



**INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH
TECHNOLOGY**

**EFFECT OF RUSHING ATTACK IN MZRP AND MULTICAST COMMUNICATION
IN MOBILE AD HOC NETWORK**

Dr. T.Karthikeyan* , S.Archana

Associate Professor, Department of Computer Science,

² Research Scholar, Department of Computer Science,

PSG College of Arts & Science, Coimbatore, India

ABSTRACT

MANET is a self organizing system of mobile nodes that exchange information through wireless network with no fixed infrastructure. Multicast is communication between a single sender and multiple receivers on a network. Otherwise it transmits a single message to a select group of recipients There are several attacks in MANET that alter the routing. Some examples are Rushing attack, flooding attack, wormhole attack etc. The rushing attack can affect the performance of MZRP(Multicast Zone Routing Protocol) routing protocol in wireless network and also see the impact of rushing attack at the different position of attacker i.e. near sender, near destination node and anywhere in the network.. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, and lack of centralized monitoring. In Rushing attack, the attacker exploits the duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group and this will affect the Average Attack Success Rate

KEYWORDS: MANETs, rushing attack, Multicast, Security, attack strategies, Security threats.

INTRODUCTION

A mobile ad hoc network is a self-organizing system of mobile nodes that communicate with each other via wireless links with no infrastructure or centralized administration such as base stations or access points[1]. Communication and collaboration among a given group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and resources, since a single message can be delivered to multiple receivers simultaneously. Existing multicast routing protocols in MANETs can be classified into two categories: tree based and mesh-based. In a multicast routing tree, there is usually only one single path between a sender and a receiver, while in a routing mesh, there may be multiple paths between each sender receiver pair. Routing meshes are thus suitable than routing trees for systems with frequently changing topology such as MANETs due to availability of multiple paths between a source and a destination. A Mobile ad-hoc network which is also known as a mobile meshnetwork is a self-configuring wireless network of mobile nodes.[2]

In MANET nodes act as the router or host to transmit the data to other nodes in multi-hop fashion. Each node forwards the packets unrelated to its own use. In MANET there are two types of routing- unicast routing and multicast routing. The unicast routing is used for one to one communication whereas multicasting is used for one to many communications. For the unicast routing different routing protocols are used like- DSDV, DSR, AODV etc. Similarly for the multicast routing there are different routing protocols like- MAODV, ODMRP, MZRP etc.[3]

Security is an essential requirement in MANET environments. Compared to wired networks, MANETs are more vulnerable to security attacks due to lack of trusted centralized authority, lack of trust relationships between mobile nodes, easy eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices[4]. The security issue of MANETs in group communications is even more challenging because of the involvement of multiple senders and multiple receivers. Although several types of security attacks in MANETs have been studied in the literature, the focus of earlier research is on unicast (point to point) applications.

Secure neighbor detection implies that two nodes detect a bidirectional link between themselves. Generally a node broadcasts an advertisement to allow its neighbor to detect it[5]. Most of the on-demand protocols perform the secure neighbor detection. In those on-demand protocols, nodes who receive a route request consider itself the neighbor of

previous-hop node. When a node transmit a request is claim a path between sender and receiver, but this secure neighbor detection cannot prevent an attacker to receiving a request. If the address of previous-hop node is unauthorized, so an attacker can claim to be any node propagating a request and next hop will trust that information. That is the reason to applying a concept of secure route discovery. In secure route discovery sender broadcast the route request very rapidly. To reduce the rushing attack, a randomized path selection technique is used. In traditional route request forwarding the receiving node receive the request and immediately forward the request but in modified technique, a receiving node collect all the route request and select a request at random and forward it. Two main parameter is used in this technique: The no. Of request packet to be collected and the algorithm by which timeout are chosen. When the no. Of request is chosen to be large, randomized forwarding will heavily rely on timeout to trigger request forwarding will reduce security. Generally perfect topology information is not available. When it is available then the timeout is based on number of between sender and receiver. Closer nodes should choose shorter timeout than far-away nodes. If topological information is not available then node can randomly choose timeout. This approach reduce the security because every node trying to choose the shorter timeout[6].

Multicasting has advantage over the multiple unicast transmission; this way network bandwidth and resource may be saved. Multicast routing can be classified into two categories: tree-based and mesh-based[7]. In tree-based multicast routing, there is a single route from source to destination. If this route break then the communication between nodes will not be possible. While in mesh-based multiple routing, every node connect to every other node in the network, so is a route break between two nodes then many alternative will be allow to forward packet from source to destination. In mesh-based multicast routing, network will frequently change the topology and found the path between the nodes.

MATERIALS AND METHODS

LITERATURE REVIEW

Satyam Shrivastava [8] has proposed to list the techniques, which are used to overcome the rushing attack and also focused on how they work.

V. Palanisamy, P. Annadurai [5] has already proposed the measure of the impact of Rushing attack and their node positions which affect the performance metrics of Average Attack Success Rate with respect to three scenarios: near sender, near receiver and anywhere within the network.

Al Shahrani, A.S[10] has highlighted the strengths and weaknesses of the Secured Dynamic Source Routing protocol that present a solution to address the rushing attack problem

PROPOSED MODEL:

Multicast Zone Routing Protocol (MZRP)The multicast extension of zone routing protocol (ZRP) is MZRP.It combines the feature of both proactive and reactive routingprotocols. MZRP is shared tree multicast routing protocol. In thistwo type of nodes - forwarding node and multicast group membernodes. In MZRP there are two phases- tree initialization phase and tree maintenance phase.

Tree Initialization Phase

To create a multicast tree over the network source node initiatea two stage processes. In the first stage source node tries to forma tree inside the zone. In the second stage it extends the tree tothe entire network. To create the tree initially source node sends aTREE_CREATE control packets to nodes within its zone throughunicast routing. The interested node joins the group by sendingTREE_CREATE_ACK packet and form the route. To extend thetree outside the zone, source node sends a TREE_PROPAGATEpacket to all border nodes of the zone.

Tree MaintenancePhase

As the multicast tree is created, the source node periodicallytransmit the TREE_REFRESH packet to refresh the multicasttree. If any node doesn't receive this packet within a specifictime interval, it removes the corresponding stale multicast routeentry. When any link break is occur then downstream nodes areresponsible for detecting and rejoining the multicast group.

Classification of AttacksThe routing attacks are classified into two main categories

- Internal vs. External attack
- Active vs. Passive attack

Internal vs. External Attack- as the name clear that the internal attacks are carried out by compromised node or malicious node that are the part of network domain. In this attacker node use thesecret information of the network. An external attack is carriedout by a node or group of nodes which are not the part of networkdomain.

Active vs. Passive attack- an active attack alters the system resources and also effects their operations. Active external attacks can be carried out by outside sources that do not belong to the network. The passive attack uses the information from the system but doesn't affect the system resources.

A. Rushing attack

Rushing attack is an effective denial of service attack, which is against the on-demand routing protocols. Rushing attack also known as "sudden forward motion attack" A rushing attack uses the duplicate suppression mechanism by which it fastly forward the route discovery reply to the routing request broadcast in order to gain the access to the forwarding data. Impact of rushing attack at the different position of attacker node

There are three scenarios:

1. When the attacker node present near the sender
2. When the attacker node present near the destination
3. When the attacker node present anywhere in the network.

Rushing Attack and its Impacts in Ad hoc Networks:

Multicast is communication between a single sender and multiple receivers on a network. Otherwise it transmits a single message to a select group of recipients. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer (and possibly a directional antenna). Furthermore, due to the limitations of the medium, communications can easily be perturbed; MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Typically, multicast on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker. The rushing attack, that acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols, including protocols that were designed to be secure. In this work, to simulate three scenarios:

- * The attacker node is place at near sender
- * The attacker node is place at near receiver.
- * The attacker node is place anywhere within the network.

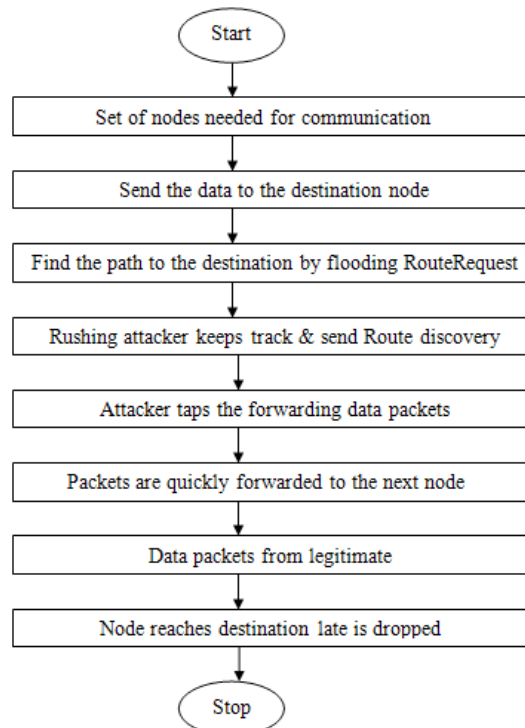


Fig. 1: Rushing Attack Formation (Adapted From [11])

Based on above scenarios, to simulate how the Rushing attack affects the network performance.

Rushing Attack Formation

Step1: Set of N number of nodes are created.

Step2: Create a connection between nodes.

Step3: Rushing node invaded into the forward multicast group.

Step4: Send the packet to the particular groups

Step5: At mean time attacker node tap all the packets.

Step6: The packets in the attacker node are then quickly forwarded to the next upcoming node.

Step7: The data packets from the legitimate node reaches the destination late and so it is dropped as duplicate packet.

Step8: Rushing node in the multicast grouping, affect the Avg Attack Success Rate.

Rushing Attack Based on Three scenarios:

The attacker node A is placed at near sender. The data packets from the sender are forwarded to both the node A and C at the same time. The attacker nodes quickly forward the data packet to node E than the node C. The attacker node forwards the packet to node E then to G and B node. Finally Receiver R receives the data packets that are forwarded by attacker node. The performance of Attack Success Rate with respect to this scenario is calculated.

Rushing Node at near sender

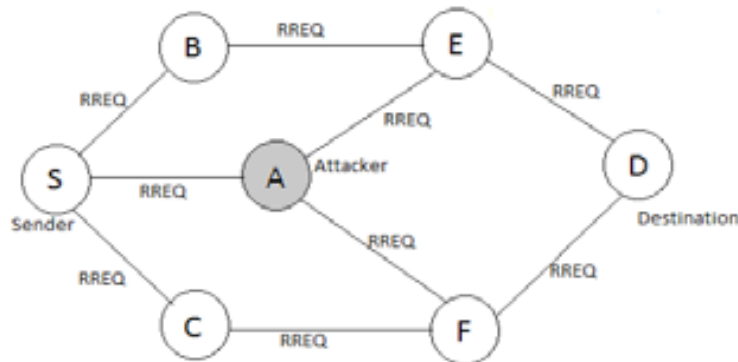


Fig. 2: Attacker Node Present Near the Sender

Algorithm for near sender

Step 1: Create a set of n number of nodes

Step2: Create a connection between the nodes

Step3: Invade the attacker node at near sender

Step4: Sender sends the packet through specified path.

Step5: Other forward nodes, forward the packet to the next node.

Step6: The attacker node taps all the packets.

Step7: The attacker node quickly forwards the packets to the next node that are closest to the receiver

Step8: The data packets are then finally reaches the destination node.

Rushing Node at near Receiver

The attacker node A is placed at near receiver. The sender node forwards the data packets to both the node B and C at the same time. The data packet can pass through either B, E and G nodes or C, F and G nodes. When the data packet reaches the attacker node A, it quickly forwards the data packet to node R. The performance of Attack Success Rate with respect to this scenario is calculated.

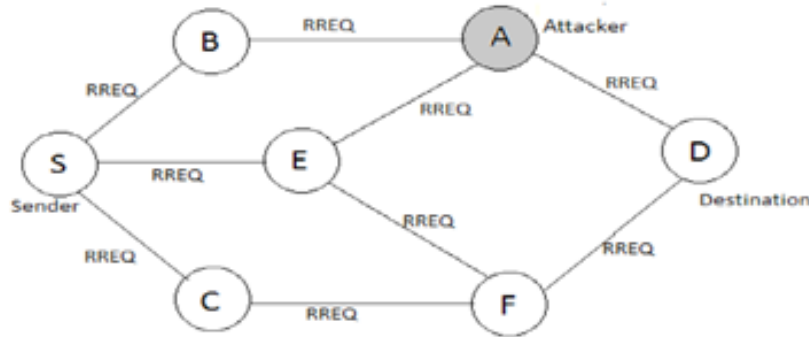


Fig. 3: Attacker Node Present Near the Receiver

Algorithm for near receiver

- Step 1: Create a set of n number of nodes.
- Step2: Create a connection between the nodes.
- Step3: Invade the attacker node at near receiver.
- Step4: Sender send the packets through specified path.
- Step5: Other forward nodes, forward the packet to the next node.
- Step 6: Attacker node tap all the packets through the specified path.
- Step7: The attacker node then quickly forwards the packets.
- Step8: Intermediate node forwards the packets to the destination node.

Rushing attack at anywhere within the network

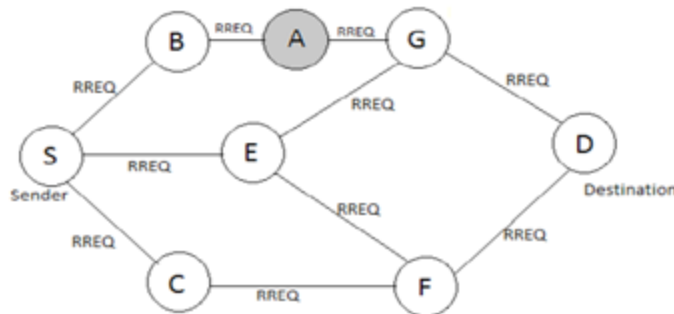


Fig. 4 Attacker Node Present Anywhere in the Network

The attacker node A is placed anywhere within the network. The data packet from the sender is forwarded to the nodes B and C. The data packet is then forwarded through the nodes B and E. But the data packet passed through the node C and then to attacker node A which quickly forwards the data packet to the node G than from the node E. The data packet is then finally reaches the receiver node R through node F. The performance of Attack Success Rate with respect to this scenario is calculated.

Algorithm for anywhere within network

- Step 1: Create a set of n number of nodes
- Step2: Create a connection between the nodes
- Step3: Invade the attacker node at anywhere within the network.
- Step4: Sender send the packet through specified path.
- Step5: Other forward nodes, forward the packet to the next node.
- Step6: The attacker nodes tap the entire packet.
- Step7: The attacker node then quickly forwards the packets.
- Step8: The intermediate node forwards packet to the next node until it reaches the destination

RESULTS AND DISCUSSION

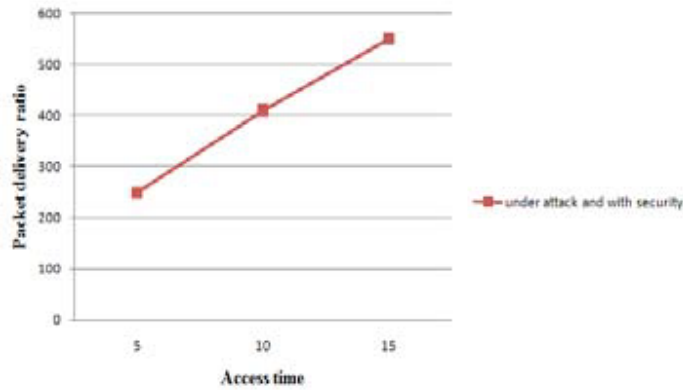


Fig. 5: PDR for 50 Nodes in MZRP Near Sender

Fig. 5 shows the Packet Delivery Ratio (PDR) is high when the attacker node is present near the sender because in MZRP inside the zone proactive approach is used whereas outside the zone reactive approach is used. Rushing attack is basically against the on-demand (reactive) routing protocols.

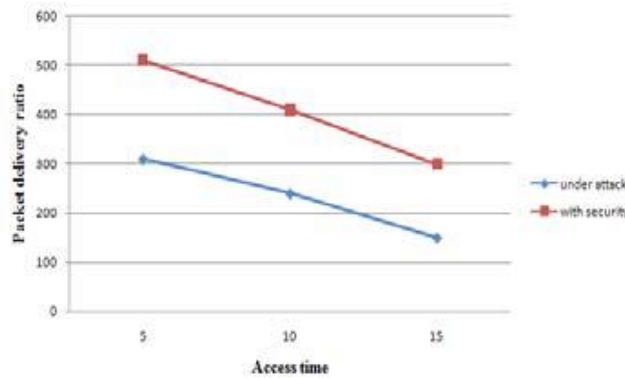


Fig. 6: PDR for 50 Nodes in MZRP Near Destination

When the attacker node is present near the destination in that case PDR (packet delivery ratio) is low. Because outside the zone reactive approach is used. By using threshold value the PDR can be improved.

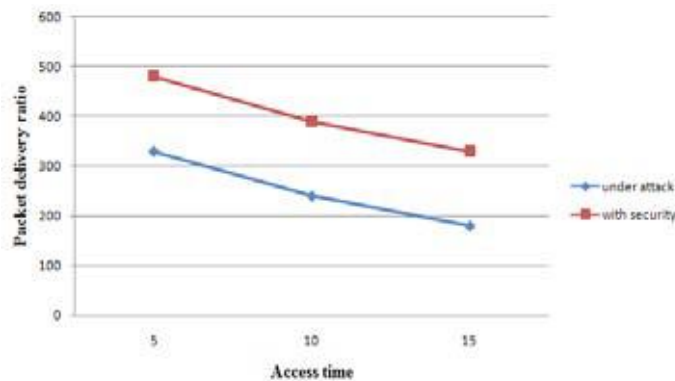


Fig. 7: PDR for 50 Nodes in MZRP Anywhere in the Network

Fig. 7 shows that the PDR is low when the attacker node is present anywhere in the network. In that case attacker node receive the request from the previous intermediate node and then forward to the other intermediate node.

CONCLUSION

The Rushing attacks are more likely to succeed in a multicast session where the number of multicast senders is small and/or the number of multicast receivers is large. The goal of the project is to draw the graph based on the rushing attack position in the network. With respect to the attack positions, the best position to launch rushing attacks is at the near receiver, have the highest success rates. The rushing attack near sender have the low success rate and final attack position is likely to take place anywhere in the network, have the least success rate.

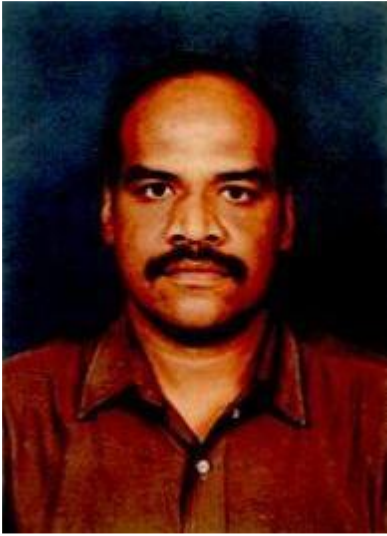

ACKNOWLEDGEMENTS

We are grateful to the God for the good health and wellbeing that were necessary to complete this Research Paper. This research paper was supported/partially supported by our PSG College of Arts and Science. We thank our colleagues from The Department of Computer Science who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

REFERENCES

- [1] Jiejun Kong, Xiaoyan Hong, Mario Gerla, — Modeling Ad-hoc Rushing Attack in a Negligibility-based Security Framework, September 29, 2006, Los Angeles, California, USA.
- [2] Bruschi, D. and Rosti, E., — Secure Multicast in Wireless Networks of Mobile Hosts: Protocols and Issues, Mobile Networks and Applications, Volume 7, 2002, pp 503 - 511.
- [3] Shaveta Jain, Kushagra Agrawal, “Simulation Based Performance Comparison of Adhoc Routing Protocols”, In International Journal of Engineering Research and Applications (IJERA) Advances in Engineering and Technology (AET- 29th March 2014).
- [4] Y.-C. Hu, A. Perrig, and D. B. Johnson, — Efficient security mechanisms for routing protocols, in Network and Distributed System Security Symposium, NDSS, 2003.
- [5] V. Palanisamy and P. Annadurai, Impact of Rushing attack on Multicast in Mobile Ad Hoc Network, IJCSIS, Vol. 4, No. 1 & 2, August 2009, USA.
- [6] YihChun Hu, Adrian Perrig, David B. Johnson, — Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols — , WiSe 2003, September 19, 2003, San Diego California, USA Copyright 2003 ACM.
- [7] Gajendra Singh Chandel, Rajul Chowksi, “Effect of Rushing Attack in AODV and its Prevention Technique”, In International Journal of Computer Applications, Vol. 83, No. 16, December 2013.
- [8] Satyam Shrivastava, “Rushing Attack and its Prevention Techniques”, In International Journal of Application or Innovation in Engineering and Management (IJAIEM), Vol. 2, Issue 4, April 2013.
- [9] K.Prabu, Dr.A.Subramani, “Performance Comparison of Routing Protocols in MANET”, In International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 9, September 2012
- [10] Al Shahrani, A.S, "Rushing Attack in Mobile Ad Hoc Networks", Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference
- [11] Gajendra Singh Chandel, Rajul Chowksi, “Effect of Rushing Attack in AODV and its Prevention Technique”, In International Journal of Computer Applications, Vol. 83, No. 16, December 2013.

AUTHOR BIBLIOGRAPHY

	<p>Dr.T.Karthikeyan received his graduate degree in Mathematics from Madras University in 1982. Post graduate degree in Applied Mathematics from Bharathidasan University in 1984. Received Ph.D., in Computer Science from Bharathiar University in 2009. Presently he is working as a Associate professor in Computer Science Department of P.S.G.College of Arts and Science, Coimbatore. His research interests are Image Coding, Medical Image Processing and Datamining. He has published many papers in national and international conferences and journals. He has completed many funded projects with excellent comments. He has contributed as a program committee member for a number of international conferences. He is the review board member of various reputed journals. He is a board of studies member for various autonomous institutions and universities. He can be contacted by email t.karthikeyan.gasc@gmail.com</p>
	<p>S.Archana is a Research Scholar in Department of computer sciences, PSG College of Arts and Science, Coimbatore. She has received Master of Computer Applications with First class degree in 2011. Her research interests are Wireless Networks Email: s.archana30@gmail.com</p>