A HMM improved Neighbor Node Analysis Approach in Mobile Network

Deepika
M.Tech Research Scholar
Deptt. Of Computer Sc. & App.,
Deenbandhu Chhotu Ram University of Science and Tech.
Murthal,
Sonepat-131039, Haryana, India

ABSTRACT
Security is one of the challenging issue for Mobile network because of its public access nature. Blackhole is the common threat in this network that capture the communication between nodes and disturb the communication network. In this work, a blackhole preventive routing scheme is presented. The work as defined a two layered analysis to identify the blackhole node and to generate the effective path. In first layer, the long term statistical information is analyzed to identify the trustfulness of node. Once the information is collected, the HMM approach is applied to identify the effective neighbor. The work in implemented in NS2 environment. The results shows that the work has improved the network throughput and decreased the communication loss and delay.

Keywords
HMM, Blackhole, Layered, Statistical

1. INTRODUCTION
A Mobile network is having the dynamic nature because of which any node can enter to the environment and perform the communication. Because of this dynamic nature, there are the chances of inclusion of some suspicious and attacker node in the network. This dynamic nature increases the security challenge in mobile network. There are number of such challenges associated with security system of MANET. These challenges are shown in figure 1. The effective communication in mobile network depends on the neighbor node analysis. It is required for each node to check the reliability and integrity of each neighbor node so that the effective communication will be performed.

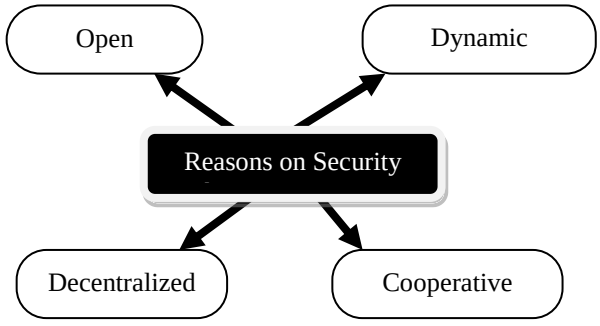


Figure 1 : Reasons of Security Threats in MANET

There are different kind of attacks performed in mobile network by internal and external nodes. Some of these attacks are shown in table 1.

Table 1 : Layer based Attack Distribution

Attacks	Solution
Data Curruption Attack	Worms and malicious code software system or firewall are used to resolve the attack.
Flooding	Point to Point Communication Analysis along with Authentication is used to perform reliable communication
Worm Hole, Blackhole	These are the forwarding attack the preventing routing mechanism is considered to avoid these kind of Attack
Traffic Disruption, WEP Blockage	This is MAC layer attack to resolve this MAC security layer is applied.
Jamming.	It is another DOS attack that slow down the communication by spread spectrum mechanism

These kind of attacks are further divided in different categories. The most broader category of this attack is shown here under

A) External and Internal Attack
These attacks are generated by some non member node of the network. These attacks basically disturb the network communication by including the fake packets or to capture the network bandwidth. DOS is most common attack performed by these kind of nodes. These attacks also performed to hijack the communicating information. Another category of attack in mobile network is the internal attack. These attacks includes the Man-in-Middle attack. This attack is performed by some intermediate communicating node to reveal the communicating information.

In this paper, an effective two layer communication analysis approach is defined to generate effective path in mobile network. In section I, the security challenges in mobile network are defined along with associated attack type. In section II, the work defined by earlier researchers is discussed. In section III, the proposed work is presented along with algorithmic approach. In section IV, the results obtained from the work are discussed. In section V, the conclusion of the work is presented.

2. EXISTING WORK
Lot of work is defined by earlier researchers to handle different security challenges in mobile network. The work defined by the researchers is discussed in this section. Axel Kring[1] has defined a neighbor node analysis approach in mobile network to generate the effective communication path. In this work, a k-

hop analysis approach is defined under constraint analysis to generate the communication path and to generate the reliable route over the network. Author has defined the malicious node analysis approach to provide safe communication. Ying Li[2] has defined a work on node tracking to provide the effective communication. Author performed the mathematical and probabilistic analysis approach to generate the effective path. Another work on the malicious node detection and a secure routing was presented by Bogdan Carbunar in year 2004. Author investigate the security threats in mobile networks so that the reliable communication will be drawn from the communication. Author has defined a secure infrastructure oriented communication in misbehaving mobile networks[3].

A work on the exploration of hijacking attack and the preventive mechanism was presented by Johann Schlamp in year 2012. Author has defined a security based work to identify the spam packets during the communication process as well as provided an effective approach to detect the victim. Author has defined the analysis through the IP prefix analysis so that the long term benefits will be obtained from the work. Author has defined the incidental communication and control mechanism in mobile network[4]. A control mechanism to restrict the outgoing spam communication was handled by Joshum Goodman in year 2004. Author has defined the conventional technique to analyze the message packets under different techniques so that the life time of the network communication will be increased. Author has defined the work to obtain the maximum profit from the communication so that reliable communication effect will be drawn[5]. Danny Dhillon has defined the work to improve the communication integrity in case of intrusion mobile network. Author defined the safeguard based approach to increase the detection rate so that effective communication schedule will be obtained[6].

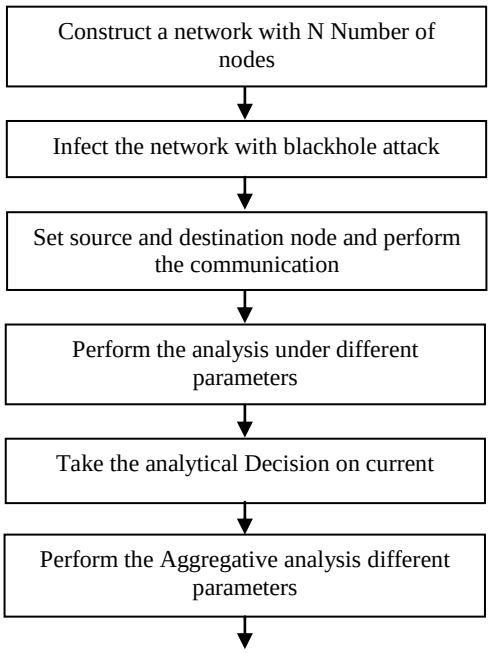
Ahmed Khurshid has presented a work on the real time analysis on different network invariants that affects the network flow. Author presented a controller device based approach to control the forwarding communication as well as the reliable communication will be drawn from the network[7]. Another work on the blackhole detection was presented by Evan Cooke in year 2004. Author defined the exploration of work under the traffic analysis so that reliable packet communication will be performed. Author defined the work based on Internet Motion sensor so that the infrastructure based effective communication will be drawn from the network[8]. A work on the effective routing in opportunistic network was presented by Umair Sadiq in year 2012. Author presented the forwarding rate analysis along with packet loss analysis to identify the communication incentive. Author presented the work to analyze the control in non linear communication network. Author defined the work in the optimal conditions so that the flow maximization will be performed[9]. The exploration of the node replication attack was presented by Mauro Conti. Author presented a energy and memory effective solution in a constrained network so that reliable communication path will be obtained[10]..

Garima Gupta has defined a work on blackhole attack and provide a delay effective scheme to minimize the attack hazards. Author defined the characteristic analysis based algorithm generate an effective route under the malicious node attack. Author defined the probabilistic behaviors analysis scheme to provide the solution against the blackhole attack[11]. A work on the topology aware analysis approach to reveal the security scheme in mobile networks. Author presented an isolated mechanism to handle the attacks and to reduce the false detection rate. Author presented a overhead analysis approach to improve the network reliability and to minimize the attack impact in mobile network[12]. A two dimensional analysis approach to improve the network QoS under different adversarial environments was presented by Peter J.J. McNeney. Author discussed two main issues to improve the QoS and to improve the network reliability. Author defined a single path adaptation and multipath adaptation mechanism to improve the network bandwidth and to incrase the network reliability[13].

3. RESEARCH METHODOLOGY

The presented work is about to provide the effective solution in blackhole infected mobile network. The work is defined to improve the network communication and reduce the communication loss and delay in infected network. The work is to provide the effective preventive path in mobile network.

In this proposed approach, a two layered analysis approach is been suggested to perform the reliable communication in blackhole-affected mobile network. This preventive analysis is based on the statistical as well as predictive analysis. At the initial stage, long term statistical analysis is performed to identify the trustful nodes over the network. This analysis is performed under different trust based statistical parameters such as loss rate, response time delay etc. Once the trust nodes are identified, the next work is to perform the short term analysis to identify the effective neighbour node. To identify the best neighbour a markov model based analysis approach is suggested in this work. The markov model is suggested to perform a predictive and probabilistic analysis of throughput and the response time between all pairs over the network. The all pair communication analysis will be done that can effectively analyze the tunnel attack over the network. Once the attack will be detected, the next work is to block these nodes and to perform a reliable communication over the network for a safe path. The route safely and reliability are the major objective of this defined work. The flow of work is given in figure 2.



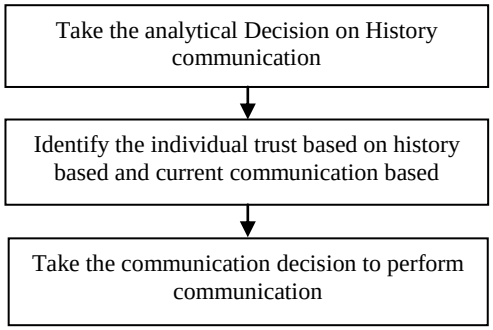


Figure 2: Flow of Work

A) Algorithm : Communication Analysis

The first stage of presented work is to perform the neighbor node analysis to identify the effective communicating node so that the effective path will be generated. The algorithm of this analysis stage is shown in table 1

Table 1 : Communication Analysis Algorithm

```
Algorithm(N,Src,Dst)
/*The Mobile Network is defined with N Nodes and with the
Specification of Src and Dst Nodes*/
{
1.      Set CurNode=Src
        [Set Src as Current Node]
2.      While CurNode<>Dst
        [Repeat the process till destination Node not
        occur]
        {
3.      Generate the List of Neighbor Node of  CurNode
called NeighNodeList
4.      For i=1 to Length(NeighNodeList)
        [Process All the NeighborNode ]
        {
5.      Perform the Analsyis on NeighNodeList(i)
        under LossRate, Communicaiton Rate and
        Delay
6.      if(LossRate<Threshold And Delay<Threshold
        And CommunicationRate>Threshold)
        {
        Set Priority=3
        }
7.      else if(LossRate<Threshold and
        CommRate>Threshold)
        {
        Set Priority=2
        }
8.      Else
        {
        Set Prioirty=1
        }
}
9.      if Any(NeighborList.Priority)=3)
        {
10.     Set Node as Next Hop
        }
11.     else
        {
        Call "HMM" to identify Effective Node
        }
}
```

B) Algorithm: HMM

The analysis algorithm assigns the priorities to the neighboring nodes based on communication analysis. If the communication is effective high priority is assigned. The next hop is identified based on this neighbor node analysis. If no high priority node exist in such case, HMM algorithm is applied to identify the effective neighbor. The algorithm for HMM approach is given in table 2

Table 2: HMM Algorithm

```
HMM(N,Src,Dst)
/*N is number of nodes and Src is the Source and Dst is the
Destination Node*/
{
1.      CurNode=Src
        [Set Src as Current Node]
2.      While CurNode<>Dst
        [Repeat Process till destination NOde not occur]
        {
3.      Generate the Neighbor Node list for CurNode
4.      For i=1 to Lenght(NeighborList)
        {
3.      Perform Communicaiton Count and Frquency Count
for Neighbor(i)
4.      Identify the Average Communication on Each
Neighbor)
        }
5.      if (FrequencyCount(Neigh(i))>Average)
        {
6.      Set ParticipateVector(i)=1
        }
7.      else if(FrequencyCount(Neigh(i))>Average*2)
        {
8.      Set ParticipateVector(i)=2
        }
9.      else
        {
10.     Set ParticipateVector(i)=0
        }
11.     if(Loss(Neighbor(i)>0 And Pariticate(i)==2)
        {
        Set Node(i) "Off"
}
```

The HMM is here to perform the communication analysis and block the blackhole node. If a node having the high communication ratio and does not providing the effective path communication is set block so that no more communication is performed over that node. The average communication analysis is here identified in terms of node based analysis.

4. RESULTS

In simulation, we can construct a mathematical model to reproduce the characteristics of a phenomenon, system, or process often using a computer in order to information or solve problems. Nowadays, there are many network simulators that can simulate the MANET. The work is here implemented in NS2 environment under defined scenario shown in table 2.

Table 2: Network Scenario

Parameter	Value
Number of Nodes	26
Topography Dimension	100 m x 100 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	AODV

The results obtained from the work are shown here under

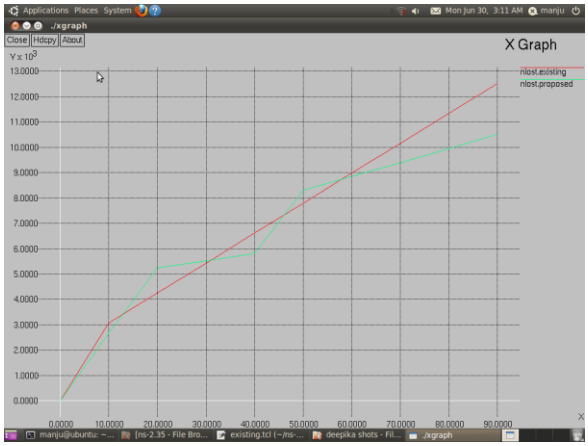


Figure 3: Packet Loss Analysis (Existing Vs. Proposed)

Here figure 3 is showing the analysis of presented work in terms of packet loss. The figure shows that the work has reduced the packet lossbecause of its analysis time. The data is transmitted only if the safe node is identified.

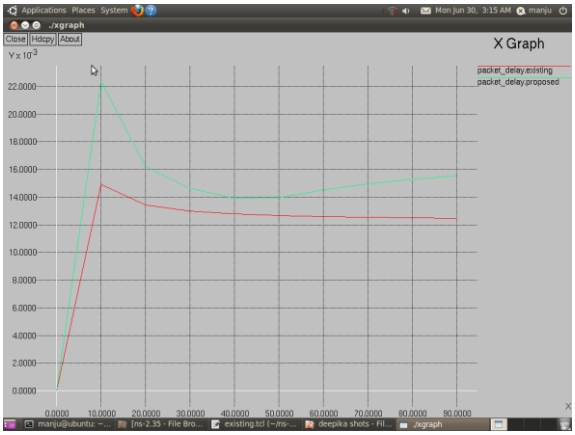


Figure 4 : Packet Delay Analysis (Existing Vs. Proposed)

Here figure 4 is showing the analysis of presented work in terms of packet delay. The figure shows that the work has increased the packet delay. The work is based on the identification of safe neighbor node because of which the analysis time is increased.

5. CONCLUSION

In this paper, an effective routing mechanism is defined using HMM based statistical analysis. The work is defined to improve communication in blackhole infected mobile network. The results shows the work has improved the communication and reduced the communication loss and delay over the network.

6. REFERENCES

[1] Axel Krings," Neighborhood Monitoring in Ad Hoc Networks", CSIIRW '10, April 21-23, 2010, Oak Ridge, Tennessee, USA ACM 978-1-4503-0017-9

[2] Ying Li," Component-Based Track Inspection Using Machine-Vision Technology", ICMR'11, April 17-20, 2011, Trento, Italy ACM 978-1-4503-0336-1/11/04

[3] Bogdan Carbunar," JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM 1-58113-925-X/04/0010

[4] Johann Schlamp," How to Prevent AS Hijacking Attacks", CoNEXT Student'12, December 10, 2012, Nice, France. ACM 978-1-4503-1779-5/12/12

[5] Joshua Goodman," Stopping Outgoing Spam", EC'04, May 17–20, 2004, New York, New York, USA. ACM 1-58113-711-0/04/0005

[6] Danny Dhillon," Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. ACM 1-59593-306-9/06/0007

[7] Ahmed Khurshid," VeriFlow: Verifying Network-Wide Invariants in Real Time", HotSDN'12, August 13, 2012, Helsinki, Finland. ACM 978-1-4503-1477-0/12/08

[8] Evan Cooke," Toward Understanding Distributed Blackhole Placement", WORM'04, October 29, 2004, Washington, DC, USA. ACM 1-58113-970-5/04/0010

[9] Umair Sadiq," CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10

[10] Mauro Conti," A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", MobiHoc'07, September 9-14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-684-4/07/0009

[11] Garima Gupta," Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10

[12] Abhijit Das," Energy Aware Topology Security Scheme for Mobile Ad Hoc Network", ICCCS'11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02

[13] 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