Malicious Node Detection in MANETs using Cooperative Bait Detection Approach and Trust Model

Ravindra Saini[#] P. Sunitha Devi[*]

[#]*M Tech., G. Narayanamma Institute of Technology & Science, Hyderabad, Telangana, India*

[*]*Assistant Professor, CSE, G. Narayanamma Institute of Technology & Science, Hyderabad, Telangana, India*

***Abstract*— Major requirement in the Mobile Ad hoc NETworks (MANETs) is that all the mobile nodes should cooperate with each other so that the proper communication among nodes can be established. But this cannot be done if malicious nodes are present in the network. This leads to the interruption in the smooth communication among nodes. Detecting Malicious node in MANETs is a challenge. This Paper present a feasible solution to detect malicious node causing Black Hole and Gray Hole attack in MANETs. This method is designed by merging Cooperative Bait Detection approach and Trust model so that it can detect malicious node in the network efficiently. This method is referred as Cooperative Bait Detection approach using Trust model (CBDT)**

***Keywords*— Mobile Ad hoc NETworks (MANET), Cooperative Bait Detection approach using Trust model (CBDT), Ad hoc On-Demand Distance Vector (AODV) routing protocol, Black hole attacks, Gray hole attacks.**

I. INTRODUCTION

MANETs is a set of autonomous mobile devices that can exchange information with each other through wireless means. Each node in MANETs are autonomous in nature i.e. in addition of sending and receiving data or information they also act as a router. In addition, any node in the network can join or leave the network making its topology dynamic in nature. MANETs don't have any fixed infrastructure. Therefore, MANETs need cooperation and trust among nodes for proper communication in the network.MANETs are the fastest growing network. MANETs are vulnerable to many attacks which involves malicious nodes that disrupt proper communication in the network and to detect malicious nodes is a challenge.

Among several available routing protocol for MANETs Ad hoc On-Demand Distance Vector (AODV) routing protocol is generally preferred, because it minimizes the routing overhead and thus enhances the performance of the network. In AODV each node maintains a routing table that stores the address of the neighbor node. Whenever a source node wants to send the data to the destination it broadcast Route Request (RREQ) message, neighbor node receives the RREQ message and updates its own routing table before forwarding it to their neighbor. When RREQ reaches the destination node or any intermediate node that has the shortest route information to the destination, replies with RREP back to the source node. Source node on receiving the RREP starts sending the data to the destination.

MANETs are vulnerable to several attacks. This paper is dealing with two types of attack Black Hole attack and Gray Hole attack.1) Black hole attack is a kind of attack in which the malicious node claims that it is having the shortest route to the destination. When source starts sending the data through malicious node believing that it is having shortest route, the malicious node starts dropping every packet instead of forwarding it to the destination. For example, in the Fig. 1 node 'A' is source node, 'J' is destination node and 'D' is the Black hole node. When 'A' sends RREQ to find shortest path between 'A' and 'J', malicious node 'D' reply with RREP claiming that it is having shortest path to 'J'. When 'A' receives RREP from 'D' it starts sending the data through 'D' but instead of forwarding the data 'D' starts dropping. 2) Gray hole attack is a variation of Black hole attack in which malicious node drops the data packet only at some particular time or on the occurrence of an event. For example, in the Fig.1'F' is the Gray hole attack whenever data is sent through this node 'F' will behave as good node but it may start behaving as malicious node at some particular time or on the occurrence of some event.

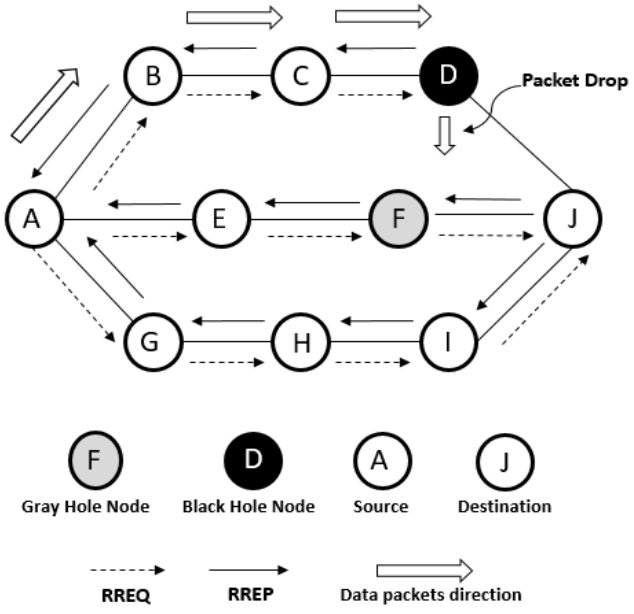

Fig. 1. Black hole and Gray hole node in the network.

Trust Model is considered as important aspect in providing secure transmission of data in MANETs. Trust is the reliability opinion held by one node (referred as evaluating node) about the other node whose Trust value is to be calculated (referred as evaluated node) in the network for secure transmission of data. There are two types of Trust: Direct and Indirect. Direct trust is the trust value calculated by an evaluating node for the node whose trust value is to be calculated based on pastbehavior experience e.g. successful delivery of data packets by the evaluated node in the network. Indirect trust is the trust calculated based on the aggregate values of the direct/Indirect Trust values calculated by other nodes in the network for an evaluated node.

II. BASIC MALICIOUS NODE DETECTION MECHANISM

Many methods have been developed to detect the malicious node in MANETs. These methods are categorized under either Proactive or Reactive defense strategy. In Proactive method, system regularly monitors the network to detect malicious node. This method detects the malicious node in its early stage as compared to Reactive strategy but requires comparatively large number of resources. While Reactive Defense strategy comes into action whenever there is significant drop in the packet delivery ratio. One of the method used in [1] to detect malicious node is that of selecting one neighbor node as bait and sends a fake RREQ to this neighbor node (bait) and if any node other than the bait node replies with RREP message, is detected as malicious node. Shortcoming of this approach is that it does not check the neighbor node before selecting it as bait. Another method used is based on the Trust model to provide the security in the network [2]. It uses dynamic recommendation selection method to filter out dishonest recommendation. It proposes clustering based technique accompanied with a deviation detectionto filter out unfair recommendations exchanged by nodes inthe network. Some of the method uses Trust model to evaluate the Trust value of a node based on the previous experience and recommendations by the nodes that know the evaluated node for a long time [3]. However, the exchange of recommendation is confined to their neighborhood. In [4] Trust model is developed which is integrated with the neighbor discovery process, this method provide security in the network by increasing the cooperation among the nodes in the network. This method like the previous one [3] exchanges recommendation only among the neighbors to avoid the traffic in the network. Various advantages of the AODV are allowing them to be deployed much rapidly at low cost in a variety of applications [5]. One of the method to detect Black hole attack uses Neural network to evaluate the trust and the analysis of routing table [5].This method is adopted from thetheory of small-world phenomenon (i.e. Six degrees of separation) to encourage cooperation between nodes.

III. DETECTING MALICIOUS NODES USING COOPERATIVE BAIT DETECTION APPROACH AND TRUST MODEL (CBDT)

This paper presents a feasible method referred asCooperative Bait Detection approach using Trust model (CBDT) to detect malicious node involved in Black hole and Gray hole attack. It detects malicious node both Black Hole and Gray hole node and add them into malicious node list to avoid them to be involved in data transmission. CBDT uses Bait technique to attract malicious node to get trapped. Once a malicious node replies for the bait RREQ, then CBDT starts Reverse tracing to identify the malicious node in the network. It uses both Proactive and Reactive defense strategies.

CBDT uses Trust Model in the following cases (1) to know the Trustworthiness of a node before selecting it as Bait (2) to check trustworthiness of all node in the route selected for sending data in communication.

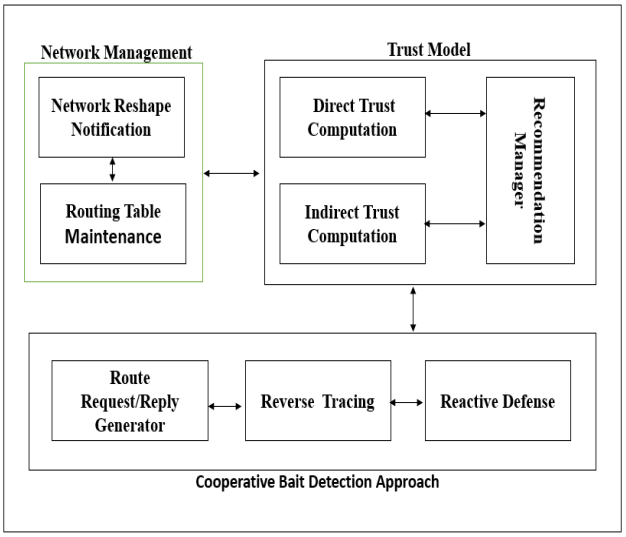

Fig. 2. Cooperative Bait Detection approach using Trust model (CBDT)

The CBDT involves the following major modules:

A. Network Management
B. Cooperative Bait Detection Approach
C. Trust Model

A. Network Management

In MANETs any node can join or leave the network, so to update the nodes about the new nodes that have joined the network and the nodes that have left the network Routing tables should be updated regularly. This paper uses the HELLO message of AODV protocol to inform each neighbor node about the nodes present in the network, so that each node can update their routing table.

B. Cooperative Bait Detection Approach

Cooperative Bait Detection Approach involves the following sub modules:

1) Route Request and Reply Generator
2) Reverse Tracing
3) Reactive Defense

1) Route Request and Reply Generator: Source Node generates a RREQ message to find the shortest path between itself and the destination, and broadcast RREQ to all its neighbor. Neighbors then broadcasts the request to their neighbors finally it reaches to the destination. Destination then sends a RREP message back to the source node. Any intermediate node that have the information about the shortest path, also send RREP message back to the source node.In the proposed method source node before sending the RREQ message, randomly selects one of its neighbor node as bait and broadcasts a fake RREQ in the network. If there is any malicious node in the network, it will reply with RREP message then system adds it into the malicious node list. When a malicious node is added into the malicious node list it is not used in sending the data.

2) Reverse Tracing: Reverse Tracing module trace out the malicious node detected in the bait step. Whenever source node sends a fake request to bait, source node already have information that there cannot be any other path shorter that the direct path between source node and the bait (neighbor node). Thus if any node replies with RREP for that fake RREQ then it is added in the malicious node list and reverse tracing module is activated to detect which node in the network have sent the RREP message to the source node.

3) Reactive Defense: Proposed method includes both proactive and reactive defense strategy. Aforementioned steps are included in the Proactive defense strategy. In Reactive defense strategy, system monitors the Packet drop ratio, if it decreases below the Threshold value then it starts the malicious node detection method to detect the malicious node in the network. Proposed method uses the reactive defense strategy that works according to (1) and (2):

$$CT_B = 1 - \frac{t_v}{t_r} \qquad (1)$$

Where:

t_v : Variation in expected data packets to be received from node *B*

t_r : Transmission Rate

If $CT_B < 0.7$ then calculate NT_B

$$NT_B = \frac{\alpha CT_B + \beta OT_B}{\alpha + \beta} \qquad (2)$$

Where:

NT_B : New trust value of node *B*,

OT_B : Old trust value of node *B*, initially $OT_B = 1$

α, β : α, β are constants and $\alpha + \beta = 1$.

If $NT_B < 0.5$ then include *B* in the malicious node list.

C. Trust Model

Trust Model involves the following sub modules

1) Direct Trust Computation
2) Indirect Trust Computation
3) Recommendation Manager

1) Direct Trust Computation: Direct trust is the trust value calculated by a node (evaluating node) for the node whose trust value is to be calculated (evaluated node) based on pastbehavior experience e.g. successful delivery of data packets by the evaluated node in the network. In the proposed method the direct trust value is taken initially as 1 i.e. all nodes in the network are considered initially as trustworthy nodes. Direct trust value is always accepted as true Trust value and is also free from dishonest recommendation from another malicious node in the network.

2) Indirect Trust Computation: Indirect trust is the trust which is calculated based on the recommendation/opinion sent by another node in the network. It is the aggregate value of the direct or indirect Trust values calculated by other nodes in the network about an evaluated node. When Source node receives RREP for the shortest path P between source and destination node, it starts sending the data packets. Simultaneously it broadcast opinion request in the network to know the trustworthiness of nodes in the path P selected for transmitting the data. If any node receiving opinion request and already have the calculated trust value for any node in the path P, then it replies the Source node with the calculated Trust value. Then it is processed by the recommendation manager to get the aggregate value for a particular node

3) Recommendation Manager: Recommendation Manager acts as an interface between Indirect trust computation module and the network. When a node X requests to know the opinion about a node Y. Recommendation Manager sends opinion/recommendation request to other nodes in the network to send the opinion/recommendation about Y. It then collects recommendation/opinion about Y from the nodes in the network and sends it to the Indirect trust computation module to get the aggregate trust value. After receiving the final trust value from Indirect trust calculation module, Recommendation Manager sends calculated trust value back to the node X which has requested the trust calculation for Y node in the network. Algorithm 1 Illustrates the working of recommendation manager module [2].

Algorithm 1: Recommendation Manager Algorithm

1. ***For*** each Opinion Request ***Do***
2. ***Send*** request to neighbours
3. ***Collect*** Opinion replies O_m , where O_m is opinion sent by node m
4. ***Construct*** the opinion list L={O_1, O_2,O_3,…,O_n}
5 ***Send*** L to the Indirect Trust Calculation Module for processing
6. ***Receive*** the Indirect Trust value 'ŧ' calculated afterpro-

cessing from the Indirect Trust Calculation Module.

7. ***Send*** 't' to the requested node

8. ***End For***

Recommendation manager sends the collected information (Opinions received) from the nodes to the indirect trust calculation module where indirect trust calculation module gives more weightage to the trust value received from the more trustworthy nodes and aggregate all the trust values and send them back to the recommendation module where it is sent back to the node that requested the recommendation.

IV. CONCLUSION

This paper presents a feasible method to detect malicious node involved in Black hole and Gray hole attack. The proposed method detects malicious node and add them into malicious node list thus avoiding them to be involved in data communication.

As a future work the method can be (1) used to develop simulation to analyze the performance of the proposed solution (2) enhanced to detect other type of attacks in MANETs or (3) merged with other security techniques to improve detection mechanism.

REFERENCES

[1]. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE Defending Against Collaborative Attacks by Malicious Nodes in MANETs:A Cooperative Bait Detection ApproachIEEESYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015

[2]. AntesarM. Shabut, KeshavDahal, and Irfan Awan Enhancing Dynamic Recommender Selection Using Multiple Rules for Trust andReputation Models in MANETs 2013 IEEE 25th International Conference on Tools with Artificial Intelligenc

[3]. Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle" Trust Management in Mobile Ad hoc NetworksUsing a Scalable Maturity-Based Model" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 7, NO. 3, SEPTEMBER 2010

[4]. Ms. SuganyaDevi.S, Dr.D. Thilagavathy, "NEIGHBOR NODE DISCOVERY AND TRUST PREDICTION IN MANETs" ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR)Volume 2, Issue 1, January 2013

[5]. Chandni Garg, Prashant Rewagade" Trust Evaluation for Detecting Black Hole Attack on AODV Routing Protocol by using Back Propagation Algorithm of Neural Network" Proc. of Int. Conf. on Advances in Computer Science and Application