Security Measure to Detect and Avoid Flooding Attacks using Multi-Agent System in MANETS

Bandana Mahapatra
Computer Science & Engineering Dept.
Siksha 'O' Anusandhan University,
Bhubaneswar, India

Prof.(Dr.) Srikanta Patnaik
Computer Science & Engineering Dept.
Siksha 'O' Anusandhan University,
Bhubaneswar, India

***Abstract*: Security is considered as one of the major challenge when it comes to infrastructure less and self dependent network without any centralized control. The vulnerability of Adhoc Network makes it susceptible to external attacks like flooding of hello messages or propagating fake routing messages etc. Such attacks generates a variety of problems like disturbing the network by flooding messages that results in waste of battery which is a vital resource to maintain the life span of the network. Most importantly cause agents to die when unable to reach destination due to fake routing messages causing a heavy loss on part of the nodes generating them to maintain the route knowledge. The paper proposes a novel technique to identify the flooding attack and measure to overcome them using Multi-Agent system.**

Keywords: ***External Attack in MANET, Flooding attacks, optimal agents in multi agent system***

I. INTRODUCTION

The Adhoc Network is a system of wireless mobile nodes where a group of nodes within close proximity make a network. Such an infrastructure less and self configured network, on account of unavailability of a proper centralized control and limited resources remains vulnerable to attacks [1]. The attack types can be broadly classified into either an external attacks or an internal attacks, where in external attacks attacker target the network medium to disrupt the normal network flow. The typical examples of external attacks can be flooding of messages or propagation of fake routing messages that give rise to Denial of Service Attack. The prevention mechanisms available to avoid such attacks in traditional network like membership authentication or firewall fails to work here due to unstable network medium and frequent topology change[2]. The volatile topology of MANETS demands concern of the researchers to formulate a proper routing scheme to achieve resilient and an effective communication among the nodes.

Mobile Agents are independent route search messages that practically goes around the network from one node to another and update the routing table according to the nodes they visit till they reach destination[3]. This technique as a solution could not prove effective when the network scales up moreover single dependent route as a communication medium posed problems like improper load balancing, unreliable route to depend upon as well as lack of alternative routes available. Multi Agent system solved efficiently load balancing problem as well as provided alternative solution but increased the computational overhead on part of the node while generating agents or causing increase in overall network traffic by launching multiple routing messages as Agents[4]. Therefore launching of huge number of Agents to maintain the network traffic tends to result in increase of network traffic as well as reduced lifetime of a node affecting the overall network. Hence this demands the need to quantify optimal number of nodes suitable for a particular network topology for a particular time. Each agents launch incur additional cost on the node hence death of an agent due to flooding attacks can be considered as a heavy loss on the part of the node.

The paper provides a novel technique of quantifying the optimal number of agents to be launched for route search, checking for possibilities of flooding attack in the network, , identifying malicious nodes and taking effective measures to block the node while using alternative routes provided by multiple agents to maintain the flexible and robust communication network flow.

2. Detecting and Avoiding Flooding Attack using Multiple Agents

The paper aims at providing a technique to detect flooding attacks in the buffer and use alternative routes to maintain a resilient network

The Fig 1. shows the proposed model consisting of 3 main modules. The node first calculates the optimal number of Agents to be launched in the network considering the current topology or network scenario[5]. These agents move around from one node to other node in search of the destination while keeping a track of the node they visit during their search period. These agents

return back to the original node once they reach the destination using the same route. These messages are received by the node and are accumulated in the incoming message buffer where the occurrence flooding attack is checked in the buffer itself so as to prevent wastage of power in reading same message again.

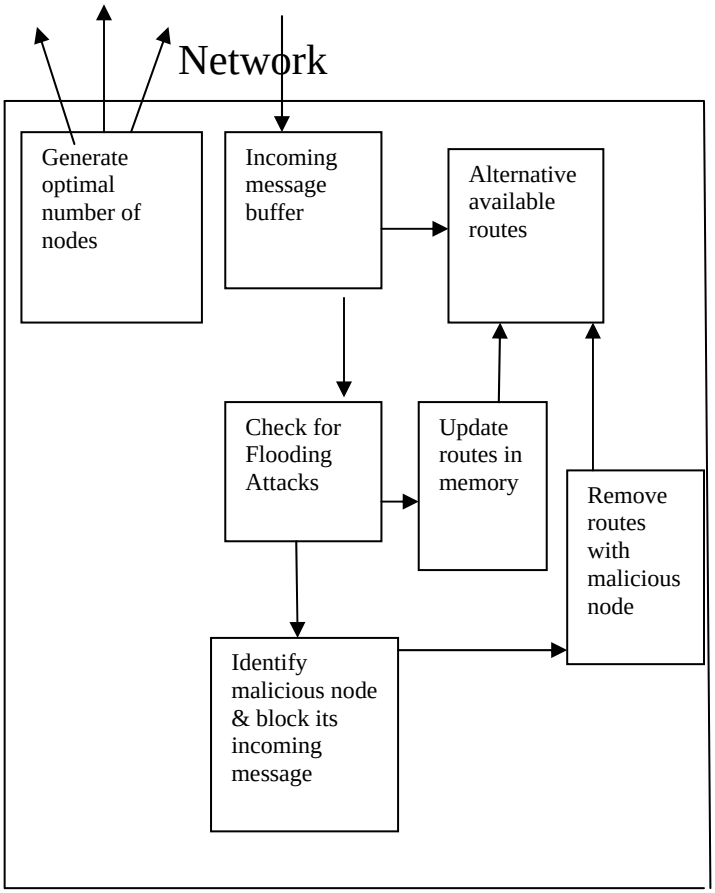

Fig1. Proposed Node Architecture for Detecting and Avoiding flooding attacks

The detection of flooding attack is dealt by blocking the node generating malicious messages and discarding all the routes that has the malicious node as an intermediary node to reach destination. The multiple agents here collect different available routes from a source to destination that helps node to maintain the communication network as well as the connectivity that makes it a resilient or a robust network capable of handling flooding attacks.

TABLE - I
ALGORITHM TO DETECT AND AVOID FLOODING ATTACKS

Start
Step1. Set Nearest_neighbor =no of hello_msg
Step2. Calculate
Agents to be launched =nearest_neighbour/2
Counter = Counter + 1
Step3. Launch agents in network
Step4. If flooding_attach== yes
Malicious_node= node_id
//Check memory route table
Step5. For i=1to N // N is no of rows in route table
If Table [i] = Malicous_node as intermediate node
Table[i]= Table[i+1].
end

A. Optimal number of Agents – The wireless Ad Hoc Network when scaled up it becomes challenging for the normal wireless routing protocols to keep the Network Routing information current. Hence the Agents become necessary once the Network size is huge. But a Single Agent Network also has its short comings like improper load balancing and only a single communication route to reach from source to destination which is also not dependable due to Ad Hoc nature of the Network. This problem can be addressed by using multi Agent in the Network for communication. Multiple Agents launched in the network though helps increasing the number of received nodes and throughput also increases the computational overhead and network bandwidth. Moreover continuous growth in number of agents becomes a bottleneck with no significant improvement brought on the network performance. This demands launch of optimal number of Agents in the network considering the variable constraints like number of received packets, dropped packets, Normalized Routing Overload, computational overhead, etc[7].

Constrained optimization is the process of optimizing an objective function with respect to some variables in the presence of those variables. Minimum of constrained non linear multivariable function is a gradient based method that is designed to work where objective function and the constraint function are both continuous first derivatives. It uses a sequential quadratic programming (SQP) method, where the function solves a quadratic programming sub problem at each iteration. It can be calculated as –

Min $f(x)$ such that

$$\begin{cases} c(x) \leq 0 \\ ceq(x) = 0 \\ A.x = beq \\ Aeq.x = beq \\ lb \leq x \leq ub \end{cases}$$

B. Detection of Flooding attacks in Memory:

Flooding is a denial of service attack designed to degrade the performance of the network or node by flooding it with large amount of traffic flood. Attacks occur when a network or service becomes weight down with packets initiated incomplete connection requests that it can no longer process a genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host memory buffer. Once this buffer is full no further connections can be made and result is Denial of Services[7,8].

The proposed Knowledge Based model consists of a buffer that receives the incoming messages and the signature module that comprises of message signatures that are categorized as Flooding attack and are subsequently blocked. The incoming messages are first received by

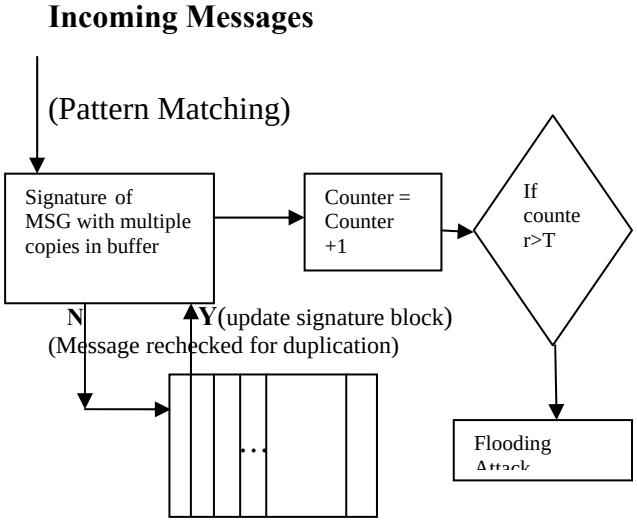

Fig 2 .Proposed Model for detecting Syn-Flood attacks in Buffer

the buffer and are pattern matched with the signature module to see if the message is sent by a malicious node creating Syn-Flood attack. If the message is a non match then it is rechecked within the buffer for tracing the possibility of Attack. If the message is found to be repeated beyond a certain threshold , the message is updated in the signature module categorizing it as DoS attack pattern.

TABLE - II

ALGORITHM TO DETECT FLOODING ATTACKS IN BUFFER

```
Start
Set Threshold T
Incoming Message→ Buffer
 If Message ==     signatures in memory
          Counter = Counter + 1
  Else
      Set  i = 1
        While (Buffer ≠ NULL)
              If Buffer [0] == Buffer[i]
                 Buffer[0] → Signatures in memory
                 Delete Msg[Buffer[0]]
          Else    i= i+1
If counter > Threshold
       Block the rotes with node_id in the memory
            Buffer
end
```

6. EXPERIMENTAL RESULTS

A. In this work we have analyzed the behavior of varying number of Agents across different network topologies. Here the constraints effecting the overall network performance is considered while quantifying the approx-optimal number of Agents. The constraints effecting the network performance considered are computational overhead on nodes, Normalized Routing Overload, and throughput of the Network.

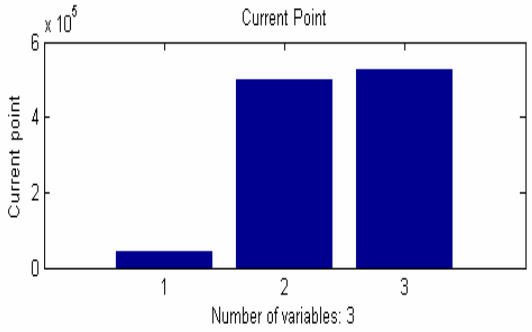

Fig 3. Impact on Constraints due to change in number of Agents Launched

The **fig.3** shows the impact of change in number of Agents launched in the network on different constraints involved in determining the overall network performance hence also determining the aprox optimal number of agents to be launched in the network by a node where the variable 1 is the throughput, 2 is normalised routing overload and 3 is the computational overhead incured upon nodes. Using Trust Regeon Reflective Algorithm and F-Mincon-Constrained non-lenear minimization the

perito Optimal Solution for Aprox optimal number of Agents that gives maximum benefit to the network is obtained, shown in Fig 4.

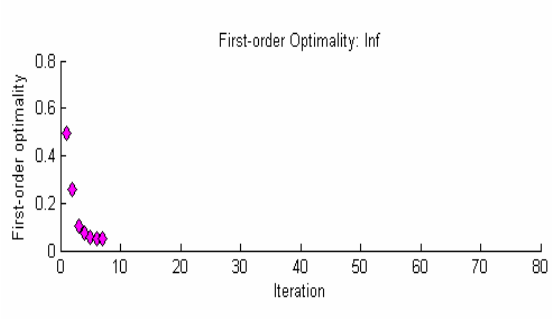

Fig4 . Perito Optimal Solution obtained from Trust Region Algorithm

B. We simulated the proposed algorithm in NS-2 environment using AODV protocol. The results obtained as projected in the Fig.5 shows a significant improvement in detection of Flooding Attacks generated in the network in comparison to AODV protocol. Fig.6 shows the increase in true positive along with reduction of false positive generated in the network[4]. The true positive leads next to the knowledge base updating thus enabling the signature updation dynamically which is advantageous to the MANETs, that are themselves dynamic in nature and are equipped with limited resources to rely upon, hence demands continuous signature to be updated.

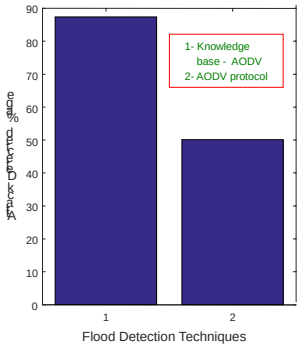

Fig.5. Knowledge Based method Vs AODV protocol

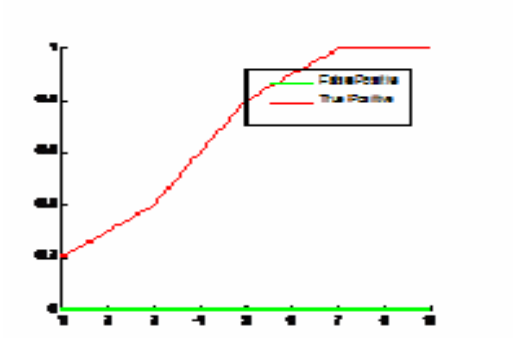

Fig.6. Alarms Generated in the Knowledge based model of Flood Detection

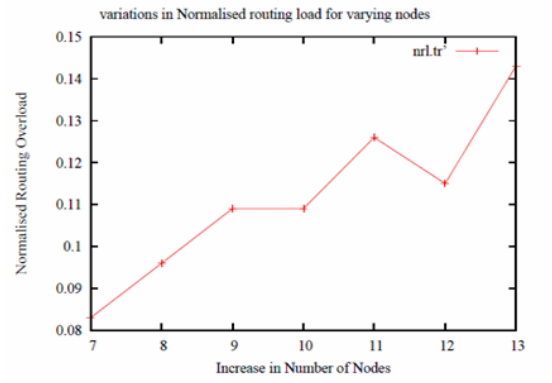

Fig.7. Normalized Routing Overload for the Scaled Network

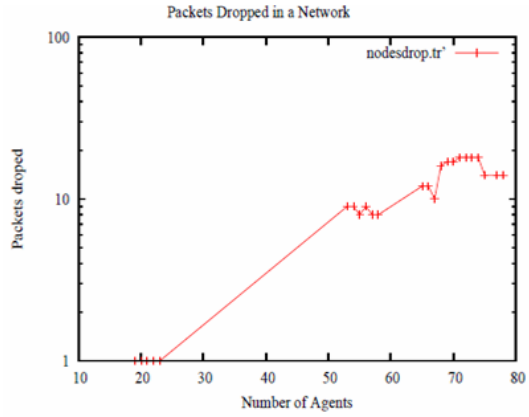

Fig.7. Overall Packets dropped in an attack condition

C. **Result Analysis**: The proposed knowledgebase DoS detection model simulated gives a rise in throughput by 37.33% and increases the packet delivery ratio as shown in the Fig. 5 as well as reduces the end to end delay giving a significant improvement over the network performance. Fig 6 and 7 shows the Normal Routing overload and Overall Packets Dropped in an attack scenario. The results shows a significant improvement in

maintaining a resilient network suffering from very low packet drop due to Syn-Flood attack condition in a network having multiple nodes supporting multiple number of Agents.

Conclusion:

In the present study we have proposed a technique for detection of the DoS Attack as well as the scheme for avoiding it using optimal number of Multiple Agents. The study on the behavior of the Agents launched into the network was conducted which provides the perito optimal numbers that will prove most beneficial considering various constraints. Further we have proposed algorithms to detect flooding attacks in the buffer itself which has helped in reducing the number of dropped packets by 74%as well as improved the Normalized Routing Overload (NRL) of the network.

References:

[1] T.Nishitha and P.Chenna Reddy, "*Performance Evaluation of AntHocNet Routing Algorithm in Ad Hoc Networks*", IEEE International Conference on Computing Sciences- 2012, pp. 207-211.

[2] Chandreyee Chowdhury and Sarmistha Neogy, "*Estimating Reliability of Mobile Agent System for Mobile Ad hoc Networks*" IEEE- Computer Society-2010.

[3] Futai, Zou ; Xinghao, Jiang ; Jianhua, Li, "*Multi-agent cooperative intrusion response in mobile adhoc networks*" International Journal of Engineering and Technology (IJET), Vol 4 No- 6 Dec 2012-Jan 2013

[4] Yavuz Tokgoz and Anthony Acampora, "*Improving Connectivity and Power Efficiency in Wireless Ad Hoc Networks Through Agent Nodes*" IEEE-2005.[5] H. Matsuo and K.Mori, " *Accelerated Ants Routing in Dynamic Networks*," in Proc. Intl. Conf. On Software Engineering, Artificial Intelligence, Networking and Parellel/Distributed Computing, pp.333-339, Aug. 2001.

[5] K.Fall and K.Vardhanan, editors**. The ns manual. The VINT Project, UC Berkley, LBL, USC/ISI and XEROX PARC, 2001.**

http://www.isi.edu/nsnam/ns/ns-documentation.html

[7] Romit RoyChoudhury, S. Bandyopadhyay and Krishna Paul, "*A Distributed Mechanism for Topology Discovery in Ad Hoc Wireless Networks Using Mobile Agents*", IEEE -2000, pp. 145-146.

[8] D.Milojick '*Mobile Agent Applications* ", IEEE concurrency, pages 80-90, July-September 1999