PN Design Against RREQ Flood Attacks in MANETs

[1] S. Ezhilarasi., M.E.,M.B.A, [2] R. Sheik Abdullah.,M.C.A.,M.Phil.,(Ph.D).,
[1]Assistant Professor, CSE, [2]Assistant Professor, CA
Roever Engineering College, Perambalur, Alagappa University College of Arts and Science, Paramakudi

Abstract:- **Mobile Adhoc network (MANET) is a wireless LAN(Local Area Network) without central base stations. Hence they are vulnerable to attacks such as flood attacks from intruders. Mobile and wireless devices belonging to MANET are called mobile nodes. The source node and destination node comprise a session pair. If the distance between them is large then the data is sent via intermediate nodes. AODV (Adhoc On Demand Vector) routing protocol offers adaption to dynamic links. When the source node needs route, it disseminates a Route REQuest(RREQ) message to its neighbor nodes in hop by hop manner. A Route REPly(RREP) message is sent back to the source whether it is newly found route or existing valid route. Attackers generate large amount of RREQ packets with out-of-domain IP address as its destination node. During route discovery process of AODV protocol, attackers deplete communication energy and processing resources. So I propose Petri Net (PN) design approach to suppress redundant RREQ packets. It is a power saving technique that is effective to elongate operational lifetime of MANETs. Duplicate copies of RREQ packets received at node are discarded and each node remembers only next hop to reach the host and not the whole route.**

Keywords: Petri net, AODV, Flooding attack, Mobile ad hoc network.

I. INTRODUCTION

When source code initiates a data session but it does not have any route information, it searches for a route by sending Route REQuest(RREQ) packet. Each packet has a unique identifier, nodes can detect and drop duplicate packets and node records source node information in route table. First, a Dual Defense Wall System(DDWS) is used to mitigate from flood attacks. The first hop intermediate node around the attacker and destination node constitute the first defensive wall RREQs can be suppressed by first defensive wall, by monitoring the frequency of RREQs and reject flooding attacks. To conserve limited bandwidth of MANET nodes, I propose PN design approach for avoiding useless RREQ packets and excluding fraudulent RREQ traffic loads. A Petri net (also known as a place/transition net or P/T net) is one of several mathematical modeling languages for the description of distributed systems for process analysis.

Duplicate copies of RREQ packets received at any node are discarded. Each intermediate node receiving this RREP creates a forward route to the destination. Thus, each node remembers only the next hop required to reach any host, not the whole route. Once the source node receives RREP, it may start to forward data packets to the destination. If the source node later receives a RREP message containing a shorter route, it may update its routing table for that destination and adopt the shorter route instead of the old one. In a conventional wired-networking environment, flooding attacks were once notorious for firing pervasive Denial-of-Service (DoS) attacks or/and Distributed DoS (DDoS) attacks on the crucial Servers. During route discovery process of AODV protocol, attackers may maliciously deteriorate the broadcast problem to deplete communication energy and processing resources on legal MANET nodes. Upon receiving RREQ packets for the first time, any legal node in an AODV-based MANET has the obligation to re-disseminate the message. Using the RREQ flooding attack, attackers would issue a massive number of RREQ packets with an out-of domain IP address as its destination node. To explore possible solutions for prior flooding attacking issues, a dual defense wall system (DDWS) was elaborated to mitigate the impact from flooding attacks.

II. RREQ FLOODING ATTACKS

In MANETs, nodes are receptive to being captured, compromised, and hijacked because they are units capable of roaming independently. The attacking pattern by RREQ flooding attack firstly selects fraudulent IP addresses which are not inside the legal IP domain defined/configured in the target MANET. Then the malicious node issues RREQ packets containing such an out-of-domain IP to call for relay service from its neighboring nodes. The reception and re-dissemination of fraudulent RREQ packets would consume much energy, and it is worse for nodes installed with limited battery without recharging gear. The excessive route entries would be added and maintained in the route table. The whole wireless network is possibly crowded with fraudulent RREQ packets fired by malicious nodes. Since these destination addresses are invalid, no node could answer RREQ packets, the reverse routes in the routing table of intermediate nodes will be occupied for longer time and it forms a heavy load on the routing table

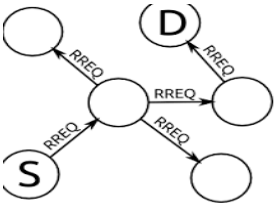


Fig.1.RREQ floods

III. EXISTING APPROACH

The flooding attack prevention (FAP) scheme to resist against RREQ flooding attacks. By FAP, one scheme composed of "Neighbor Suppression" had been suggested to resist the RREQ flooding attack. the processing priority of an RREQ from a specific node is stored. The drawbacks are RREQ frequency threshold is mentioned. The denial threshold of stop forwarding RREQs for the neighbor nodes cannot be conducted clearly. For each intermediate node, it did not give any feasible approach to learn of the status of neighbor nodes. Once the node has been suppressed due to excessive RREQs from some unstable but legal node, it is impossible to recover RREQ relay service back forever for some legal nodes. Since each RREQ priority depends on its sender's firing frequency, each node must record every RREQ it receives and reserve the space to hold the priority value after calculating frequency.

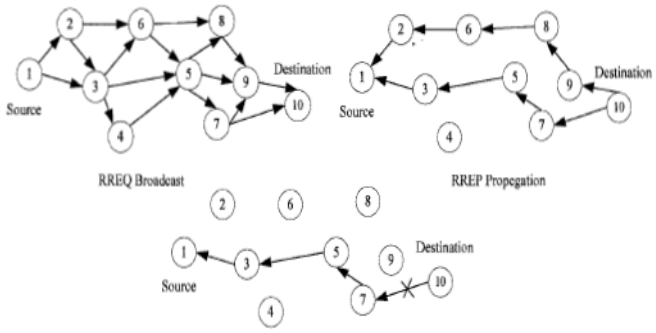
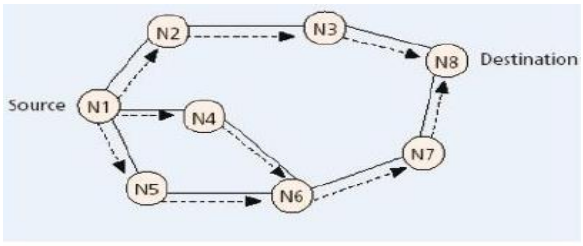


Fig.2. RREQ and RREP messages

A. Route Discovery in AODV-based Protocol

When a source needs to initiate a data session to a destination but does not have any route information, it searches for a route by flooding a ROUTE REQUEST (RREQ) packet. Each RREQ packet has a unique identifier so that nodes can detect and drop duplicate packets. An intermediate node, upon receiving a non-duplicate RREQ, records the previous hop and the source node information in its route table. It then broadcasts the packet or sends back a ROUTE REPLY (RREP) packet to the source if it has a route to the destination. The destination node sends a RREP via the selected route when it receives the first RREQ or subsequent RREQs that
traversed a better route

To manifest the hop-count metric, the relayed RREQ packets are incremented one in the Hop Count field. Before broadcasting the RREQ, the originating node buffers the RREQ ID and the Originator IP address (its own address) of the RREQ for PATH_DISCOVERY_TIME, which is given a default value by 2× NET_TRAVERSAL_TIME. Hence node would discard RREQs without reprocessing and re-forwarding after checking these newly arriving <RREQ ID, Originator IP Address> pair with the one existing in its buffer. To prevent a routing loop, the RREQ packet contains a unique RREQ ID identifying the particular RREQ when taken in conjunction with the originating node's IP address. When a node receives the RREQ, it checks <RREQ ID, Originator IP Address> pair. If the RREQ has been received, the node will discard the duplicated RREQ silently The MANET topology changes over time because of node mobility. AODV-based nodes therefore would perform route maintenance when each node monitors the links to the nodes it is directly connected to.



Path discovery in AODV

B. RREQ Flooding Attack in MANETs

In MANETs, nodes are receptive to being captured, compromised, and hijacked because they are units capable of roaming independently. Since tracking down mobile nodes is difficult, attacks by compromised nodes are far more damaging and much harder to detect. For limited energy budget in most mobile nodes, the energy depletion phenomenon could be deteriorated by roaming attacking nodes. One potential RREQ flooding attack in MANETs The attacking pattern by RREQ flooding attack firstly selects fraudulent IP addresses which are not inside the legal IP domain defined/configured in the target MANET. Then the malicious node issues RREQ packets containing such an out-of-domain IP to call for relay service from its neighboring nodes. Two precious resources are wasted instantly One is that the reception and re-dissemination of fraudulent RREQ packets would undoubtedly consume much energy, and it would become worse for those nodes installed with limited battery without recharging The
other one is that excessive route entries would be added and maintained in the route table of each nodes for trying to conduct the path discovery.

To reduce the congestion caused by the dissemination of RREQ packets issued by all nodes in the MANET, three major controlling techniques are utilized in : rate of firing RREQ packets, the waiting time for the arrival of RREP packet, and prolongation of waiting times in case of resending RREQ packet without receiving the responsive RREP packet. On controlling the rate of firing RREQ packets, it is requested that a node should not originate more than RREQ_RATELIMIT RREQ messages

per second The first time a source node broadcasts a RREQ packet, it awaits NET_TRAVERSAL_TIME milliseconds for the reception of a RREP message. IF a RREP is not received within that time, the source node then is allowed to send a new RREQ packet. Finally repeated trials by a source node at route discovery for a single destination. However malicious nodes would violate such abovementioned rules.

Ignoring the limitation by parameter RREQ_RATELIMIT, they would try to originate massive RREQ packets in high frequency using out-of-domain IP addresses in the "Destination IP Address" field of the RREQ packet. They would also resend RREQ packets without waiting for the arrival of RREP packet, and even they may send excessive RREQ packets with maximum TTL value of IP layer in a burst manner. To some extreme scenario, the whole wireless network is possibly crowded with fraudulent RREQ packets fired by malicious nodes. Since these destination addresses are invalid, no node could answer RREQ packets

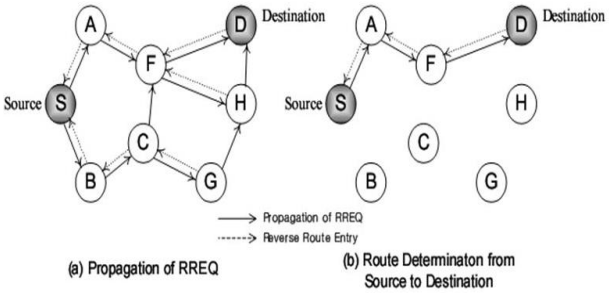


Fig.4. RREQ in MANET

IV. DUAL DEFENSIVE WALL SYSTEM (DDWS)

The first is that attackers are apt to disseminate massive RREQ packets without obeying the rule which the RREQ sending rate should not exceed RREQ_RATELIMIT. The second is that attackers adopt fraudulent IP addresses as destination nodes to trigger bogus route discoveries. We refer to nodes that are one-hop away (i.e., in the direct range of transmission) as "Direct-Hop Nodes" (DHNs) and the covering area under a node's transmission range

A. Data Structures on Priority Assessment Index

An index scheme was designed to monitor each node issuing RREQ packets, whether it is a legal or a malicious node. The proposed approach to alleviate RREQ flooding attacks is termed as RREQ Priority Assessment Index (PAI) scheme, and abbreviated as RREQ_PAI scheme The RREQ_PAI scheme configures two pieces of data structures: DS_1 and DS_2, and are shown as follows:
(1)DS_1: Field format of DHN Table (DHNT):
(2) DS_2: Field format of RREQ_PAI

To grasp the DHN status around each legal node, the proposed DDWS utilizes the Hello messages to collect DHN's information and creates the DHNT defined in DS_1. In principle, a node may offer connectivity information by broadcasting local Hello messages. A node should only use Hello message if it is part of an active route. Every HELLO_INTERVAL milliseconds, the node checks whether it has sent a broadcast (e.g., a RREQ) within the last HELLO_INTERVAL. If it has not, it may broadcast a RREP with TTL=1, called a Hello message with the RREP message fields set by <Destination IP Address, Destination Sequence Number, Hop Count, Lifetime>=<The node's IP Address, The node's latest sequence number, 0, ALLOWED_HELLO_LOSS * HELLO_INTERVAL>. Whenever a node receives a Hello message from a neighbor, the node should make sure that it has an active route to the neighbor, and create one if necessary. For the first two fields in DHNT, <DHN IP address, AOL> can be recorded by exchanging Hello message with its DHNs in the node's hamlet. The field AOL indicates that the value "1" means that the route is active and the value "0" is lost. The third field, RREQ_PAI, is derived from the RREQ_PAI table. This RREQ_PAI values imply that the node is an attacker with the strongest and moderate tendency when RREQ_PAI is 3 and 2 respectively. It implies that it is a legal node when RREQ_PAI is 1.

Before proceeding with a data session in mission-oriented MANET, the legal nodes are requested to exchange Hello messages per PAI scheme The AOL (Active Or Lost) status of legal DHNs is recorded in its DHNT as well. Each entry in RREQ_PAI table represents a specific DHN around itself. The two fields, <RREQ Number, RREP Number> count the total numbers of RREQ and RREP received, and the field, Time Stamp, records the instant when receiving the first RREQ packet for a specific DHN. The proposed cooperative DDWS provides a flexible and efficient mechanism which allows downgrading/upgrading on RREQ_PAI value to reflect reasonable changing status on all DHNs in any legal node's hamlet. Such techniques to downgrade/upgrade on RREQ_PAI value are implemented by the threshold policies.

B. Threshold Policies of RREQ_RATELIMIT

Given an instant, dynamic PAI on each DHN, each incoming packet passes through the PAI mechanism before being forwarded to the next-hop neighbor. Legal nodes neighboring this DHN should hold RREQ packets and then forward them by the threshold policies of RREQ_RATELIMIT. the RREQ_RATELIMIT rule presents two control parameters: Max_Threshold and Min_Threshold that can be calculated by the following expressions:
Max_Threshold = m × RREQ_RATELIMIT (1)
Min_Threshold = RREQ_RATELIMIT (2)
The value m is the numbers of DHN and the parameter RREQ_RATELIMIT default value is configured to 10. The above two system parameters, Min_Threshold and Max_Threshold, will be used to be decision metrics on identifying which level of DHNs would stay in one of three levels: normal, greylist and blacklist. One identification scheme adopts the flow rate (FR) of RREQs received as the classifying rule and is given by:

Normal FR ≤ Min_Threshold ≤ Grey FR ≤ Max_Threshold ≤ Black FR (3)

For example, in the current period for some normal DHN, it is found that its flow rate appears to be abnormal and getting higher (exceeding Min_Threshold), but not exceeding the Max_Threshold yet. To be prudent, it is better to classify such a DHN into the greylist rather than the blacklist by just only one observation because such an abnormal flow rate may be transient and unstable accidents. Logically, such a normal-greylist blacklist approach is an innovative scheme

C. Level of Priority and RREQ_PAI Grading

While processing RREQ packets passing by, each node categorizes its neighbor nodes issuing RREQ packets into one of these three levels according to the current disseminating metrics on RREQ streaming behavior. Numerically, to assess the malicious tendency for each DHN around a legal node, we use RREQ_API=1, 2and 3 to specify the corresponding levels of normal, greylist and blacklist respectively. Level 3 is the strongest tendency (blacklist) which this DHN is trustless and regarded as an attacker. Any legal node should discard all packets received and refuse further forwarding service from this attacker's packets. Level 2 (greylist) is the moderate tendency implying that this DHN is considered to a potential attacking suspect. Level 1 (normal) implies that the DHN is treated as a legal node and the relay service on it will be conducted normally. Level of Priority and RREQ_PAI Setting (RREQ_PAI) Malicious tendency Forwarding service by router nodes RREQ_PAI = 1 Normal (Legal node) Router node holds packets and forwards them per threshold policy of RREQ_RATELIMIT RREQ_PAI = 2 Greylist (Moderate) This DHN is treated as a gray node. The relay service is conducted with downgrading/upgrading scheme. RREQ_PAI = 3 Blacklist (Strongest) Forwarding service is rejected on this DHN and discards its packets silently.

V. PN Design Approach

Petri Nets (PNs) are a graphical mathematical modeling tool application to many systems. They are a promising tool for describing and studying information processing systems that are characterized as being concurrent, asynchronous, distributed, parallel, nondeterministic and/or stochastic. A PN is identified as a particular kind of bipartite directed graph populated by three types of objects. They are places, transitions, and directed arcs connecting places and transitions. A PN is a 5-tuple, PN ={P, T, I, O, M0} where:

P = {p1, p2, …, pm} is a finite set of places, where m > 0;

T = {t1, t2, …, tn} is a finite set of transitions with P∪T ≠ ∅ and P∩T = ∅, where n > 0;

I: P × T → N is an input function that defines a set of directed arcs from P to T,
where N={0, 1, 2…};

O: T × P → N is an output function that defines a set of directed arcs from T to P.

M0: P → N is the initial marking

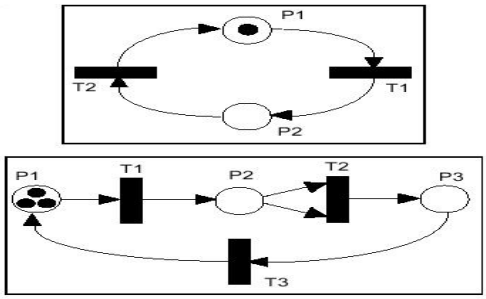


Fig.5. Petri net design

A. Petri Net Concepts

For the proposed approach, PAI can be upgraded or downgraded dynamically.In the DDWS framework, the defensive task is conducted via a two-layer defensive scheme. The first defensive wall (FDW) is executed by DHNs around node originating RREQs using information stored in its DHN Table. The corresponding PN notations for states (places) and transitions (events) are defined in PN_Notation Hence those RREQ packets originated from non-registered suspicious node can be discarded by the FDW.

PN_Notation 1 There are seven transitive states (places) for a router node during modeling the DDWS system:
P1: Buffer for arriving RREQ packet.
P2: DHN Table where the IP address of incoming RREQ is present or absent.
P3: Buffer holding RREQ packets under processing.
P4: DHN Table where the PAI state is in one of three basic states.
P5: RREQ_PAI=1 for the entry node originating RREQ (Normal).
P6: RREQ_PAI=2 for the entry node originating RREQ (Greylist).
P7: RREQ_PAI=3 for the entry node originating RREQ (Blacklist).

PN_Notation 2 Given the set of transitive states (places) B= {P1, P2, …,P7}, we define the state
transitions (events) for a router node during modeling the DDWS system:
t1: Transition 't1' is enabled when RREQ packet arrives in place 'P1'.
t2: Transition 't2' is enabled when non-registered RREQ packet has been removed.
t3: The IP address of arriving RREQ is absent in DHN Table.
t4: The IP address of arriving RREQ is present in DHN Table.
t5: RREQ_PAI state is 2 (moderate).
t6: RREQ_PAI state is 3 (strongest).
t7: RREQ_PAI state is 1 (normal).
t8: Enabled when time duration D2*b had been elapsed and no RREQ reception beyond D2.
t9: Forwarding RREQs, and RREP response after D1*a time duration.
t10: Forwarding RREQs, and it is found that (1/Max_Threshold)< ΔT*c ≦(1/Min_Threshold).

t11: Checking ΔT, and it is found that ΔT≦(1/Max_Threshold).
t12: Forwarding RREQs, no RREP response after D1 time duration.
t13: Checking ΔT, and it is found that ΔT≦(1/Max_Threshold).
t14: Enabled when D2 has been elapsed and no RREQ reception beyond D2.
*a: D1=2× NET_TRAVERSAL_TIME
*b: D2=8× NET_TRAVERSAL_TIME
*c: ΔT=time interval between two arriving successive RREQs.
If the RREQ reception frequency exceeds (1/Max_Threshold), it implies that a storm flooding scene emerges and a urgent action should be taken to reject forwarding immediately.

C. Lifetime elongation approached by saving power consumption

From the viewpoint of power-saving requirement, one of the major design issues to prolong operational lifetime of MANET is to efficiently manage power consumption under RREQ flooding attack. the radio power consumption including transmitting and reception incurred would be saved considerably as well. On energy budget of nodes in an AODV-based network, each hop-wise transmission of an RREQ packet is counted as the energy expenditure composed of transmission energy associated a couple of receiving energy expended by its DHNs. Obviously, the power consumption has been improved considerably.

VI. CONCLUSION

For the RREQ flooding attack attackers would launch massive RREQ packets with an out-of-domain IP address being its destination node. The forwarding services conducted by all the intermediate nodes would be resulted in considerable power consumption among legal mobile nodes, and hence the operational lifetime for the whole Ad Hoc network would be alleviated accordingly. To improve the operational lifetime for Ad Hoc networks, the proposed power-saving technique can be applied to elongate the operational lifetime of AODV-based MANETs economically and effectively. The proposed approach can suppress redundant RREQ packets by the co-operation of destination node and neighbor nodes under one-hop range of attacking node. On qualitative analysis, a Petri Net design is provided for in-depth understanding system profile. With almost above 80% improvement ratio on average power consumption in the exemplified scenario, the proposed power-saving approach indeed provides a feasible cost-efficient technique to enhance the longevity of the Ad Hoc network.

REFERENCES

[1] W. Keiss, M. Mauve, A survey on real-world implementations of mobile ad-hoc networks, Ad Hoc Networks 5 (2007) 324-339.
[2] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, J.-P. Sheu, The broadcast storm problem in a mobile ad hoc network, Wireless Networks 8 (2002), 153-167.
[3] Q. Gu, P. Liu, C.-H. Chu, Analysis of area-congestion-based DDoS attacks in ad hoc networks, Ad Hoc Networks 5 (2007) 613-625.
[4] P. Yi, Z. Dai, Y. Zhong, S. Zhang, Resisting flooding attacks in ad hoc networks, in: IEEE ITCC 2005, 2 (2005) 657-662.
[5] N. Komninos, D. Vergados, C. Douligeris, Detecting unauthorized and compromised nodes in mobile ad hoc networks, Ad Hoc Networks 5 (2007) 289-298.
[6] S. Li, Q. Liu, H. Chen, Tan, A New method to resist flooding attacks in ad hoc networks, in: IEEE WiCOM 2006, pp.1-4, Sep. 2006.
[7] J.-S. Lee, P.-L. Hsu, Implementation of a remote hierarchical supervision system using Petri Nets and agent technology, IEEE Transactions of Systems, MAN, and Cybernetics – Part C: Applications and Reviews, 37 (2007).
[8] R. Davidrajuh, B. Lin, Exploring airport traffic capability using Petri net based model, Expert Systems with Applications, 38 (2011) 10923-10931.