Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.375 – 379

Restructuring DSR for Preventing Flooding Attack

Atul Kumar Agrawal
Asst. Prof., ATC INDORE, agrawal273@yahoo.com

Abstract - Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. MANET has no clear line of boundaries for both legitimate network users and malicious attackers. In the presence of malevolent nodes, important challenges in MANET are to design the robust security solution that can protect MANET from various routing attacks. Dynamic Source Routing (DSR) algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. High mobility exist in ad-hoc network, we cannot get the route for longer duration. Hence, DSR algorithm finds an alternative route when the existing communicating route are not exits. It becomes a time consuming process if the communicating route fails frequently. This paper presents a new method to improve performance of DSR in Ad Hoc Network.

Keyword: MANET, Flooding Attack, DSR

1. INTRODUCTION

Wireless communications are gaining popularity because of the availability of inexpensive wireless devices such as laptop, PDA, mobile phones etc. Now a day's not only the mobile devices are getting smaller and cheaper but they can able to run more application and network services. Wireless cellular systems are in use since 1980s. Cellular systems operate with the aid of a centralized supporting structure such as an access point or base stations. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. But the presence of a fixed supporting structure limits the adaptability of wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks which can work without any central administration. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless connection. Due to mobile nodes, the network topology may change

rapidly and unpredictably over time. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to mobile about while communication with others. The path between each pair of the nodes may have multiple connections and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Generally there are two distinct approaches of wireless networks

INFRASTRUCTURE BASED NETWORK

In this type of network the mobile node can able communicate with each other with the help of access point or some central base station which provide the radio coverage for communication. The access point does not only control the medium access, but also act as a bridge to other wireless or wired network. Several nodes, called stations are connected to access points. The station and the access point which are within the same radio coverage form a Basic Service Set (BSS) and different BSS are connected to each other via a distribution system (DS). A distribution system connected to various BSS via access point forms a Extended service Set (ESS).

AD HOC NETWORK

Ad hoc network is collection of wireless node which does not requires any infrastructure to work. Node can able communicate with each other if they are in the coverage range of each other. In ad hoc network, the complexity of each node is higher because every node has to implement medium access mechanism.

2. FLOODING ATTACKS

In the flooding attack the malicious or selfish node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network The flooding attack is possible in all most all the on demand routing, even in the secure on demand routing ARAN, SRP ,Ariadne , SAODV etc. On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In the route discovery the source node flood the network by sending the RREQ packets .Because the priority of the RREQ control packet is higher then data packet then at the high load also RREQ packet are transmitted. A malicious node exploits this feature of on demand routing to launch the attack. Flooding attack is hard to detect because it seems as a normal node with frequent broken routes due to high mobility. The MANET has some salient characteristics like continuous changing topology, limited battery, limited bandwidth etc. So intruders try to exploit properties of the network to launch this attack. Some RFCs of routing algorithm specifies the maximum number of RREQ packets that can be originated by any node per second. But the malicious node can able to change this rate limit.

Flooding attack can be classified in two categories based upon the type of packet used

1. RREQ flooding

2. DATA flooding

RREQ FLOODING

In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval. In this, the intruder or the malicious node generate many route request packet (RREQ) and disable the limited flooding feature. It seems like a normal node with frequent broken links due to high mobility.

DATA FLOODING

In the data flooding the malicious node generates many data packets and send it to the IP which does not exists in the network.

3. DSR

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was exclusively designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network topology to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration. Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing [3]. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route table are frequently updated as new routes are learned. The protocol consists of two major parts: route discovery and route maintenance. The function of DSR routing protocol is in this way: When two nodes which are want to communicated with each other, not in wireless range , if the source node has the related route to destination in its cache table, it will enters the route in data packet headers and the packets will be sent from that specified route, and if it does have the related route to destination, it should start the route discovery process. In route discovery process, route request packet (RREQ) is distributed in network until these packets reach the destination from one route. In this manner, as soon as receiving the first route request packet, destination sends the route reply packet (RREP) to the originator of RREQ. if a link is down because of the movement of middle nodes, a route error packet is sent to the destination and destination tests another route, this task is repeated until the reply reaches the goal. Therefore, destination seeks another route when current route is down. This mechanism causes delay in packet delivery.

4. PROPOSED APPROACH

Algorithm for prevention of the RREQ flooding attack

Algorithm RREQ flooding prevention:
Begin: **if** any node j receives RREQ packet from any node ‘i’ **then**
if node ‘i’ is a friend to j and Z[i]=0 **then**
increment X[i]
X[i]=X[i]+1
if X[i] > Xtf
discard the RREQ packet
Z[i]=1 //blacklist the node i
else
forward the RREQ packet to the next node
endif

end if
if node 'i' is an acquaintance to node j and Z[i]=0 **then**
increment X[i]
X[i]=X[i]+1
if X[i] > Xta
forward the RREQ packet
//Put the RREQ in delay queue and analyze the behavior .If still continue
to broadcast RREQ packets then declare as a Malicious node
Z[i]=1
else
forward the RREQ packet
endif
endif
if node 'i' is an stranger to node j **then**
increment X[i]
X[i]=X[i]+1
if X[i] > Xts
discard the RREQ packet
else
forward the RREQ packet
endif
endif
endif
End

5. SIMULATION RESULTS

In our work we used DSR as a routing protocol. In our simulation we work on 50 nodes to form an ad hoc node and used the random waypoint mobility model for them. All the 50 nodes move in the 1500 x 300 region. The same network model is used to estimate the effect of flooding attack and then our prevention algorithm. We had work on many scenarios to analyze the results so that we can better understand the behavior in presence of malicious node. We assume that each node independently move within the network area and the simulation run for 300 seconds.

Table 1 Loss Comparison

Loss (DSRA-Old)	Loss (DSRAP1-New)
78.03497831	46.05083826
76.69457944	40.10678084
73.75915822	44.68385201
84.16769737	44.72543257
79.20605909	53.12343504
88.54088804	58.55779939

6. CONCLUSION

Because emergence of pervasive computing and availability of the mobile devices, mobile ad hoc networks came into the existence. Mobile ad hoc networks facilitates anywhere, anytime communication, due to the flexibility and open media nature, mobile ad hoc networks are more prone to security threats compared to the wired network.
Therefore security needs are higher in mobile ad hoc networks compared to the previous networks. Many types of attack are possible in mobile ad hoc networks but a flooding attack which is a denial of service type of attack is very dangerous because it tries to consume all most all the resources of the MANET which is limited here.

REFERENCES

[1] Manel Guerrero Zapata & N. Asokan "Securing Ad Hoc Routing Protocols" Wise' 02 September 28,2002,Atlanta Georgia, USA inedxed in ACM 1-58113-585-8/02/009

[2] Mouhcine Guennoun and Khalil El-khatib "A scalable wireless intrusion detection system",IJCSIS, Vol 1,No. 1, may 2009.

[3] Dana Zhang and Christopher Leckie "An evaluation technique for network intrusion detection system" INFOSCALE'06 Proceeding of first international conference on scalable information system,may 29 june 1 2006,Hong kong,ACM 2006 1-59593-428-6/06/05

[4] Elizabeth M. Royer and Santa Barbara Chai-Keong Toh "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks"IEEE personal communication,Apr 1999

[5] David B. Johnson David A. Maltz Josh Broch "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks **"**http://www.monarch.cs.cmu.edu/

[6] Adam Burg " Ad hoc network specific attacks"Seminar Ad hoc networking: concepts, applications, and security Technische Universität München, 2003

[7] N. Bhalaji, Sinchan banerjee and 3A.Shanmugam A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks" Journal of Computer Science 4 (7): 538-544, 2008 ISSN 1549-3636 © 2008 Science Publications.

[8] Malcolm Parsons and Peter Ebinger "Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networks".

[9] Zhang and lee"intrusion detection system in ad-hoc networks"MOBICOM 2000 bostom MA USA.

[10] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad hoc Networks", In Proc. ACM/IEEE Int'l. Conf. on Mobile Computing and Networking, pp 275-283, 2000.

[11] Marianne A. Azer,Sherif M. El-Kassas and Magdy S. El-Soudani "A survey on anomaly detection methods for Ad Hoc networks",Ubiquitous computing and communication journal.

[12] Tiranuch Anantvalee and Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks"

