AN EFFECTIVE ATTACK PREVENTING ROUTING APPROACH IN SPEED NETWORK IN MANETS

Bhupender[1], Gopal Singh[2]

[1]Student, M.Tech, Dept of Computer Sc. & App., MDU, Rohtak, Haryana
[2]Asstt. Professor, Dept of Computer Sc. & App., MDU, Rohtak, Haryana

Abstract

A Speed Network is specialized mobile network in which mobile nodes are defined with mobility. QoS Optimized Routing is challenge in such type of network. The criticality of network increases, when the network is infected with some attack. In this present work, a predictive routing approach is defined for Speed Network. The prediction is here performed to observe the node mobility so that effective routing will be performed. Once the mobility is predicted, the communication analysis is performed to generate the effective route for communication. The obtained results shows the reduction in communication loss and network delay.

Keywords: *MANET, Speed Network, Predictive Routing, QoS*

---***---

1. INTRODUCTION

A Mobile Network is defined as the collection of vast number of mobile users and a Mobile Ad-Hoc Network (MANET) is defined as a collection of wireless mobile nodes forming a temporary network without using any centralized access point or administration .In this type of speed network to perform the equalize communication, the bandwidth estimated communication is required. Mobile network is a decentralized communication network with topology specification so that the routing functionality over the network will be improved. These kind of network are defined with the specification of mobile nodes. The nodes generates the path by generating the forwarding message[2,3].

There are number of indoor and outdoor applications of mobile network respective to size and the communication form in the network. These network types includes the small scale, large scale, static and dynamic network. The network design depends on the network protocols so that the network issues will be reduced and the communication will be effective over the network. These network types includes the network organization, link management and routing in effective way. The network is defined under different concerns such as security, latency etc. The environmental and the communication vectors are available that affects the network communication and the performance [6].

Mobile network suffers different kind of networks because of its cooperative communication. These attacks can be categorized respective to the type of attacker or based on the type of attack. In this section, the various categorization of network attacks are discussed[9].

1.1 External and Internal Attack

As the name suggests, the external attack is performed by the some external node that is not part of network itself. These kind of attack is performed by sending the fake packets over the network and by increasing the network load. The nodes suffers from different kind of attacks and to avoid these attacks some centralized mechanism can be implemented over the network such as firewall. The firewall is defined as the restricted constraint to obtain the un authorized access over the network. Another kind of critical attack in mobile network is performed by the network nodes itself. This kind of attack is performed to gain the network access or the service access so that that more network benefits will be obtained. The information extraction of other network nodes is also the reason for generation of these kinds of attacks. The attacker gain the access to the network and provide the compromised communication over the network[9].

1.2 Active and Passive Attack

According to the type of attack or the motive of the attack, the attacks are divided in two main categories called passive and active attacks. The active attacks can be performed by some internal or external nodes to disturb the network performance. These kind of attacks are performed to hijack the information or to inject the communicating packets with some fake information. These kind of attacks includes the attacker position analysis so that the network operations will be disturb and the network operations will be captured. Whereas the passive attacks just extract the network information and does not attacks the actual communicating data. This kind of attack is generally performed by some internal nodes. The man in middle attack is such kind of attack. [10].

In this paper, an optimized routing approach is defined for attacked speed network. Network is here suffered from packet dropping attack. In this section, the mobile network is defined along with security constraints and attack forms over the network. In section II, the work defined by earlier researchers to provide effective routing in attack network. In section III, the effective routing approach is presented along with algorithmic approach. In section IV, the results obtained from the work are discussed. In section V, the conclusion obtained from the work is presented.

2. EXISTING WORK

In this paper, the work defined by the earlier researchers is presented an discussed. Peter J. J. McNerney[2] has defined a work on optimization of mobile network under different issues. Author attempted to address these two issues together by proposing a 2-Dimensional Adaptation Architecture (2-DAARC) for achieving QoS in MANETs containing blackhole attackers. The architecture supports two forms of adaptation: single-path adaptation (SPA) and multi-path adaptation (MPA). The architecture is evaluated against the INSIGNIA QoS framework, which uses a single-path bandwidth adaptation approach. Enrique Hernández-Orallo[3] has defined a collaborative approach for identification approach using Mobile network. Author has defined a collaborative communication analysis to avoid the selfish node attack. Author presented the analysis over the network nodes by applying the watchdog over the network nodes. Author performed the analytical study over the network so that the network communication overhead. Kevin A. Li[4] has defined a detection and notification approach of Buddy Proximity in Mobile phones. Author has presented a application based analysis over the network to improve the network communication. The network has defined the effective analysis on the noise and power consumption analysis so that the network effectiveness will be improved. M.Shobana[5] has defined a geometric routing approach under black hole attack analysis. The paper has included the node communication associatively analysis to provide the effective communication. Author improved the protocol and achieve the safe communication over the network. Ítalo Cunha[6] has presented a measure method analysis under fast and accurate blackhole identification with binary tomography. Author has defined a path based probing technique to reduce the communication loss and to improve the data rate over the network.

Poonam[7] has defined a node detection approach for trust evaluation based model for misbehaving node detection. Author presented a trust aware routing over the mobile network to reduce the forwarding attack over the network. Author defined the node behavior analysis so that the trustful communication will be obtained. Xueying Zhang[8] has defined a study on security features in cognitive networks. Author has defined a security system to ensure the communication security by monitoring the network parts under specific communication parameters and specialized characteristics. Piyush Agarwal[9] has presented a copperative attack analysis approach in case of blackhole and gray hole attacks. Author defined a controlled and collaborative communication approach to avoid the data disruption along with block communication analysis in mobile network. S Madhavi[10] has presented a study on different kind of attacks in case of AODV and MAODV protocols. Author discussed different associated issues in mobile network. Author provided a study again different network attacks. These attacks includes the routing attacks and the communication over the network. Alberto Medina[11] has defined measurement interaction approach for effective communication evaluation in mobile network. Author has presented the effective network evolution to provide the effective end to end communication over the network. Author analyze the network under different communication parameters and different network operations to obtain the route discovery. Author performed the analysis again the congestion and the network attacks. Author provided the measurement against different attacks. The work is presented in the form of a framework to obtain the effective communication through web servers.

Yunyue Zhu[12] has defined a elastic burst detection approach in data streams. Author defined a data structure based analysis to provide the aggregative communication in window analysis approach. Author performed the direct computation against magnitude analysis and to provide the window analysis based communication over the network. Author has reduce the data loss for communication. Kamaljit Kaur[13] has defined black hole attack in cloud network in AODV and DSDV protocols. Author has presented a comparative analysis on different network protocols to provide safe communication over the network. Author has performed the network evaluation under attack analysis so that the attack impact will be observed. Chris Grier[14] has defined comparative analysis for compromised network service. Author has provided a service model to provide the compromise communication over the network. Author has provided the network malware analysis to provide the web communication under emergency services. Author performed the traffic analysis over the network. Rajesh Yerneni[15] has defined defined an effective performance measure approach for AODV network against blackhole attack. Author has provided the safe communication for secure AODV protocol. Author has reduce the network attack and provide the safe communication under random value analysis. Author has performed the safe packet delivery under the blackhole attack. Damianos Gavalas [16] Mobility of nodes may affect the service oriented aspects as well as the application-oriented aspects of ad hoc networking. At the network level, accurate node mobility prediction may be critical to tasks such as call admission control, reservation of network resources, pre-configuration of services and QoS provisioning. At the application level, user mobility prediction in combination with user's profile may provide the user with enhanced location-based wireless services, such as route guidance, local traffic information and on-line advertising. Divya Bharti[17] make the of different protocols (AODV/DSR) for the performance analysis of their proposed mobility control scheme and the impact of this method over the selected protocols. They analyzed the performance of the protocols on the basis of different parameters like Throughput, Packet Delivery Ratio, Routing Load etc.

3. PROPOSED WORK

In this present work, an effective routing approach is defined in attack speed network. The work is defined against the packet dropping attack. In this attack, the intermediate node does not work effectively and perform the data loss while forwarding the nodes. As the work is a speed network, the complete work is divided in two main stages. In first stage, the speed analysis over the network is performed. The speed analysis includes the identification of direction and mobility ratio of the network. To perform the mobility estimation, the positional analysis is performed on two time frames. The node movement analysis is performed for these time frames and based on these, the speed and direction of nodes is identified. Once the node physical attributes are collected, the next work is to perform the effective route over the network. The work is to provide the secure communication over the network. To perform this, the neighbor node analysis is performed under communication parameters that are speed, direction ,loss rate and delay. And the whole research process will work as follows:

1. Establish the Mobile Network.
2. Modify the node parameters with inclusion of speed and directional aspects.
3. Specify the source and destination nodes.
4. Set source as current node and identify the feasible nodes under velocity and communication parameters.
5. Identify the node with least mobility and effective distance and set as feasible nodes.
6. Analyze the feasible nodes under the loss and delay analysis.
7. Identify the best node from neighbor list and set as current node.
8. Repeat the process till destination node not arrived.

Based on this initial communication analysis, the effective next neighbour is elected for the communication. The algorithmic approach for the identification of speed and direction of nodes in table 1.

Table 1: Neighbor Node Identification

```
NeighborNodeAnalysis(Nodes,N)
/*Nodes is the List of N Mobiles in Network*/
{
1.    Define the Source Node Src Respective to Which Position Analysis is Performed
2.    For i=1 to N
      [Process All Nodes]
      {
3.        P1=GetPosition(Nodes(i),T1)
          [Get the Position Information of Node at Time Frame T1]
4.        P2=GetPosition(Nodes(i),T2)
          [Get the Position Information of Node at Time Frame T2]
5.        Distance=Abs(P2-P1)
          [Get the Distance covered by node in time frame]
6.        Speed=Distance/(T2-T1)
          [Calculate the speed of Node movement]
7.        Center=GetPosition(Src,T2)
          [Set the source node as the center point respective to which the position is obtained]
8.        Theta=CosInv((P2.X-Center.X)/Radius)
          Theta=SinInv((P2.Y-Center.Y)/Radius)
          [Get the Theta value for Node Movement]
9.        if (Theta in Plane)
          {
          Set Nodes(i) as Neighbor Node
}}
```

After the identification of neighbor node, the next stage is to perform the communication in mobile network under attack analysis. In this work a attack preventive communication approach is defined for effective communication over the network. The algorithmic approach for the work is shown in table 2.

Table 2: Effective Route Generation

```
Algorithm(Nodes,N)

/*Nodes is the List of N Mobiles in Network*/

{
1.    Define the Source Node Src and Dst as Destination Node
2.    Set CurNode=Src
      [Set Src as Current Node]
3.    While CurNode<>Dst
      [Repeat the Process till Destination Node not Arrived]
      {
4.        For i=1 to N
          [Process All Nodes]
          {
5.            if(Neighbor(Node(i),CurNode)
              [Process the Neighbor Nodes]
              {
6.                Perform the Analysis on Node(i) under LossRate, CommRate and Delay Parameters

7.                if (LossRate(Nodes(i))<Threshold And CommRate(Nodes(i))>Threshold And
                      Delay(Nodes(i))<Threshold)
                  {
                  Set Nodes(i).Priority=High
                  }
8.                else if (LossRate(Nodes(i))<Threshold And CommRate(Nodes(i))>Threshold )
                  {
                  Set Nodes(i).Priority=Medium
                  }
9.                else
                  {
                  Set Nodes(i).Priority=low
                  }
              }
          }

10.       Idenitfy the Neighbor Node with Priority High called NodeP
11.       Set CurNode=NodeP
          [Set high prioirty node as next hop]
      }
}
```

The following figure 1 shows the effective path generated between source and destination with the help of the above two algorithms. Here the source node 1 sends the route request message to all its neighbours, after that comparision between the nodes 2, 3 and 4 to be the next hope. The node with least packet drop, less communication delay and in same planer will act as next hope. The same procedure is repeated again and again till the destination is reached. Then next link is created between 1 and 3, 3 and 6 , and so on till the destination node reaches. Here red line shows the final connection between source and destination.

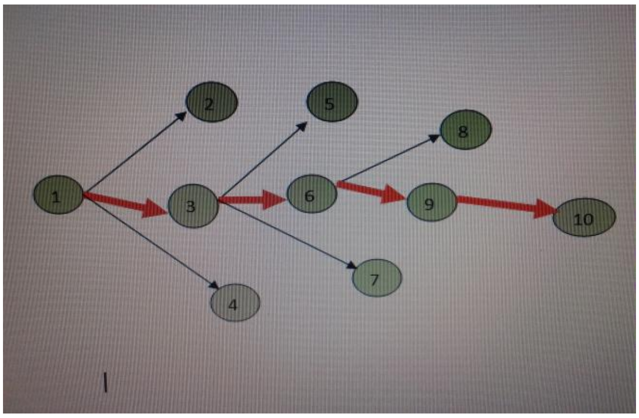

Fig 1: Selected Path 1-3-6-9-10

4. RESULTS

The presented work is simulated in NS2 environment. The results obtained from the work are discussed in this work. The first stage of work is to define the network under specific parameters. These parameters are shown here in table 3.

Table 3: Simulation Parameters

Parameters	Values
Number of Nodes	20
Protocol	AODV
Simulation Time	100 Sec
Packet Size	512
MAC protocol	802.11

The result analysis is here performed under communication loss and delay parameter. The results are shown here under:

X-axis- Simulation Time
Y-axis- Packet Lost

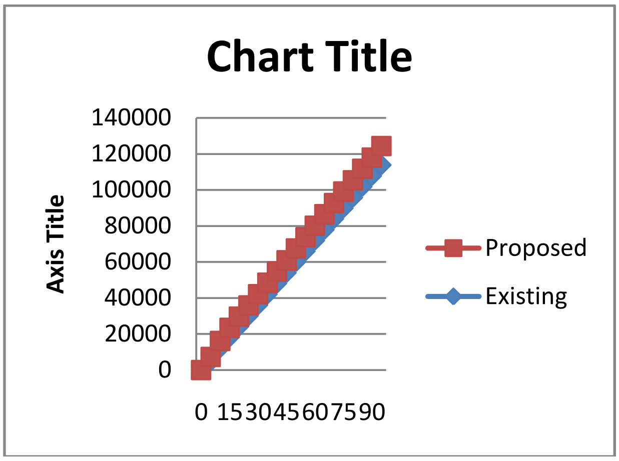

Fig 2: Communication Loss (Existing Vs. Proposed)

The figure 2 is showing the comparison graph to represent the number of packets lost over the network. Here X-Axis represents the simulation time and the Y-axis represents the number of packets lost in the network. In case of Proposed network, the energy adaptive is implemented. The results shows that the presented work gives the packet lost initially, but as the algorithmic approach is implemented and the route reconfiguration is done, after that no more data lost is there .The tabular graph of loss rate is in following :

Table 4: Packet loss

Time Frame	Existing	Proposed
0	0	0
5	4770	2540
10	12250	3938
15	18236	5165
20	24220	5439
25	30152	5711
30	36098	5979
35	42132	6251
40	48154	6527
45	54038	6797
50	60086	7421
55	66025	7760
60	72020	8099
65	78001	8440
70	84001	8769
75	89915	9118
80	95866	9463
85	101915	9802
90	107877	10144
95	113873	10483

Similarly the following table will show the communication delay during the whole process of communication.

Table 5: Communication Delay

Time Frame	Existing	Proposed
0	0	0
5	0.032025	0.032142
10	0.026918	0.026932
15	0.023838	0.023204
20	0.02213	0.021707
25	0.021222	0.020899
30	0.020687	0.020388
35	0.020255	0.020047
40	0.019969	0.019797
45	0.019759	0.019614
50	0.019599	0.019944
55	0.019458	0.02027
60	0.019352	0.020542
65	0.019254	0.020791
70	0.019172	0.021002
75	0.019101	0.021189
80	0.019042	0.021355
85	0.018989	0.0215
90	0.018942	0.021636
95	0.018901	0.021759

Here the delay has increased because now the data transmission is done with the help of safer node i.e. the every next hope is now a safe node and there will be a less amount of data loss.

In following graph :
X-axis- Simulation Time
Y-axis- Delay

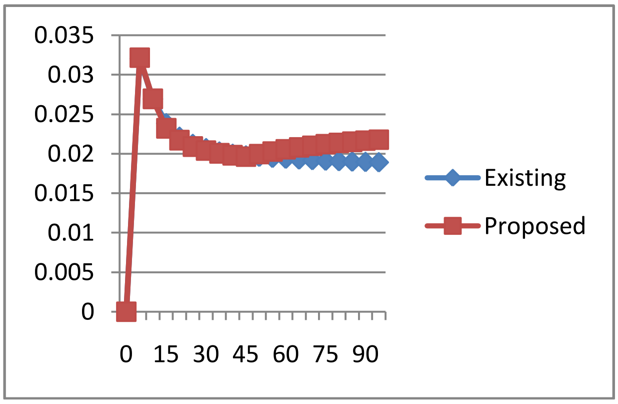

Fig 3: Communication Delay (Existing Vs. Proposed)

The figure 3 is showing the graph to represent the packet delay over the network. Here XAxis represents the simulation time and the y axis represents the packet delay over the network.

5. CONCLUSIONS AND FUTURE SCOPE

In this paper, an effective communication approach is defined in infected speed network. The presented work has defined a two stage algorithm for speed and communication analysis. The work has provided the effective communication over the network. The results shows the work has reduced the communication loss and communication delay.

In this present work we have analyzed different kind of random scenarios under different parameters under AODV protocol. Here we have find the limitation of protocol respective to the environment. The work here is tested on random scenarios, in future some other real time scenarios can also be implemented. Here the work is tested under the scalability vector, in future some other vector can also be considered. In this work, the mobile network is considered. In future, PAN or the sensor area network can be considered.

REFERENCES

[1]. Performance Evaluation of Mobility Speed over MANET Routing Protocols: Yasser Kamal Hassan, International Journal of Network Security, Vol.11, No.3, PP.128-138, Nov. 2010
[2]. Peter J. J. McNerney," A 2-Dimensional Approach to QoS Provisioning in Adversarial Mobile Ad Hoc Network Environments", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10
[3]. Enrique Hernández-Orallo," Evaluation of Collaborative Selfish Node Detection in MANETs and DTNs", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10
[4]. Kevin A. Li," PeopleTones: A System for the Detection and Notification of Buddy Proximity on Mobile Phones", MobiSys'08, June 17-20, 2008, Breckenridge, Colorado, USA. ACM 978-1-60558-139-2/08/06
[5]. M.Shobana, "Geographic Routing Used In Manet For Black Hole Detection", CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India] ACM 978-1-4503-1310-0/12/10
[6]. Ítalo Cunha, "Measurement Methods for Fast and Accurate Blackhole Identification with Binary Tomography", IMC'09, November 4–6, 2009, Chicago, Illinois, USA. ACM 978-1-60558-770-7/09/11
[7]. Poonam, "Misbehaving nodes Detection through Opinion Based Trust Evaluation Model in MANETs", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India ICWET'11, February 25–26, 2011, Mumbai, Maharashtra, India. ACM 978-1-4503-0449-8/11/02
[8]. Xueying Zhang, "The Security in Cognitive Radio Networks: A Survey", IWCMC'09, June 21–24, 2009, Leipzig, Germany. ACM 978-1-60558-569-7/09/06
[9]. Piyush Agrawal, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks".
[10]. S Madhavi, "Survey of Attacks on AODV and MAODV", International Conference and Workshop on Emerging Trends in Technology (ICWET 2010) – TCET, Mumbai, India ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India. ACM 978-1-60558-812-4

[11]. Alberto Medina, "Measuring Interactions Between Transport Protocols and Middleboxes", IMC'04, October 25–27, 2004, Taormina, Sicily, Italy. ACM 1-58113-821-0/04/0010

[12]. Yunyue Zhu, "Efficient Elastic Burst Detection in Data Streams", SIGKDD '03, August 2427, 2003, Washington, DC, USA. ACM 1-58113-737-0/03/0008

[13]. Kamaljit Kaur, "Comparative Analysis of Black Hole Attack over Cloud Network using AODV and DSDV", CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India] ACM 978-1-4503-1310-0/12/10

[14]. Chris Grier, "Manufacturing Compromise: The Emergence of Exploit-as-a-Service", CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10

[15]. Rajesh Yerneni, "Enhancing performance of AODV against Black hole", CUBE 2012, September 3–5, 2012, Pune, Maharashtra, India. ACM 978-1-4503-1185-4/12/09

[16]. Mobility Prediction in Mobile Ad Hoc Networks Damianos Gavalas Department of Cultural Technology and Communication, University of the Aegean Trikoupi & Faonos St., 811 00, Mytilene, Lesvos, Greece,Chapter Submitted to the Encyclopedia of Next Generation Networks and Ubiquitous Computing A book edited by Editor: Samuel Pierre

[17]. Performance Analysis and Mobility Management in Wireless Sensor Network Divya Bharti, Manjeet Behniwal, Ajay Kumar Sharma International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013

[18]. Impact of Node Mobility on MANET Routing Protocols Models by Bhavyesh Divecha, Ajith Abraham, Crina Grosan.