he is with SAMS College of Engg. & Tech, Chennai, India, as Asst. Prof and Head of the Department of Computer Science and Engineering.