Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Probabilistic Analysis Approach for Reliable Transmission in MANET

Manupriya
M.tech student,
Vaish college of Engg, MDU, Rohtak
India

Sangeeta Malik
Asst. Professor
Vaish college of Engg, MDU, Rohtak
India

Abstract—A Mobile network always suffer from internal and external security flaws because of its public access as well as provides high degree of communication over the network. One of such threat is the node failure over the network. The node failure can occur because of congestion or Man in middle Attack. In this paper, a probabilistic analysis approach is defined to identify the bad node over the network as well to identify the Safe path over the network. The probabilistic solution presented here is parametric analysis where a conditional decision is taken by taking the load as main decision vector and the secondary vectors are throughput, delay. A heavy load route is critical if the probabilistic throughput value is closer to zero. The work is implemented in NS2 environment, Obtained results shows the effective throughput and the lesser loss rate.

Keywords- Probabilistic Analysis, Muti-Decision Vector, Conditional Analysis, Load

1. INTRODUCTION

Mobile network is not new network architecture but even then it is more permissible research area because of its unlimited use and the growth. The use of Mobile network is been increased with the extension of new communication medium, communication technologies like 3G, $G etc. As the scope and use of the network is been increased, in same ratio the threats in such network are also increasing day by day. A Mobile network is busy network with lot of communicating users in parallel. Because of this network always suffer from some kind of internal or the external attack over the network. Some of the common problems and the threats suffered by mobile network [1]

The attacks in mobile networks are divided in two broad categories called Active and the passive Attacks. The active attack is about the misbehaving node over the network that damages the communication and in result the link failure and the data loss occur over the network. Whereas the passive attack does not damage a node or the network but they utilize the network selfishly to get the major access of bandwidth. These two kinds of attacks are further classified under number of other attacks defined in same section [2]. One of the crucial attacks in mobile network is DOS (Denial of Service) attack. The attacker can be a internal or external user that prevent the main user to access the required resources effectively. They either perform the authenticated access to the resources or increase the traffic over the network so that the resource access efficiency is degraded. Flooding is a type of DOS attack that increase the network traffic extensively with unnecessary communication [3,4,5].

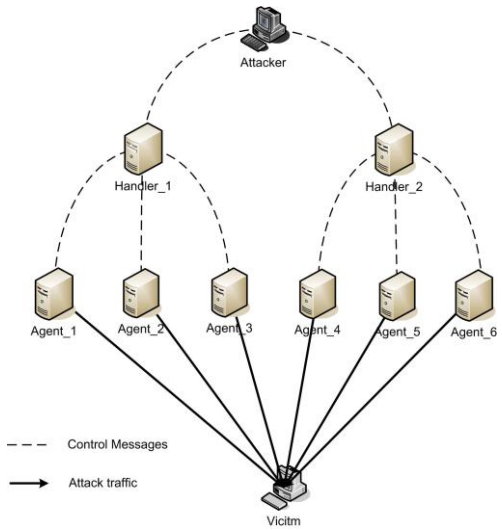

Figure 1: DOS Attack

Here Figure 1 is showing the basic architecture followed by DOS attack. A DoS (Denial-Of-Service) attack is a large-scale attempt by malicious users to flood the victim network with a massive number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. The task of deploying these attack agents requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the control Handler program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control Handler program, the real attacker can stay behind the scenes of the attack [15]. Flood attack basically causes the system crash, slow down the communication and switches the network to saturated form. Another category of DOS attack is the Bandwidth depletion attack, it is also the flood attack but it is basically done by targeting a specific user. All the channels available to the victim are flooded by the attacker so that the victim communication is degraded or blocked [6,7].

Blackhole is another power attack in which a malicious node presents itself as a valid node and direct the communication in that direction. Blackhole attack does not forward the packets and broadcast the fake information about its own identity. These nodes provide the fake information transition over the network so that heavy data loss occurred. To succeed a black hole attack, malicious node should be situated at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. Rushing attack is another series attack that occurs generates a two end tunnel in a network. It propagates the fast and large communication within the tunnel so that the rest communication over the network is degraded and slow down. The rushing attack at lower level work as the DOS attack and degrade the communication over the network [8,9,16].

2. Existing Work

Bo Wang develops a method to distinguish bad nodes over the network by performing the analysis on peers from cooperative ones as well as solely. The author has defined local observations on AODV protocol to analyze its behavior. In this presented approach, a finite machine model to define the AODV based implementation. Author has applied a series of statistical tests to perform the feature based analysis on the neighboring nodes and to identify the selfish node over the networks [1]. Jamal N Al Karaki to identify the bad node over the network. The author has defect a cooperative analysis approach to detect the bad node over the network [2]. Alberto Rodriguez-Mayol has defined and evaluates two main techniques to improve the communication and ability to detect the selfish node. Author defined a watch dog mechanism to perform the detection of bad nodes over the network. The author basically proposed a preventive mechanism for safe communication over the network [3]. T. Jaya has defined a reconfiguration approach to perform the safe communication in case of link failure over the network. The author presented an approach to perform the efficient transmission as well as provide the recovery over the transmitting node effectively [4]. Anuj Joshi defined a work on efficient content authentication method in ad hoc network. The challenges in ad hoc networks are defined in this paper. The paper defined secure packet forwarding and provides a new solution by performing the observation to provide the neighboring node analysis over the network [5]. S.Lakshmi present an adaptive selfish aware queue scheduler for a M/M/1 and M/M/n queuing mechanism to schedule the packets for selfish nodes in mobile ad-hoc networks using AODV as the routing protocol[6]. Another author presented a Leader election approach to provide the node for intrusion detection in Mobile Ad Hoc Networks (MANETs). The author has defined the resource consumption all the nodes, the most cost-efficient to perform the analysis for the energy level and to perform the election of best suitable node for the communication [7].

Djamel Djenouri propose in this paper a novel cross-layer based approach to detect data packet droppers, that Author optimize and decrease its overhead. Contrary to all the current detective solutions, ours is applicable regardless of the power control technique employment [8]. Hadi Otrok Address the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster [9]. K. Paul Detect a large range of attacks on Dynamic Source Routing (DSR) protocol. Authors provide a low-cost mechanism informing other nodes of the system about the accused and provide an inference scheme to blame the accused and malicious accuser without doubt [10]. Hanif S. Kazemi presents the design and implementation of a distributed network monitoring system for MANETs. Presented system is completely distributed, generates no additional traffic on the network and produces a dynamic picture of the network level and node level information on a graphical user interface. In Presented proposed scheme, multiple monitoring nodes collaborate to achieve a reasonably accurate snapshot of the network conditions [11]. In Year 2012, Raman Singh, Amandeep Verma performed a work, "A Dynamic Bandwidth Assignment Approach under DDoS Flood Attack". In this work Three experiments are performed. First experiment shows the performance analysis of drop tail queue which is widely used in routers. In the second experiment proposed approach of dividing users in to two groups of genuine users and malicious users and then assign high bandwidth to genuine users and low bandwidth to malicious users is performed. In the third experiment a formula for dynamic bandwidth assignment is derived [12]. Prajeet Sharma, Niresh Sharma, Rajdeep Singh performed a work "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network". The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably [13]. In Year 2013, Mohan K Mali1, Pramod A Jadhav performed a work, "Review of DDoS and Flooding Attacks in MANET". In this work, introduction of dynamic counter-based broadcast technique for detecting and

controlling flooding attack, average distance estimation technique for detecting and rate limiting technique for controlling DDoS attack [14].

3. PROPOSED WORK

In this present work, we have defined a two way probabilistic analysis model to analyze the neighbor nodes under the probabilistic vectors. These vectors are defined in two major domains first vector is the connectivity vector used to identify the possible connectivities with the neighboring nodes. Once these connectivities are obtained, a probabilistic ratio is driven respective to the load on each neighboring node. Based on this load analysis, the aggregative load decision is taken. Now this individual load analysis and the aggregative load will work as the primary vector to take the probabilistic decision.

At the second level of this work, the current node and the neighboring nodes are been analyzed under the different analysis vectors. In this work we have taken two main vectors called throughput and the delay. Now the probabilistic decisions of these parameters are drawn with effect of primary parameter called load. This parameter is drawn respective to the aggregative as well as the individual load vector. Once these all vectors are defined, the node with lowest probabilistic loss value and minimum delay value will be selected as the next communicating nodes. In the same way, the node having the maximum probabilistic loss and the maximum probabilistic delay will be taken as the bad node. The communication over this node will be terminated temporarily for the current session. In this work we have defined the nodes with energy vector also. As some communication is performed over a node, some amount of Energy gets lost over that node. Because of this node start losing data and after some time node becomes dead.

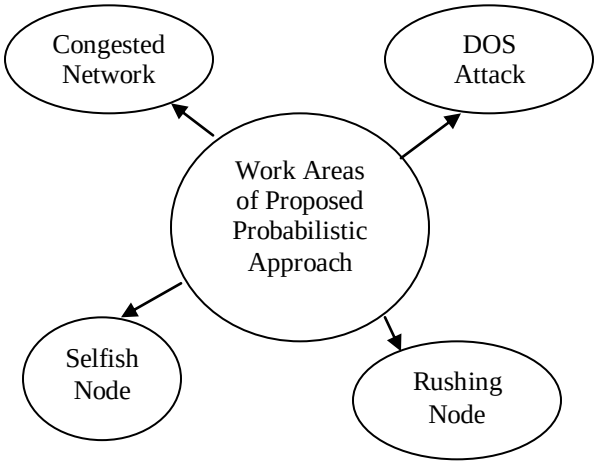

Figure 2: Work Area of Proposed Approach

Work area of presented approach is shown in figure 2. The presented work is effective enough in case of congested network as well as where some congestion oriented attack is there. The presented work will work for the following cases.

A) Algorithm

Algorithm (Nodes,N)
{
(i) Design a network with N number of nodes and with specific constraints like energy, position etc.
(ii) Define the source and the destination node
(iii) Perform the communication between source and Destination
(iv) Set Source and CNode and perform the communication
(v) While CNode <> Destination
(vi) {
(vii) Generate the List of NeighborNode called NList
(viii) Set Count=0
(ix) Set ALoad=0
(x) For i=1 to Length(NList)
(xi) {
(xii) If (Communication(I,CNode)<>0)
(xiii) {
(xiv) Count = Count+1
(xv) ALoad=ALoad+Throughput(I,CNode);
(xvi) }
(xvii) }

(xviii) For i=1 to Length(NList)
(xix) {
(xx) Get Throughput and Delay on each neighbor Node
(xxi) TRatio=Throughput(NList(i))/Count
(xxii) DRatio=Delay(NList(i))/Count
(xxiii) ATRatio=Throughput(NList(j))/ALoad
(xxiv) ADRatio=Delay(NList(j))/ALoad
(xxv) }
(xxvi) Find the Neighbor Node with Minimum TRatio, DRatio, ATRatio, ADRatio called node j
(xxvii) Set j as CurNode
(xxviii) }

4. RESULTS

The presented work is implemented in NS2 environment. The simulation is performed under a Mobile Network Scenario. The Scenario taken for the work is shown as under in table 1.

Table 1: Simulation Parameters

Parameters	Values
Number of Nodes	50
Area	500x500
Protocol	AODV
Interval	.01
Traffic Type	CBR
Antenna Type	Omni Antenna
Simulation Time	15 sec

The scenario is 50 nodes that are distributed randomly in a work area of 500x500

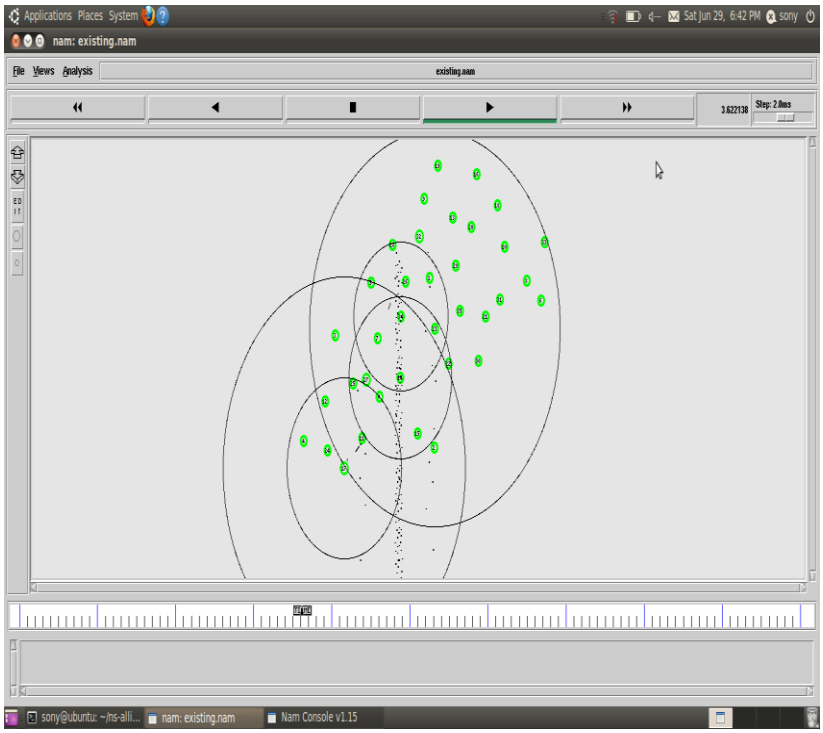

Figure 3: Packet Loss

Here Figure 3 is showing the Packet loss over the network. These bad nodes do not allow passing data to the next nodes and dropping all the packets.
The analysis of the work is performed under two main parameters called packet transmitted and packet lost

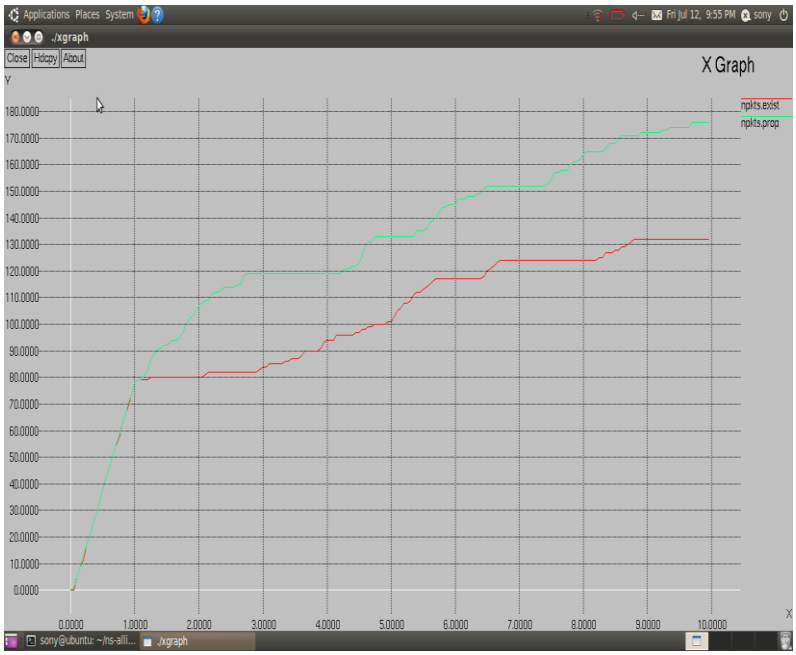

Figure 4: Throughput Analysis

Here Figure 4 is showing the comparison of proposed work with existing protocol transmission under the heavy traffic. As we can see, the green line is showing the packet transmission in case of proposed work and red line is showing the throughput in existing approach. X axis is showing the simulation time. As we observe that the proposed work has improved the throughput up to an extent.

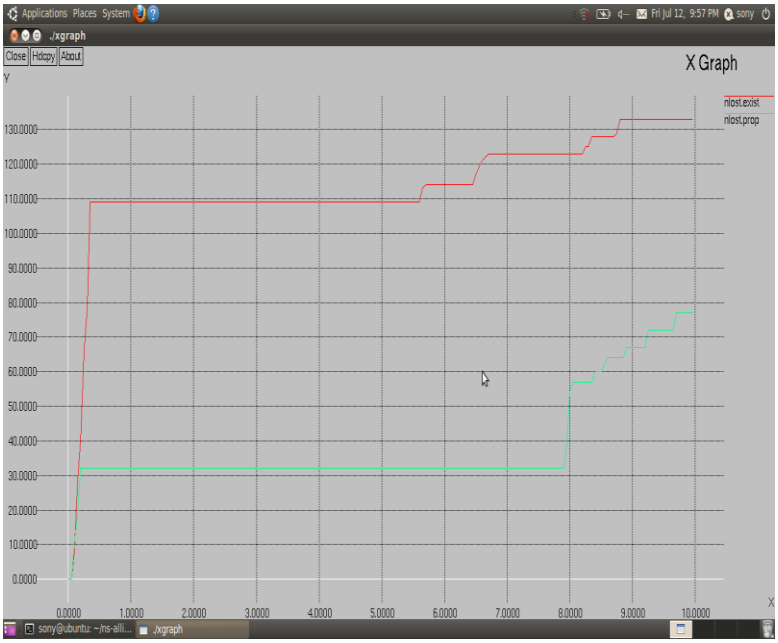

Figure 5: Packet Loss Analysis

Here Figure 5 is showing the comparison of proposed work with existing protocol under the heavy traffic. As we can see, the green line is showing the packet loss in case of proposed work and red line is showing the throughput in existing approach. X axis is showing the simulation time. As we observe that the proposed work has reduced the communication loss over the network.

5. Conclusion

In this paper, A probabilistic analysis approach is been presented to perform the reliable communication over the network. The presented approach has divided the analysis parameters in two levels called primary and secondary vector. The secondary vector is here analyzed under the primary vector. The obtained result shows that the work has improved the network throughput and reduced the loss rate.

Acknowledgement

Authors are highly thankful to the Principal, VCE, Rohtak, for providing this opportunity to carry out the present thesis work. The constant supervision and support received from the coordinator of Department has been of great help for carrying out this work and is acknowledged with reverential thanks.

REFERENCES

[1] Bo Wang,"Distributed Detection of Selfish Routing in Wireless Mesh Networks".

[2] Jamal N. Al-Karaki,"Stimulating Node Cooperation in Mobile adhoc Networks", Wireless. Pers Commun vol. 44, pp(219-239),2008

[3] Alberto Rodriguez-Mayol,"Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile adhoc Networks", Personal Indoor and Mobile Radio Communications ,IEEE 21st International Symposium on 26-30 Sept. 2010

[4] T.jaya,"Detection of selfish nodes in Wireless mesh networks using Hierarchial clustering", International Conference on Computing and Control Engineering ,2012.

[5] Anuj Joshi, "Efficient Content Authentication in Ad hoc Networks- Mitigating DDoS Attacks", International Journal of Computer Applications, pp (0975 – 8887) ,june 2011.

[6] S.Lakshmi, " Design And Analysis Of An Adaptive Selfish Scheduling Algorithm Using AODV Protocol In MANET", Indian Journal of Computer Science and Engineering (IJCSE) ,vol. 3 no.3, pp (428-435), ISSN : 0976-5166, Jun-Jul 2012.

[7] Alireza Shahrbanoonezhad, " A Hybrid System for Detecting Misbehaving Nodes in Ad Hoc Networks", International Journal of Information and Electronics Engineering, vol. 2, no. 3, May 2012**.**

[8] Djamel Djenouri, "Struggling Against Selfishness and Black Hole Attacks in MANETs", vol. 8, Issue-6, pp(689-704), August2008.

[9] Hadi Otrok,"A game-theoretic intrusion detection model for mobile adhoc networks", Journal of Computer Communications, 31(4):pp(708 – 721), 2008.

[10] K. Paul, "Context Aware Detection of Selfish Nodes in DSR based adhoc Networks", Global Telecommunications Conference, IEEE, vol.1**,**pp(178-182), 2002.

[11] Hanif S. Kazemi, "Distributed Monitoring System for Mobile Ad Hoc Networks: Design and Implementation.

[12] Raman Singh, Amandeep Verma, "A Dynamic Bandwidth Assignment Approach under DDoS Flood Attack" journal of advances in information technology, vol. 3, no. 2, may 2012.

[13] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.

[14] Mohan K Mali, Pramod A Jadhav, "Review of DDoS and Flooding Attacks in MANET" International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013.

[15] Gaurav Kumar Gupta, Mr. Jitendra Singh, "Truth of D DoS Attacks in MANET" Global Journal of Computer Science and Technology Vol. 10 Issue 15 (Ver. 1.0) December 2010.

[16] Kamini Maheshwar; Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment" European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-9.

