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

Bandana Mahapatra, Srikanta Patnaik
Departement of Computer Science Engineering, Siksha O Anusandhan University, India

Article Info

Article history:

Received Dec 9, 2016
Revised Mar 14, 2017
Accepted Mar 30, 2017

Keyword:

AdHoc network system
External attack in MANET
Flooding attacks
Optimal agents in multi-agent system

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

Corresponding Author:

Bandana Mahapatra,
Computer Science & Engineering Dept.,
Siksha 'O' Anusandhan University,
Bhubaneswar, India.
Email: bandana11@gmail.com

1. 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 attack or an internal attack. In external attack, attacker target the network medium to disrupt the normal network flow. The typical examples of external attack 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 attack types in traditional network are membership authentication, firewall which fails to work due to unstable network medium and frequent topology changes [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], [4]. 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 [5]. 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 [6]. Each agents launched 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 [7], [8].

2. RELATED PAPERS

Romit roy Choudhury, S. Bandyopadhyay and Krishna Paul [9] proposed a distributed Mechanism for Topology discovery in Ad Hoc Wireless Networks Using Mobile Agents where they have defined a concept of information aging on link affinity based on which a predictive algorithm running on each node can predict the current Network topology based on the current Network information stored at that node. Link affinity, associated with a link between two nodes n and m, is a prediction about span of life of that link in a particular context. They have applied this notion to predict topology by each node and thus be cautious before data transfer is initiated.

Ryokichi Onishi Samyasu Yamaguchi, Hirao Ki Morino Hitoshio Aida Jadosaito proposed “The Multi Agent System for Dynamic Network Routing”. They proposed that by multiplying each entry in routing table to store much more information from Agents evaluating them to make better use of information succeeded in rating the Network continuously by 40%. They also suggested that Agents themselves are often written in relatively slow interpreted languages and slightly gain weight for containing code. However if the entire system saves more bandwidth resource for control and reacts more quickly these overheads of Agents might be acceptable.

Bounpadith Kannhovong, Hidehisa Nakayama, Yoshiaki Nemoto, and Neikato [10] have conducted a survey on the state of the art of security issues in Manet. They have examined routing attacks like link spoofing, colluding miserly attacks and defense mechanisms against such attacks in existing MANET protocols.

Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong in their paper [11] have designed a generic defense against the Adhoc Flooding Attack in mobile Adhoc Network. Their designed mechanism aims at recording the rate of route_request message. Once the threshold is exceeded nodes deny any further request packets from the intruder.333.

Meenakshi Patel, Sanjay Sharma, Divya Sharan have proposed in their paper [12] the mechanism for detection and prevention of Flooding Attack using SVM. They have schemed a new method based on AODV behavioral metrics for detecting and preventing Flooding Attacks in MANETS. They have used the PDER, Co and PMIR as metrics to predict the Flooding attacks.

3. 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.

ALGORITHM – 1
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_attack = = 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
```

Algorithm-1represents the procedure adopted by the proposed model for detection of Flooding Attacks and measures adopted to avoid it which is shown as Figure 1. The Figure 1 shows the proposed model consisting of 3 main modules. Module1 is generating optimal number of agents, module2 is about detection of flooding attacks in buffer and module 3 deals with measures to avoid flooding attacks and maintaining a resilient network.The node first calculates the optimal number of Agents to be launched in the network considering the current topology or network scenario [5].

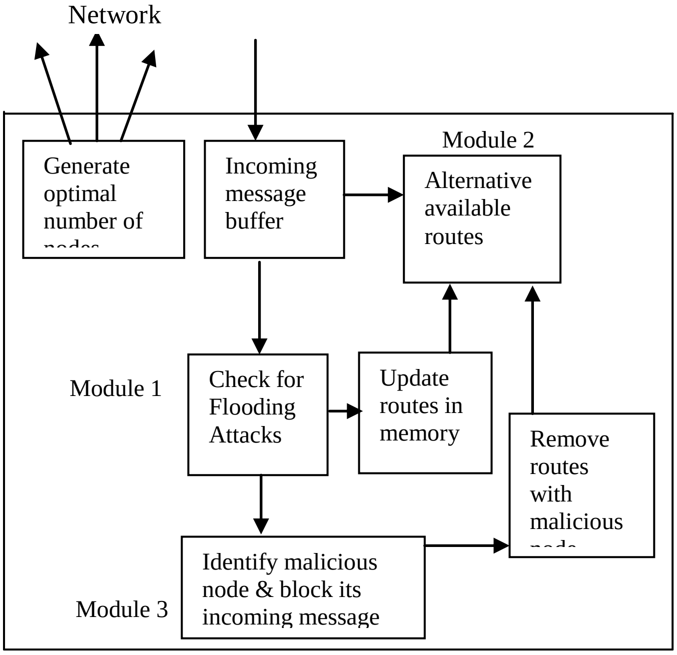
Network
Module 2
Generate optimal number of nodes
Incoming message buffer
Alternative available routes
Module 1
Check for Flooding Attacks
Update routes in memory
Remove routes with malicious node
Identify malicious node & block its incoming message
Module 3

Figure 1. Proposed Node Architecture for Detecting and avoiding flooding attacks

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 of flooding attack is checked in the buffer itself so as to prevent wastage of power in reading same message again.

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.

3.1. 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 multiple agent in the Network for communication. Multi-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 may be calculated as – Min f(x) such that:

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

3.2. Detection of Flooding attacks in Buffer

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 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.

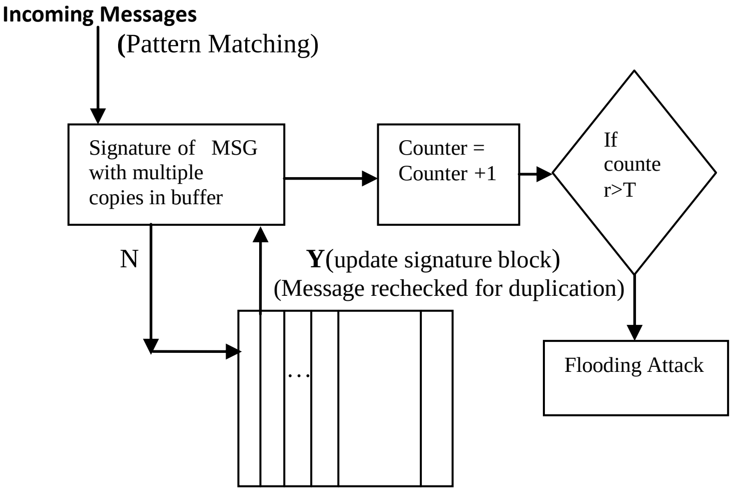
Incoming Messages
(Pattern Matching)
Signature of MSG with multiple copies in buffer
Counter = Counter +1
If counte r>T
N
Y(update signature block)
(Message rechecked for duplication)
…
Flooding Attack

Figure 2. Proposed Model for detecting Syn-Flood Attacks in Buffer

ALGORITHM -2
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
```

3.3. Measures to Avoid Flooding Attacks and Maintain a resilient Network

This module is capable of both identifying malicious nodes as well as taking preventive measures to avoid such attack maintaining a robust and resilient network**.** Once the message buffer encounters a repeated message pattern beyond the threshold levels, the node id of the malicious node sending messages is identified and all further messages from the node is blocked. The routes available with the node having the malicious node as an intermediate one is blocked and alternative routes available through multi agents is used for message communication between the source and destination node.

4. EXPERIMENTAL RESULTS

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.

The Figure 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 Figure 4.

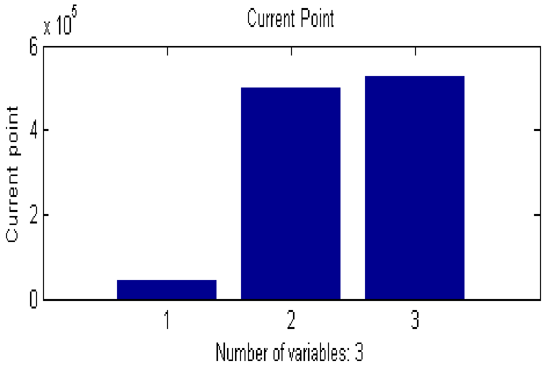

Figure 3. Impact on Constraints due to change in number of Agents Launched

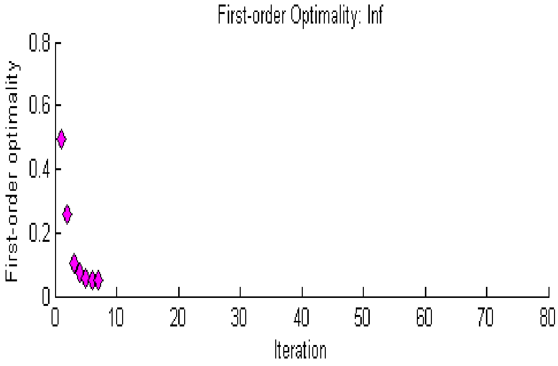

Figure 4 . Perito Optimal Solution obtained from Trust Region Algorithm

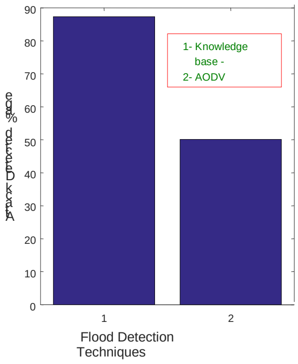

Figure 5. Knowledge Based method Vs AODV protocol

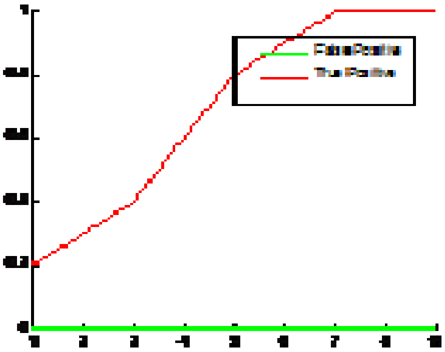

Figure 6. Alarms Generated in the Knowledge based model of Flood Detection

We simulated the proposed algorithm in NS-2 environment using AODV protocol. The results obtained as projected in the Figure 5 shows a significant improvement in detection of Flooding Attacks generated in the network in comparison to AODV protocol. Figure 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.

4.1. 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 Figure 5 as well as reduces the end to end delay giving a significant improvement over the network performance. Figure 7 and 8 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.

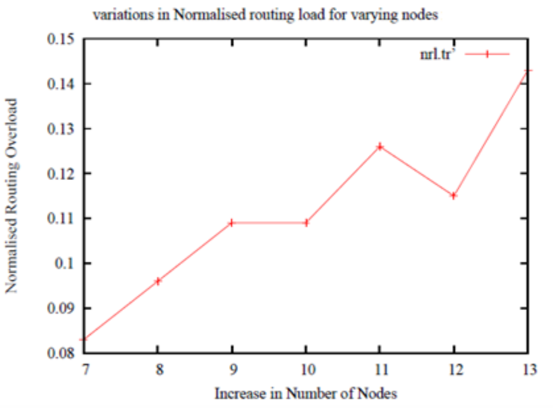

Figure 7. Normalized Routing Overload for the Scaled Network

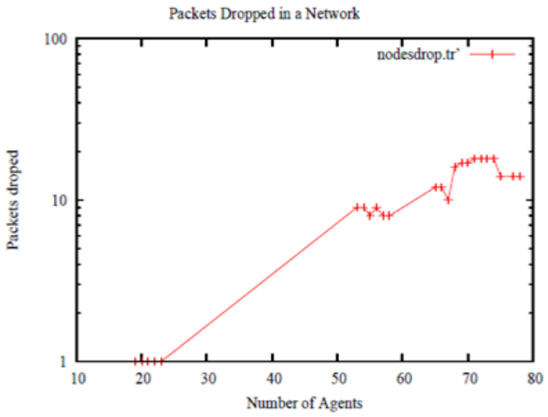

Figure 8. Overall Packets dropped in an attack condition

5. CONCLUSION

In the present study we have discussed regarding the Syn-Flood Attack and how dropping or a failure of agents due to heavy network traffic is a heavy loss incurred upon the nodes as well as the network medium as a whole. Thereafter we have proposed a model that would detect the syn-flood attack in the buffer itself saving the energy wastage in processing of such messages as well as generating optimal number of agents so as to keep the network medium traffic low. The model also maintains a robust communication medium while identifying and blocking routes through the malicious node. Further a study on the behavior of the agents launched into the network has been conducted which provides us with a parito optimal number giving us the most beneficial number of agents to be launched. The proposed algorithm of the model has been tested across NS2 medium that gave us the reduced number of drop of packets by 74% and improved NRL of the network. the proposed algorithm, has shown an increase in number of Syn-Flood attack detection by 37% along with increase in rate of true positive alarms generated in the node.

REFERENCES

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

[2] Z. Futai, *et al.*, "Multi-agent cooperative intrusion response in mobile adhoc networks," *International Journal of Engineering and Technology (IJET)*, vol/issue: 4(6), 2013.

[3] P. Braun and W. Rossak, "Mobile Agents," Elsevier, 2005.

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

[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, 2001.

[6] Y. Tokgoz and A. Acampora, "Improving Connectivity and Power Efficiency in Wireless Ad Hoc Networks Through Agent Nodes," IEEE, 2005.

[7] K. Fall and K. Vardhanan, "The ns manual," The VINT Project, UC Berkley, LBL, USC/ISI and XEROX PARC, 2001. http://www.isi.edu/nsnam/ns/nsdocumentation.html

[8] R. R. Choudhury, *et al.*, "A Distributed Mechanism for Topology Discovery in Ad Hoc Wireless Networks Using Mobile Agents," IEEE, pp. 145-146, 2000.

[9] B. Kannhovong, *et al.*, "A Survey of Routing Attacks in Mobile AdHoc Networks," *IEEE Wireless Communications*, 2007.

[10] P. Yi, *et al.*, "A New Routing Attack in Mobile Ad Hoc Networks," *International Journal of Information Technology*, vol/issue: 11(2).

[11] M. Patel, *et al.*, *"Detection and Prevention of Flooding Attack Using SVM,"* International Conference on Communication Systems and Network Technologies (CSNT), 2013.

[12] D. Milojick, "Mobile Agent Applications," *IEEE concurrency*, pp. 80-90, 1999.

BIOGRAPHIES OF AUTHORS

Ms. Bandana Mahapatra is Asst. Professor of Computer Science and Engineering at SOA University, Bhubaneswar, India since 2008. Her research interest is Security in AdHoc Network and Artificial Intelligence. Her contribution also includes other issues in Adhoc Network like efficient power management or searching shortest path for communication using artificial intelligence. She is currently pursuing her PhD under SOA University, Bhubaneswar.

Dr. Srikanta Patnaik is a Professor of Computer Science and Engineering at SOA University, Bhubaneswar, India. His research interest is in Machine Intelligence and Robotics, and he has published more than 100 technical papers in the international journals and magazines of repute. His name has been placed in the MARQUIS Who's Who in the World for the 2004 and he was also named as the International Educator of the Year 2005, by International Biographical Centre inGreat Britain. He is the Editor-in-Chief of the *International Journal of Information and Communication Technology*, and *International Journal of Computation Vision and Robotics*, as well as President and Chief Mentor of Interscience Research Network (IRNet), which is a professional body to encourage researchers and scholars to enhance their research throughput.