ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

An Efficient Attack Detection Method in Proactive Source Routing Protocol for Mobile Adhoc Networks

S.Kanagalakshmi, N.Pappu Sivanantham

M.E, Dept of CSE Specialization in Network, J.P College of Engineering, Ayikudi, India

Assistant Professor, Dept of CSE, J.P College of Engineering, Ayikudi, India

ABSTRACT: The main objective of this project is to provide a data transmission for mobile devices and avoid the packet loss. Data forwarding regulates how packets are taken from one link and put on another. Routing determines what path a data packet should follow from the source node to the destination.Proactive source routing protocol is used to find the neighbor and neighbor's neighbor by sending HELLO request and also this protocol reduce the routing overhead and time delay. Dynamic distribution detection technique is used to detect the attacked node from the network for avoiding the data losses and Flooding attack detection technique is used to prevent many attacked node in network. This frame work can improves timeliness of data delivery by reducing waiting time of the nodes which to be in the communication.

KEY WORDS*:* PACKET LOSS, MANET, WAITING TIME, MOBILE DEVICES, DATA TRANSMISSION.

I.INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. An Ad-hoc network is a temporary network connection created for a specific purpose. Each user has a unique network address that is recognized as the part of the network. Collection of nodes that do not rely on a predefined infrastructure. Auto-configurable network and self-organizing. Nodes are mobile and hence have dynamic network topology. Nodes in ad-hoc networks play both the roles of routers and terminals.

OLSR [1] protocol is suitable for large adhoc networks. But latency should more in the Mobile ad hoc networking: imperatives and challenges the Self-configuring network of mobile routers (and associated hosts) connected by wireless links. This union forms a random topology. Routers move randomly free. Topology changes rapidly and unpredictably. But it can create the dynamic network and data loss occurs. In the Ad-Hoc On-Demand Distance Vector Routing Builds on DSDV algorithm and the improvement is on minimizing the number of required broadcasts by creating routes on an on-demand basis (not maintaining a complete list of routes). Broadcast is used for route request the Advantages are uses bandwidth efficiently, is responsive to changes in topology, is scalable and ensures loop free routing the disadvantages are Nodes use the routing caches to reply to route queries. The Result is "uncontrolled" replies and repetitive updates in hosts' caches yet early queries cannot stop the propagation of all query messages which are flooded all over the network. In the Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks Based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. 2 major phases: Route discovery – uses route request and route reply packets and Route maintenance – uses route error packets and acknowledgments. The advantage is No periodic hello message and fast recovery - cache can store multiple paths to a destination. The limitations are the packets may be forwarded along stale cached routes. It has a major scalability problem due to the nature of source routing. Same as AODV, nodes use the routing caches to reply to route queries. In the multihop network the data forwarding is the major issue. Data forwarding regulates how packets are taken from one link and put on another. Routing determines what path a data packet should follow from the source node to the destination. Opportunistic data forwarding refers to a way in which data packets are handled in a multihop wireless network. Where an intermediate node looks up a forwarding table for a dedicated next hop, opportunistic data forwarding allows potentially multiple downstream nodes to act on the broadcast data packet. One of the initial works on opportunistic data forwarding is selective diversity forwarding. A lightweight proactive source routing (PSR) protocol to facilitate opportunistic data forwarding in MANETs. In PSR, each node maintains a breadth-first search spanning tree of the network rooted at it. This information is periodically exchanged among neighboring nodes for updated network topology information. Thus, PSR allows a node to have full-path information to all other nodes in the network, although the communication cost is only linear to the number of the nodes. This allows it to support both source routing and conventional IP forwarding. if any attack that means any node can't forward the information there is the major issue in the network. Proactive source routing protocol refers to a way in which data packets are handled in a multi-hop wireless network. Dynamic distribution detection technique is used to detect the attacked node form the network for avoiding the data losses. Flooding attack prevention technique is used to prevent many attacked node in network. Flooding attack prevention technique is used to prevent multiple attacked nodes in network by separating nodes into three types that are friend node, acquaintance node and stranger node. Using this way this technique find out the attacked node so this frame work can improves timeliness of data delivery by reducing waiting time of the nodes which to be in the communication and also reduce the data loss.

II.RELATED WORKS

Significant works have been done in securing the ad hoc network. Some researches defined the method for secure routing but secure routing also can not able to handle the flooding attack. The first flooding attack prevention (FAP) method was proposed in [6]. In their paper, first they described RREQ flooding and data flooding. This was the first paper that addressed the prevention of flooding attack in ad hoc network. The authors proposed the separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbor suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value. To deal with data flooding they used path cutoff method. In this method when node identifies that sender is originating data flooding then it cutoff the path and sends the route error message. In this way attack is prevented up to some extent but the disadvantage of this method is flooding packet still exists in the network. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less than RATE_LIMIT then the request is processed otherwise check whether it is less than BLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less than BLACKLIST_LIMIT then put the RREQ in the delay queue and process after queue time out occurs. This method cans Handel the network with high mobility. In [12], the author analyzed the flooding attack in anonymous communication. They used the threshold tuple which consist of three components: transmission threshold, blacklist threshold and white listing threshold. if any node generates RREQ packet more than transmission threshold then its neighbor discards the packet if it crosses the transmission threshold more than blacklist threshold then it Blacklist the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node. In [1], the author used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non-trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they define the three threshold value. If any node receives the RREQ packets then checks the relationship and based on that it checks for the threshold value if it is less than the threshold then forward the packet otherwise discard the packet and blacklist the neighbor node. The main problem with this method was it does not work well with higher node mobility.

To prevent the flooding attack in MANET that can work well in higher node mobility situation, we proposed a novel technique which uses the trust estimation function and delay queue in basic AODV routing protocol.

In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. A single threshold is set up for all the neighbor nodes. The given solution is neighbor suppression. In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated. After the data flooding has occurred, the steps are being initiated to curb the flooding attack. Similar solutions are proposed in [12] where a rate-limitation component is added in each node. This

component monitors the threshold limit of request packets sent by the neighboring nodes and accordingly, drops the packets if the limit is exceeded.
Data Flooding is also addressed in this work. In our scheme we have categorized the neighboring nodes as strangers, acquaintances and friends with different thresholds Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. and provide a cutoff once the threshold is reached by using the AODV protocol.

III.PROPOSED SYSTEM

1) DYNAMIC DISTRIBUTION DETECTION TECHNIQUE

To proposed and analyzed a Dynamic distribution detection algorithm is used to avoid the data loss problem in a multihop network. First to initialize the network for calculating distance and data carrying is very difficult in multihop network .If any data may lost its very hard to find the solution. The allocating the source and destination and calculate the distance between them. There are many alternative path and intermediate nodes are available between source and destination. So the distance based the shortest path may chose and send. In the network the each message can be encrypted after that that can send to the destination. If node can leak the message based upon energy or other damage that node called attacker node. Dynamic distribution detection technique is used to detect the attacked node form the network for avoiding the data losses. These techniques are used for better data transmission. Based upon the technique the leakage node can detected via nearby and chosen the alternative node in the path that information send to source and destination after that it can allow performing operation. Using these techniques the multihop network communication can done effectively.

2) FLOODING ATTACK PREVENTION TECHNIQUE

Flooding attack prevention technique is used to prevent the multiple attacked node in network for avoiding the data loss. This technique separate the nodes into three types that are friend node, acquaintance node and stranger node. Friend node means it satisfy the threshold value for data forwarding in network. Acquaintance node may be forward the data to next node because some process is processing there so the next process is waiting in queue until that node finish the process but after that sometimes node do not forward the data to next node because the threshold value may not be enough. Stranger node is one type of node they should not forward the data to next node because that threshold value very low. Here Boolean value is used for stop and start the process. If the Boolean value is 0 means it starts the process otherwise stop the process. Using this way we can prevent many attacked node in network and avoid the data losses.

All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes will be strangers to each other. A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into friends (most trusted), acquaintances (trusted) and strangers (not trusted). In an ad hoc network, the relationship of a node i to its neighbor node j can be any of the following types
i. Node i is a stranger (S) to neighbor node j :
Node i have never sent/received messages to/from node j. Their trust levels between each other will be very low. Any new node entering ad hoc network will be a stranger to all its neighbors. There are high chances of malicious behavior from stranger nodes.
ii. Node i is an acquaintance (A) to neighbor node j
Node i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.
iii. Node i is a friend (F) to neighbor node j :

10.15680/ijircce.2015.0303092

Node i sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less.

IV. PSEUDOCODE

FLOODING ATTACK PREVENTION ALGORITHM

```
Begin
If an intermediate node send packet to node _i‘ then
{
Analyse the Network Parameters Phase
{
MEASURE Dr (u),Pwr (u),f(w)
IF (Dr (u),Pwr (u),B(w) are enough) then
Node _i is a friend and Z[i] = 0 then
Increment X[i]
Forward the data packet
Else
If X[i] > Xpf
Drop the data packet and set
Z[i] = 1
}
Analyse the Network Parameters Phase
{
MEASURE Dr (u),Pwr(u),f(w)
IF(Dr(u),Pwr(u),B(w) are may be low or enough) then
Packet waits in queue some time
Node _i ‘is an acquaintance and Z[i] = 0 then
Increment X[i]
Forward the packet
Else
If X[i] > X pa
Drop the data packet and set
Z[i] = 1
}
Analyse the Network Parameters Phase
{
MEASURE Dr (u), Pwr (u) ,f(w)
IF (Dr (u), Pwr (u), B (w) are not enough) then
If node _i‘is an stranger and Z[i] = 1 then
Drop the data packet
}
End
}
```

The packets are successfully received by n0 else if Xrs < X, the packets are dropped. Again if the n3 is sending X packets to n0, is compared with the threshold value of acquaintance. If Xra > X then the packets are successfully received by n0. Else if Xra < X, the packets are dropped. Similarly the transfer of X packets from n4 is compared with the threshold value for friend (Xrf). The same procedure is followed for preventing DATA flooding attacks from the neighboring nodes. Let X[i] denotes the number of packets delivered from neighboring node i, where $1 \leq i \leq n$. Xrf, Xra and Xrs are the threshold values as discussed in the previous section. Let Z[i] is a Boolean array to activate or stop the process.

VI. EXPERIMENTAL RESULTS

To analyze the performance of the proposed system lots of simulation experiments are conducted. The proposed system is implemented in Network Simulator (NS2). In the simulation experiments several parameters are used. They are listed in the below table.

Number of Nodes	50
Area Size	1000 x 1000
Target Size	[500,500]x [500,500]
Simulation Duration	50

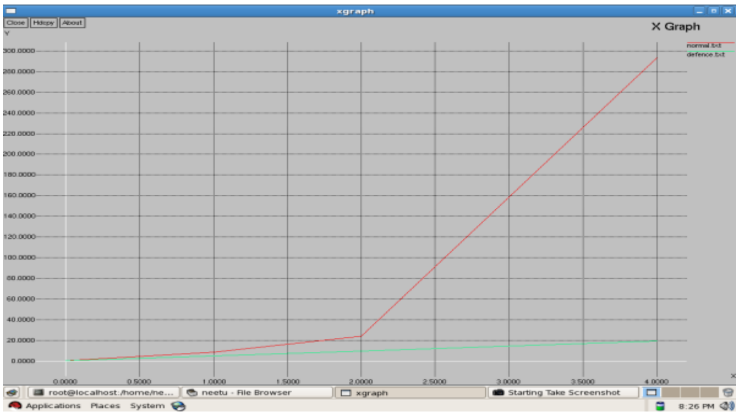

Figure 1: Comparison of Routing overhead by varying malicious nodes in scenario 40 nodes

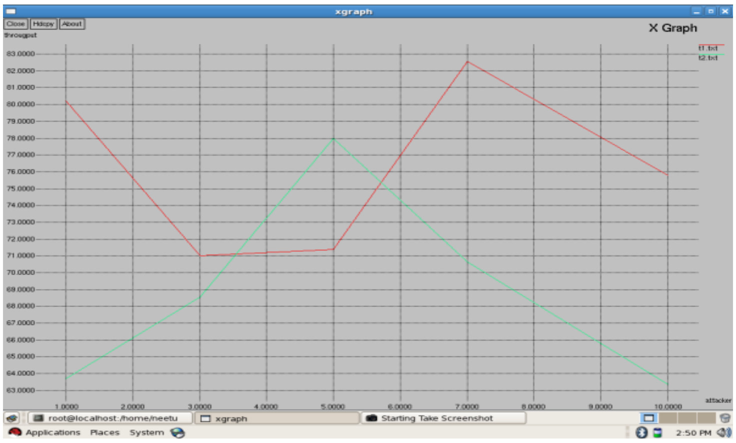

Figure 2: Comparison of Throughput by varying malicious nodes in scenario 10 nodes

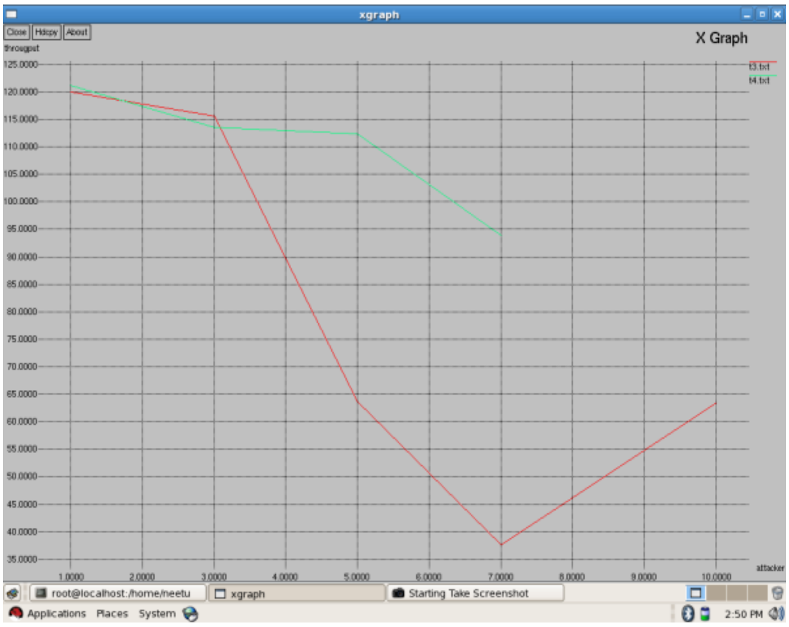

Figure 3: Comparison of Throughput by varying malicious nodes in scenario 20 nodes

We propose the following solution. To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. If Xrs, Xra, Xrf be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, Xrf > Xra > Xrs. If Yrs, Yra, Yrf be the DATA flooding threshold for a stranger, acquaintance and friend node respectively then Yrf > Yra > Yrs. If the specified threshold level is reached, further RREQ packets from the initiating node are ignored and dropped. Thus, flooding is prevented in the routing table.

Node0 is an intermediate node, denoted by n0. Let n1, n3, n4 are the three neighboring nodes to n0 where n4 is a stranger node, n3 is an acquaintance node and n1 is a friend node. Each node is sending X number of packets to n0. For RREQ flooding attacks prevention, when the packets are being sent from the n4 to n0, the number of packets sent (X), is compared with the threshold value of stranger.

VII. CONCLUSION

Proactive Source Routing (PBR) Protocol is used to support opportunistic data forwarding in MANET and that protocol is used to handle the data packets in a multihop network, reduce the routing overhead, and increase the data transmission rate. The proposed Dynamic distribution detection technique is used to Detect the attacked node form the network by checking the Quality Of Service parameters for each node in the network then give the attacker node details for avoiding the data losses. Then Flooding attack prevention technique is used to prevent multiple attacked node in network. Both the techniques are used for better data transmission in MANET. In future the nodes are checking with the hash value and give security to nodes. The simulation result shows that the algorithm is feasible and has superior performance.

REFERENCES

[1] George Theodorakopoulos and John S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE JSAC, Vol.24. No.2, February 2006.

[2] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks I(2003)pages 13-64, Elseiver publications.

[3] Jie Li and Jien Kato, Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine, April 2008

[4] Panagiotis Papadimitratos and Zygmunt J.Haas, Secure Data Communication in Mobile Ad hoc Networks, IEEE JSAC, Vol.24, No.2, February 2006.

[5] P.Papadimitratos and Z. Hass and P.Samar. The Secure Routing Protocol (SRP) for Ad hoc Networks. Draft-papadimitratos-secure-routing-protocol-00.txt, Dec.2002.

[6] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang: Resisting Flooding Attacks in Ad Hoc Networks. Coding and Computing. ITCC 2005. International Conference on Information Technology Volume 2, Issue, April 2005, 657 – 662.

[7] A. A. Pirzada, A. Datta and C. McDonald, Incorporating Trust and Reputation in the DSR protocol for Dependable Routing, Computer Communications, Special issue on Internet Communications Security, Vol. 29, pages 2806-2821, Elsevier Press, 2006.

[8] Revathi Venkataraman, M. Pushpalatha: Security in Ad Hoc Networks: An extension of dynamic Source Routing in Mobile Ad Hoc Networks. In proceedings of the 10th IEEE International Conference on Communication Systems, Singapore, 2006.

[9] C.Siva Ram Moorthy, B.S. Manoj: Ad hoc Wireless Networks Architectures and Protocols, Prentice Hall, 2004.

[10] Y.Sun et al., Defense of trust management vulnerabilities in distributed networks, IEEE Communications Magazine, February 2008.

[11] Y.Sun et al., Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc networks. IEEE JSAC, vol.24, no.2, Feb.2006

[12] Venkat Balakrishnan et al. Mitigating Flooding attacks in Mobile Ad hoc Networks Supporting Anonymous Communications. In proceedings of the 2nd International Conference on Wireless and Ultra Wideband Communications (Auswireless 2007).

[13] Yi Ping, Hou Yafei, Bong Yiping, Zhang Shiyong & Dui Zhoulin, Flooding Attacks and defence in Ad hoc networks. Journal of Systems Engineering and Electronics, VoL. 17, No. 2, pp. 410- 416, 2006.

[14] L. Zhou and Z.J. Haas. Securing Ad hoc Networks. IEEE Networks, vol.13, no.6, pp.24-30. 1999.

[15] Young-Bae Ko and Nitin Vaidya, Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom‘98), pages 66–75, October 1998.

[16] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1 —Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks — Proceedings of the Seventh International Conference on Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)0- 7695-2736-1/06 $20.00 © 2006

[17] Bo-Cang Peng and Chiu-Kuo Liang ‖Prevention techniques for flooding attack in Ad Hoc Networks‖

[18] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao —prevention of flooding attack in mobile ad hoc network‖. International Conference on Advances in Computing, Communication and Control (ICAC3‘09).

[19] Ping Yi, Yue Wu and Futai Zou and Ning Liu, —A Survey on Security in Wireless Mesh Networks‖, Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[20] Nishu Gag and R.P.Mahapatra, —MANET Security Issues ,‖ IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[21] S.kannan,T.Kalaikumaran,S.Karthik and V.P.Arunachalam —A Review on attack prevention methods in MANET‖ journal of Modern Mathematics and Statistics 5(1): 37-42, 2011

10.15680/ijircce.2015.0303092