Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Networks

Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari
Faculty of Computing,
Universiti Teknologi Malaysia (UTM)
Skudai 81310, Johor, Malaysia
{mohsen.gh100, sabdrazak}@gmail.com, ismailfauzi@utm.my and hassan.chizari@gmail.com

***Abstract*—Because of the nature of wireless channels, Mobile Ad-Hoc Networks (MANETs) are vulnerable against many threats and attacks. Beside of this, the mobility of the network nodes made the security of routing protocols one of the most interesting research areas over Ad-Hoc networks. Moreover, Rushing attack became one of the common attacks against routing protocols in MANETs. Although there are many researches over Rushing attacks, the security research community suffers from a famine of evidence to present the exact position of this kind of attacks in MANETs clearly. Therefore, we paid particular attention to this issue to clarify the position of Rushing attacks against routing protocols and the functionality of this category of attacks. We hope that our document be useful for other researchers in understanding mentioned issue in face with this class of attacks.**

Keywords: Rushing Attacks, Routing Protocols, MANETs

I. .INTRODUCTION

In the recent years, many researchers worked on the area of security in Mobile Ad-Hoc Networks (MANETs). The main reason is that providing security for these networks is a very challenging issue due to their specific features. The main property of MANETs is that there is not any fixed infrastructure in these sort of networks, so all nodes should work together to keep the network integrated. Thus, many significant network functions such as routing must be run by the existing nodes. It can be claimed that this function is one of the most significant ones that made the this kind of networks a prone one to be vulnerable against many security attacks.

There are many protocols that try to handle the issue of routing in MANETs. In general, routing protocols for MANETs can be classified into two categories; "Periodic Protocols" and "On-demand Protocols." Although these protocols help the MANETs work easily, but they are weak against many attacks that we introduced them in section 4.

On-demand routing protocols such as ODMRP [1] and MAODV [2] use duplicate suppression technique to prevent flooding. It means that if the source node that needs to find the path to the destination, floods the network with the route discovery packets, existing intermediate nodes will process only the first non-duplicate packet and will drop the other duplicate ones. By the use of the Rushing attack, the attacker tries to abuse this feature by sending the route discovery packets quickly to gain access to the forwarding group.

Since, Rushing attacks occur against routing protocols in Ad-Hoc networks, we assigned the background of the main issue to the first and the second sections of this paper. We presented an overview on mobile Ad-Hoc networks in section 2. Then in section 3, we focused on existing routing protocols in MANETs. In continue to what mentioned in section3, we introduced possible attacks against routing protocols and classified them in two groups in section4. The main achievement of this section is to determine the position of the subject "Rushing attacks" in the "Attack against routing protocols" scientific topic. In the next section, we concluded Rushing attack's functionality as an instance of Routing-disruption attacks. Actually, by the use of simple examples we demonstrated that Rushing attacks can be investigated in three scenarios based on the attacker's position.

To solve mentioned problems, many researchers tried to present secure protocols against Rushing attacks. Although those protocols are safe in some situations, they are not the best way to prevent this kind of attacks. Based on our studies, there are three methods which are mentioned in part 6. These methods can be used as a part of any protocol oreven can be combined together as a protocol to be able to prevent Rushing attacks in MANETs.

II. MOBILE AD-HOC NETWORKS

MANETs are one of the important categories of wireless communicating networks. These networks have special characteristics that made the use of them easy, but vulnerable against many threats and attacks. Some of the significant criteria are investigated as follow for this class of networks:

- ***Network Infrastructure.*** Base on this property, MANETs do not have any fixed infrastructure. Therefore, all the nodes work together to perform the network functions (such as routing) by multihopping approach [3,4].
- ***Self-Organization.*** Due to the running of the network functions by the means of existing nodes, MANETs are self-organized. It is worth mentioning that the nodes inside a mobile Ad-Hoc network must be able to determine their configuration parameters [5].
- ***Mobility.*** This property emphasizes on this fact that the nodes are able to repositioning themselves or leave the network at any time [5].
- ***Multihopping.*** Because of running network functions by the use of existing nodes in such a multihopping network, the path from source to destination traverses several other nodes [5].
- ***Network Topology.*** The Network Topology is random, dynamic and unpredictable. The reason is that existing nodes are mobile and can change their position easily. In addition, wireless connections are temporary and error prone that makes the topology weakly connected [3,6].
- ***Scalability.*** Mobile Ad-Hoc networks can easily grow even to thousands of nodes [5].
- ***Resource limitations.*** MANETs suffer from the traditional resource problems in wireless and mobile networks such as bandwidth optimization, power control, and transmission-quality enhancement, etc. [6,7].
- ***Security.*** The wireless nature of communicating channels made MANETs unsecure. More precisely, the active and passive adversaries can eavesdrop or spoof the channel. As a result, MANETs are assailable much more than the traditional fixed-infrastructure networks [3,4,5].

III. ROUTING PROTOCOLS

Due to the special characteristics of mobile Ad-Hoc networks (e.g. the dynamic nature, limited resources, etc.) it is very difficult to design routing protocols especially from security viewpoint.

In continue to what mentioned above, it seems that routing protocols in Ad-Hoc networks must be highly optimized to delegate new routing information as quickly as changing the conditions. Moreover, it seems that interactions between the nodes must be faster and more frequent than they are in the traditional wired networks.

One of the most important drawbacks of routing protocols in this category of networks is that security mechanisms are not lightweight and appropriate for resource-constrained nodes. Mentioned drawback can cause some problems such as making delay or preventing exchanges of routing information. These problems can lead to reducing routing effectiveness, consuming network or node resources extremely, leading too many new opportunities for possible Denial-of-Service attacks through the routing protocol, etc.

In continue to mentioned background above, it can be claimed that all routing protocols in Ad-Hoc networks are placed into one of the two main categories as follow [8]:

Periodic Protocols. In this kind of protocols, any node exchange routing information to the other ones periodically in order to make each node aware of current routes to all destinations [9,10,11].

On-demand Protocols. In this kind of protocols, any node tries to exchange routing information in order to pass the received data packet during the need to discover a route [1,2,12,13].

It is worth noting that beside of two mentioned categories, there are some routing protocols, which are a hybrid model of Periodic and On-demand ones (for more details, refer to [14]).

IV. ATTACKS AGAINST ROUTING PROTOCOLS IN MANET

This section classifies and introduces possible attacks against mentioned routing protocols in the previous section. These attacks can be classified into two followed categories [15, 16]:

- ***Routing-disruption attacks.*** In this kind of attacks, the attacker tries to act in such a way that seems actual data packets were directed in a dysfunctional path. Some example of these attacks are mentioned as follow:

- ***Blackhole***: An attacker in a blackhole attack distributes fake routing information (like, claiming falsified short distance information) to attract the traffic. This attacker then drops the data packets.
- ***Gray hole****:* This attack is similar to the blackhole attack, but the attacker drops the packets selectively.
- ***Gratuitous detour****:* In this attack, an attacker adds virtual nodes to the route to make the path longer than what it is.
- ***Wormhole****:* In this kind of attack, a pair of attackers use a tunnel channel through a private network connection. Obviously, they can distribute existing packets faster than normal cases in a multi-hop route. As a result, tunneling the routing control message can disrupt the routing algorithm.
- ***Rushing****:* In this attack which is against On-demand routing protocols, an attacker distributes ROUTE REQUESTS quickly throughout the network. Consequently, existing nodes will drop any original legitimate ROUTE REQUESTS, because of the duplicate suppression rule in those protocols.
- ***Resource-consumption attacks.*** In this category of attacks, the attacker adds extra packets into the network to waist essential network resources such as bandwidth, etc. Moreover, the attacker sometimes tries to consume the node resources such as memory or computation power.

Next section investigates the Rushing attack as a Routing-disruption attack.

V. RUSHING ATTACKS

Rushing attacks, which can be assigned to the Routing-disruption attacks are against On-demand routing protocols such as ODMRP [1], MAODV [2], FGMP [12], and ADMR [13]. The significant vulnerability of these protocols is that they use duplicate suppression method in their operations. If roughly speaking, when a source node floods the network with the route discovery packets to find the destination path, intermediate nodes only process the first non-duplicate packet and drop the other ones. In a Rushing attack, the attacker tries to use the duplicate suppression by quickly forwarding the route discovery packets to gain access to the forwarding group.

The Rushing attack can act as an effective Denial-Of-Service attack against all currently proposed On-demand MANET routing protocols [17,18]. The next subsection, investigates this attack based on the different positions of the attacker.

A. Different Scenarios of Rushing Attacks

In this section, we are going to describe Rushing attacks based on the attacker's position. As we will see, this issue is explained through some simple examples. The three possible scenarios are as followed [17,18,19]:

Rushing node near the Sender node

In this scenario as illustrated in the Figure 1, the sender, "S" sends the packets to receiver, "R" as the destination node. In addition, the attacker "A" is located near the "S." Thus, at the same time packets can be forwarded to both nodes "A" and "C," which is another neighbor of the "S". Therefore, the attacker "A" can forward the packets to the node "E" faster than the node "C" and the rout will be completed with "G," "B" and finally the receiver "R." As a result, "R" receives the data packets, which are forwarded by the attacker node [17,19].

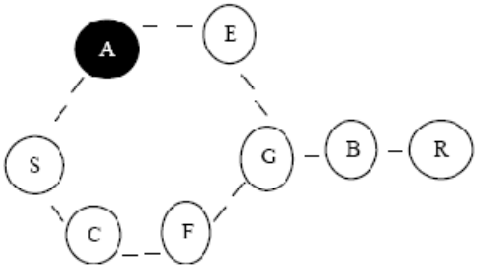

Figure 1. Rushing attacker near the sender [17,19]

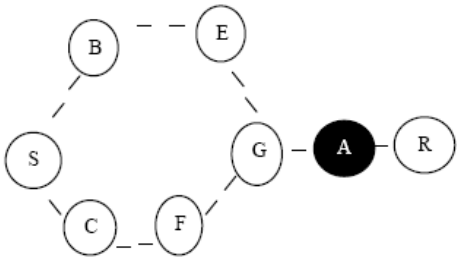

Figure 2. Rushing attacker near the receiver [17,19]

Rushing node near the Receiver node

As it is depicted in the Figure 2, in the second scenario the sender node "S" sends the packets to the receiver one "R." In this case, the attacker "A" is located near the receiver node. Therefore, the sender "S" forwards the data packets to the both nodes "B" and "C" simultaneously.

It is not important that the data packets forward to the receiver "R" by passing the rout which includes "B, E" or "C, F" because they must be forwarded by the attacker "A" to reach the receiver node "R" [17,19].

Rushing node at anywhere within the network

In the last scenario that can be seen in the Figure 3, the attacker "A" can be everywhere in the network.

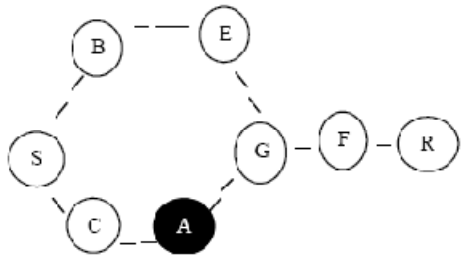

Figure 3. Rushing attacker at anywhere within the network [17,19]

After that the Sender node "S" sends data packets through the specified path, the other forwarding nodes can pass the packets to the next neighbor. Then, the attacker "A" taps the entire packets. As a result, the attacker can quickly forward the packets to the intermediate nodes and the path will continue until the packets reach to the destination node "R" [17,19].

VI. A SUBSET OF PROPOSED DEFENSES AGAINST RUSHING ATTACKS

In this section, we are going to describe some proposed methods against the Rushing attacks. Our guideline to reach this decryption is based on what Hu et al. proposed in [20]. Based on this evidence, a subset of three methods "Secure Neighbor Detection", "Secure Route Delegation" and "Randomized ROUTE REQUEST Forwarding" as an integrated protocol, is able to prevent Rushing attack [20]. Our aim is to introduce some possible solutions against Rushing attacks to show a guideline for the beginners and we do not claim that these methods are the best,

The subsections (6.1), (6.2), and (6.3) introduce the mentioned techniques. It can be deduced that the use of any mixed method can be used against Rushing attacks.

A. Secure Neighbor Detection

As a simple scenario of the Rushing attack, the attacker forwards a ROUTE REQUEST upper than the normal radio transmission range (e.g. via using a higher gain antenna), thus she can suppress subsequent requests from this Route Discovery. In this case, both of the sender and the receiver entities, can verify that either other parties are within the normal direct wireless communication range by the use of secure Neighbor Detection method.

In a Secure Neighbor Detection method, if two nodes are able to communicate because of being in the same maximum transmission range, they can detect each other as neighbors. Therefore, by the use of this technique the attacker is not able to introduce two nodes, which are not within the maximum transmission range as neighbors. Moreover, she is unable to show herself as a neighbor of another node without being able to hear the packets.

B. Secure Route Delegation

In the SECURE ROUTE DELEGATION method, each node must be able to verify that all the Secure Neighbor Detection steps were done between any adjacent pair of nodes. To achieve this goal, Secure Route Delegation uses Secure Border Gateway Protocol (S-BGP). We can describe this method in a simple scenario; one node such as I1 receives current ROUTE REQUEST (originating from Sender node of message destined for Receiver node) at first. Then I1 performs the secure neighboring detection and finds that I2 is a neighbor node. In this method, I1 delegates the ROUTE REQUEST to I2. Actually, I1 does not delegate the whole message, because I2 can reconstruct all the fields of the message and verify the signature. The ROUTE DELEGATION message can be packed with the last message of the Secure Neighbor Detection. If I2 believes that I1 is really a neighbor, he will accept the ROUTE DELEGATION and continue the protocol. Therefore, signs another ROUTE DELEGATION for the next neighbor.

C. *Randomized ROUTE REQUEST Forwarding*

The Use of Secure Neighbor Detection and Secure Route Delegation techniques are not sufficient enough to defend against the Rushing attacks. The main reason is that an adversary can still get the advantage of ROUTE REQUEST. By the use of a random selection technique beside the two other mentioned ones, the chance of a Rushing adversary to dominate all returned routes will be minimized. In the traditional ROUTE REQUEST forwarding method, when a node receives the request, immediately forwards it and drops all subsequent ones. However, it is obvious that in Randomized ROUTE REQUEST Forwarding, when a node receives some ROUTE REQUEST messages, first gathers the number of them, then selects one of them randomly to forward. It is worth mentioning that two important factors that should be considered in this method are the amount of collected ROUTE REQUEST packets and the chosen timeout algorithm.

VII. CONCLUSION

Because of special properties and requirements of mobile Ad-Hoc networks, it is very difficult to make them secure. In order to defend against existing attacks, many protocols offered by researchers but there are still many drawbacks. Rushing attacks are one of the common attacks in MANETs that utilize the duplicate suppression feature of routing protocols. In this paper, we reviewed a subset of proposed Rushing attacks. In addition, we reviewed a subset of proposed methods to prevent this kind of attacks.

REFERENCES

[1] S.J. Lee, W. Su, M. Gerla, 2002. On-demand Multicast Routing Protocol in Multihop Wireless Mobile Networks, ACM/ Kluwer Mobile Networks and Applications 7 (6) 441–453.

[2] E.M. Royer, C.E. Perkins, 1999. Multicast operation of the Ad-Hoc On-demand distance vector routing protocol, in: Proceedings of MobiCom '99, Seattle, WA.

[3] Van der Merwe, J., Dawoud, D., and McDonald, S., 2007. A survey on peer-to-peer key management for mobile Ad-Hoc networks. ACM Comput. Surv. 39, 1, Article 1.

[4] Wua, B., Wua, J., Fernandeza, E., Ilyasa, M. , Magliveras ,S., 2005. Secure and efficient key management in mobile Ad-Hoc networks. Elsevier.

[5] Gerla, M., 2005. Ad-Hoc Networks. Springer.

[6] Giordano, S., 2002. Mobile Ad-Hoc Networks.Wiley.

[7] Wu, J., Stojmenovic, I., 2004. Ad-Hoc Networks. IEEE Computer Society.

[8] Hu, Y-C., Perrig, A., Johnson, D., 2003. SEAD: secure efficient distance vector routing for mobile wireless Ad-Hoc networks. Elsevier B.V.

[9] R.V. Boppana, S. Konduru, 2001.An adaptive distance vector routing algorithm for mobile, Ad-Hoc networks, in: Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001).

[10] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, 2001. Optimized Link State Routing Protocol, Internet-draft, draft-ietf-manet-olsr-05.txt.

[11] J.J. Garcia-Luna-Aceves, C.L. Fullmer, E. Madruga, D. Beyer, T. Frivold, 1997. Wireless Internet Gateways (WINGS), in: Proceedings of IEEE MILCOM _97.

[12] C.-C. Chiang, M. Gerla, L. Zhang, 1998. Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks, AJ. Cluster Comp, Special Issue on Mobile Computing 1 (2) 187–196.

[13] J.G. Jetcheva, D.B. Johnson, 2001. Adaptive demand-driven multicast routing in multi-hop wireless Ad-Hoc networks, in: Proceedings of ACM MobiHoc'01, Long Beach, CA.

[14] Z.J. Haas, 1997. A routing protocol for the reconfigurable wireless network, in: 1997 IEEE 6th International Conference on Universal Personal 1997 IEEE 6th International Conference on Universal Personal Communications Record: Bridging the Way to the 21st Century (ICUPC _97), vol. 2, pp. 562–566.

[15] Hu, Y-C., Perrig, A., 2004. A Survey of Secure Wireless Ad-Hoc Routing. IEEE SECURITY & PRIVACY

[16] Dasgupta, M., Choudhury, S., Chaki, N., 2010. Routing Misbehavior in Ad-Hoc Network. International Journal of Computer Applications 0975 – 8887 Volume 1 – No. 18.

[17] Nandy, R., Barman Roy, D., 2011 .Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme. Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043.

[18] Goyal, P., Batra, S., Singh, A., 2010. A Literature Review of Security Attack in Mobile Ad-Hoc Networks. International Journal of Computer Applications (0975 – 8887) Volume 9– No.12.

[19] Palanisamy, V., Annadurai, P., 2009. Impact of Rushing attack on Multicast in Mobile Ad-Hoc Network. International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[20] Hu, Y-C., Perrig, A., Johnson, D., 2003. Rushing Attacks and Defense in Wireless Ad-Hoc Network Routing Protocols. Copyright 2003 ACM 1581137699/03/0009.