Trust Based Solution To Packet Drop Attack In The MANET

Mr. Vishvas Haridas Kshirsagar
Department of Computer Engineering
Sinhgad Institute of Technology, Lonavala, Pune, India
Savitribai Phule Pune University, Pune, India
kshirsagar.vhk@gmail.com

Prof. Ashok M. Kanthe
Department of Computer Engineering
Sinhgad Institute of Technology, Lonavala, Pune, India
Savitribai Phule Pune University, Pune, India
ashokkanthe@gmail.com

***Abstract*— The Mobile Ad-hoc Network (MANET) is self-organizing communication network of the mobile node. The MANET does not have any prior structure of communication. The mobile ad hoc network creates a network with the help of intermediate nodes. The network is open network environment so that intermediate node can participate in the communication. The MANET has a serious security problem, because of the public nature of the network. The malicious node can quickly enter into the system. The security issue mainly contains a denial of service attacks like packet drop attack, black hole attack, gray hole attack, etc. The system based on receive and reply messages. It helps to generate mutual trust between neighboring nodes. This proposed algorithm works on trust based on removal of packet drop attack in MANET. This proposed algorithm implemented in Network Simulator 2.35. The concept of trust and energy is used for detection malicious node present the network. The power of node is used to differentiate between altruism and selfishness node. This work has proved with mathematical analysis of packet drop attack. The proposed algorithm formulates the packet drop problem of MANET with the help of continuous Bayes' theorem**

Keywords—Altruism, Continuous Bayes' Theorem, Mutual Trust, Mobile ad-hoc networks, Network simulator, Packet Drop Attack, Selfishness.

I. INTRODUCTION

The MANET is an autonomous network where all nodes are created, operated and managed by themselves [9, 10]. The MANET in which, all nodes are communicating on the basis of mutual trust between them. But some of the nodes are malicious; they are doing a malicious activity that cause degrading the performance of the network. The detection of the malicious node from the network is very difficult because of all nodes are necessary to communicate each other. In the MANET, devices are acts as autonomous nodes; the so malicious device can join the network at any time without any notification. The malicious node may misuse that needed information that is very harmful to the community.

The concept of trust is a subjective degree of belief about the behaviors of a particular entity, more ever "it is a belief about competence or honesty in a particular context [1]. Most widly used protocol in MANETs is the Ad-hoc on-demand distance vector (AODV) routing protocol. AODV is vulnerable to the well-known packet drop attack. It works on trust.

This paper is organized as follows. In Section II discusses the related work. Section III gives detail description of concept. Section IV provides a methodology for a packet drop attack mechanism. Section V describes an analytical approach towards detecting packet drop attacks in mobile ad hoc networks. Section VI describes the simulation and results analysis. Conclusion and future work in Section VI.

II. RELATED WORK

Ing-Ray Chen et al. proposed trust management in mobile ad-hoc network for bias minimization and application performance maximization [1], In which states that trust management mechanism in the MANET and its implementation to increase the performance. This approach is an integrated social and quality-of-service trust to improve the bias and performance.

Jin-Hee Cho et al proposed on the tradeoff between altruism and selfishness in MANET trust management [2], In which considered the tradeoff between a node's individual welfare vs. global well-being and identify the best design condition of this behavior model to balance to selfish vs. altruism behaviors.

Vishvas Kshirsagar, et al. proposed Analytical Approach towards Packet Drop Attack in Mobile Ad-hoc Networks [3]. This paper states the mathematical model of detection of an attack, also gives mathematical model proof with scenarios.

Md. Amir et al. proposed the mathematical model for the detection of selfish nodes in MANETs [4]. In this paper, proposed model works with existing routing protocol and suspected nodes are undergone selfishness test.

A. M. Kanthe et al. introduced the Impact of Packet Drop Attack and solution for the overall performance of AODV in mobile ad-hoc networks [5].

III. PACKET DROP ATTACK

MANET consist of various kinds of attacks such as black hole attack, gray hole attack, packet drop attack, these all are a denial of service attack [5]. In the black hole attack, a black hole node drops all the incoming packets by interpreting it as a valid shortest path. Ultimately destination node never receives any information from the source node. Hence, the performance of the network is compromised. In thpacket drop attack, attacker node drops all packets that are passing through it as similar to black hole node, but difference is that it is not attracting neighboring nodes to drop the packet [3, 5]. So there is no any co-operating packet drop attack happens in the MANET. Figure 1 represents the packet drop attack in the MANET.

In the packet drop attack, as malicious node does not attract neighboring nodes to drop the packet, so it is less harmful to network than black hole attack [5]. In the packet drop attack malicious node purposefully attract the packets towards it and drop them to decrease the performance of networks. Packet Droppers are the malicious node that drops the packets routing through them.

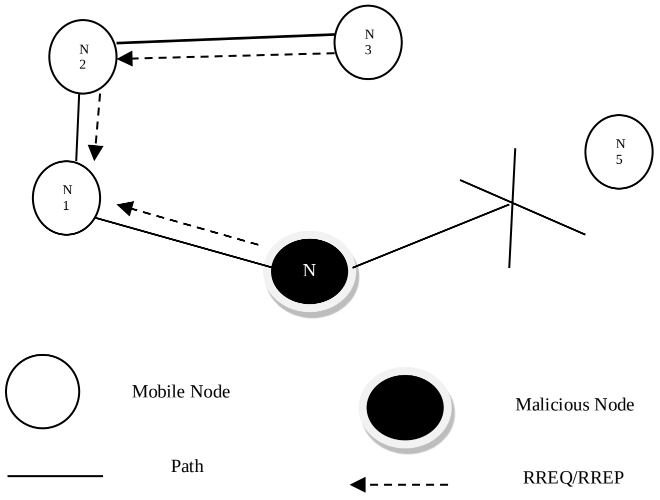

Fig. 1. Packet Drop Attack [3]

The proposed work gives the detection technique of packet dropper node (Malicious Node) in MANET using Bayes' theorem.

IV. PROPOSED METHODOLOGY

Their nodes are presented which dropping the packets. Identification of these nodes whether they are dropping packets due to energy consumption or purposefully. On this conclusion here consider two factors one is 'trust' and other is 'energy'. Trust is mutual understanding between different nodes present in the MANET. Trust is used to identify the malicious node or not. The trust management in the MANET is like usually RREQ and RREP message passing between nodes. The energy is used to distinguish between altruism and selfish node.

A. TRUST:

The mobile ad hoc network, trust is an imperative factor for seamless communication. The trust is used to create trusted list, and it can be use for communication. The source can communicate with the destination node by picking nodes from trusted list. So this communication is trusted communication. It minimizes the overhead of detecting malicious activity in the network and removal of it. But trust is generated with the help of RREQ and RREP message passing between nodes. Generation of trust in the network, it undergoes send and receive process. The serious problem is while generating trust node may go into sleep mode due to inefficient energy. If any node goes into sleep mode due to the inefficient power, it will push into blacklisted node even though it is not a malicious node. To overcome this problem, another concept is used.

B. ENERGY:

To differentiate between altruism and selfish node, we can use energy model. While generating trust in which node has not replied due to inefficient power. That node goes into a black list that is not entered into trusted list even though it is not a malicious node. The selfish node does not participate in the communication process; it decreases the performance of the network. Distinguish between altruism and the selfish node is done with the help of energy model. This model calculates the energy of each node, on that classifies lower energy node and higher energy node. If any node is not replied for RREQ there also calculate energy, then it cannot add to the blacklist even though it not replied. It helps to distinguish between altruism and selfish node.

C. ALGORITHM FOR CREATING TRUST LIST TO DETECT PACKET DROP ATTACK:

```
[Initialization E (Energy Level) and T (Trust Level) to 0]
Step 1 Start (send RREQ to each neighboring node)
Step 2 Check if reply from node
        If yes goto step 3
        If no goto step 9
Step 3: Add details of replying node into routing table
        If rt=rtable.rt_lookup(rp->rp_dst)
        If yes T=T + 0.1 and E=received E
            If T > 1 then T=1
        If no T=0.5 and E=received E
Step 4 Check if replying node is in the trust list
        If yes check E < 20 then remove from trust list
        If no goto step 5
Step 5  Check replying node T and E values
          If T > 0.5 && E > 20 Add to trust List and
           reliable = 1
        If no goto step 6
Step 6: Reset the reliable flag
```

```
            reliable = 0
    Step 7: Check if replying node is final destination node
            If yes do not add node to trust list
            If no goto step 8
    Step 8: Execute rests part of  receivreply function
    Step 9: Stop
```

This algorithm creates the trusted list. The generated trusted list contains only trusted and working energy level nodes are available. It helps to identify the selfish nodes and altruism nodes of the networks. This trust list is stored in local RAM of each node.

V. ANALYTICAL APPROACH FOR PACKET DROP ATTACK

The trust list helps to detect the malicious activity of the network and also differentiate between an altruism and selfishness nodes that avoid getting blacklisted because of the energy level of nodes. Each node maintains a list, in the local buffer that contains the list of trusted and un-trusted nodes.

The trusted list is used to detect malicious node. The overhead is reduced with the help of the trusted list as there is no need to analyze the nodes in the trusted list.

Each node maintains the trusted list as its data structure in its local buffer.

In a direct reputation method, the two counters, total forwarded packets and total dropped packets of the replying nodes are used.

A. *Mathematical model for detecting packet drop attack:*

This approach gives a simple mathematical model with the help of existing routing protocols of MANET, which will be able to identify the packet dropper node using probability.

The Bayes' theorem [6] expresses how a subjective degree of belief should rationally change to account for the evidence. Here assume that each node maintains their local records of trusted and un-trusted node list, so as to find whether network contains malicious node or not based on trusted and un-trusted list [3]. If there are more un-trusted nodes than trusted node, it states that there will be poor performance of the network.

In Ad-hoc Networks, each node maintaining the trusted list in their local memory, on this information calculate the probability of trusted and un-trusted node present in the network.

Let,

S: Event that node is trusted

$\bar{S}$: Event that node is un-trusted

Pos: Event that node test is positive or negative

By using Bayes' theorem [6, 3],

$$P\ (S\ |\text{Pos}) = \frac{P(S)P(\text{Pos}|S)}{P(S)P(\text{Pos}|S)+P(\bar{S})P(\text{Pos}|\bar{S})} \ldots\ldots\ldots\ldots\ldots\ldots \text{(1) [3]}$$

P(S | Pos) gives the probability of performance of the network based on trusted and un-trusted nodes in the network. This model applies to each node by considering some trusted node and the un-trusted node that is stored in local RAM of the node. If the result is greater than 0.5, the node is not malicious.

Probability shows the possibility of the particular event is present or not, so fifty percentages may be possible, or fifty percentages may not, so consideration is 0.5 as a benchmark reading [4, 6].

VI. SIMULATION AND ANALYSIS

The proposed algorithm is implemented in Network Simulator (NS-2). NS-2 is open source network simulation tool. The 802.11 MAC layer implemented in ns-2 is use for simulation. The protocol used is AODV. The various parameters are considered to compare the results.

Table 1: Scenario for Mathematical Model

PARAMETER	USED IN SIMULATION
Channel Type	Channel/Wireless Channel
Antenna type	Omnidirectional
Radio propagation model	Two-ray ground
Link Layer type	LL
MAC type	IEEE 802.11
Protocol for simulation	AODV
Number of packets	50
Number of nodes	30
Simulation time	100 second
Pause time	0.07 second
Area(meter square)	300*300 m^2

Table 1 shows the simulation parameters that are used in the simulation. The network simulator helps to take values for generating simulation parameters, on which can be analysis the performance of the network. Figure 2 to 4, x-axis represents the pause time and y-axis represents throughput, delay, and energy respectively. All graphs in which, blue lines shows that network in normal environment, the red line shows parameters under attack and the green lines shows after solution applied over packet drop attack.

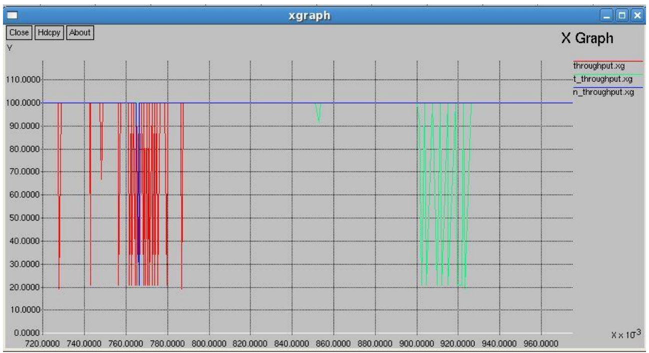

Figure 2 Throughput Vs. Pause time

Figure 2 shows the graphs generated between the throughput and the pause time. Figure 2 shows that when the attack occurs in the network the throughput minimized as compared to the performance in the under attack scenario. After applying the solution to packet drop attack from the network, the throughput is improved.

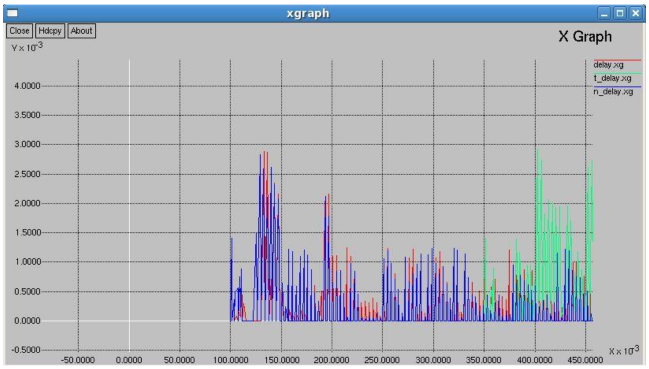

Figure 3 Delay Vs. Pause time (second)

Figure 3 shows delay versus puase time. Figure 3 shows, when the network is under attack, the packet delivery ratio decreases as compared. When the gray hole is detected and removed from the network, the delay is minimum.

Figure 4 shows the performance of the network in terms of energy. Figure 4 represents the variation of energy with respect to pause time. The figure shows that the energy of the nodes decreases as the network is under attack because the malicious nodes are dropping the packets passing through it and by processing more packets.

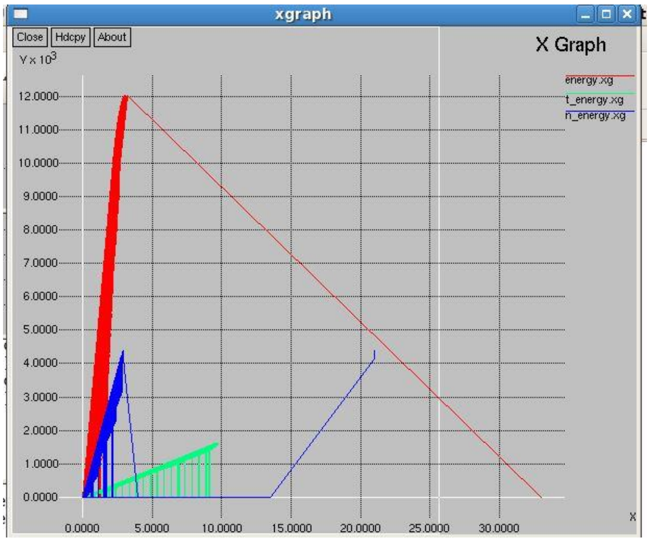

Figure 4 Energy Vs. Pause time

VII. CONCLUSION

The trust list helps to detect the malicious activity of the network and also differentiate between an altruism and selfishness nodes that avoid getting blacklisted because of the energy level of nodes. Each node maintains a list, in the local buffer that contains the list of trusted and un-trusted nodes. This help to detect malicious node and also differentiate between altruism and selfishness node.

Acknowledgment

We would like to thanks, Prof. Ashok M. Kanthe for supporting the research work. Prof. A. M. Kanthe is a cooperation and mobility program in the field of higher education.

REFERENCES

[1] AbIng-Ray Chen, Jia Guo, Fenye Bao, Jin-Hee Cho, Trust management in mobile ad hoc networks for bias minimization and application performance maximization. Elsevier B. V Journal with ISSN:1570-8705, 2014

[2] Jin-Hee Cho, Ing-Ray Chen, On the tradeoff between altruism and selfishness in MANET. Elsevier B. V Journal with ISSN:2217-2234, 2013

[3] Vishvas Kshirsagar, Ashok M. Kanthe, Dina Simunic, “Analytical Approach towards Packet Drop Attack in Mobile Ad-hoc Networks.” IEEE ICCIC 2014,

[4] Md. Amir KhusruAkhtar, G. Sahoo, "Mathematical Model for the Detection of Selfish Nodes in MANET" IJCSI, 2010 ISSN 2231 –5292,

[5] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "The Impact of Packet Drop Attack and Solution on overall Performance of AODV in Mobile Ad-hoc Networks" IJRTE, ISSN: 2249-8958, Volume-2, December-2012.

[6] Sheldon Ross, “A first Course in Probability”, Eighth Edition, Prentice Hall., 2002.

[7] Andrew Gelman, "Prior distribution", Volume 3, pp 16341637, Encyclopedia of Environ metrics (ISBN 0471 899976), 2002

[8] C.Perkins, E.B. Royer, S.Das, Ad hoc On-Demand Distance Vector Routing, Proceeding of the 2nd IEEE Workshops on Mobile Computing System and Applications(WMCSA),pp.90-100,1999.

[9] C. Perkins, E. B. Royer and S. Das, “Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft”, RFC 3561, IETF Network Working Group, July 2003.

[10] R. Prasad, S. Dixit, R Van Nee, “Globalization of Mobile and Wireless Communication” March 2011, Springer, P 335

[11] L. Gavrilovska, R. Prasad, Ad-hoc Networking Towards Seamless Communications” Springer 2006, p. 284.

[12] Andrew Gelman, "Prior distribution", Volume 3, pp 16341637, Encyclopedia of Environ metrics (ISBN 0471 899976), 2002

[13] Md. Amir Khusru Akhtar, V. S. Shankar Sriman, G. Sahoo, "A Methodology to overcome Selfish Node attack in MANET", Knowledge Management and E-learning: An International Journal, Serial Publication-2009.